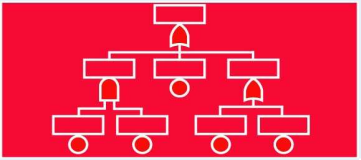
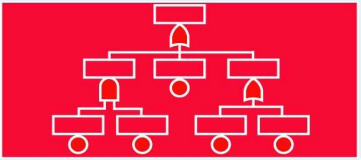
Chapter 3
System Analysis
Failure Modes, Effects, and Criticality Analysis

Marvin Rausand
Department of Production and Quality Engineering
Norwegian University of Science and Technology
marvin.rausand@ntnu.no



Introduction



What is FMECA?

Failure modes, effects, and criticality analysis (FMECA) is a methodology to identify and analyze:

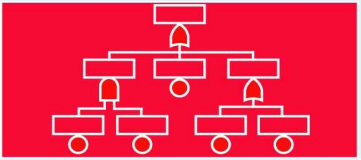
- All potential failure modes of the various parts of a system
- The effects these failures may have on the system
- How to avoid the failures, and/or mitigate the effects of the failures on the system

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)

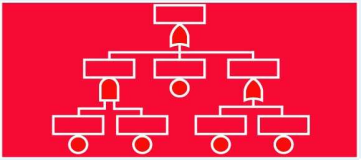
FMECA is a technique to "resolve potential problems in a system before they occur"

– SEMATECH (1992)



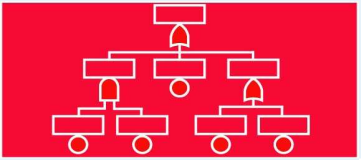
FMECA – FMEA

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.



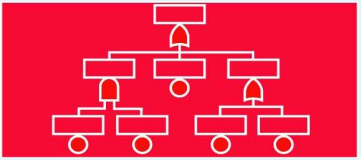
Background

- 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



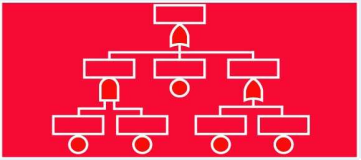
What can FMECA be used for?

- 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.



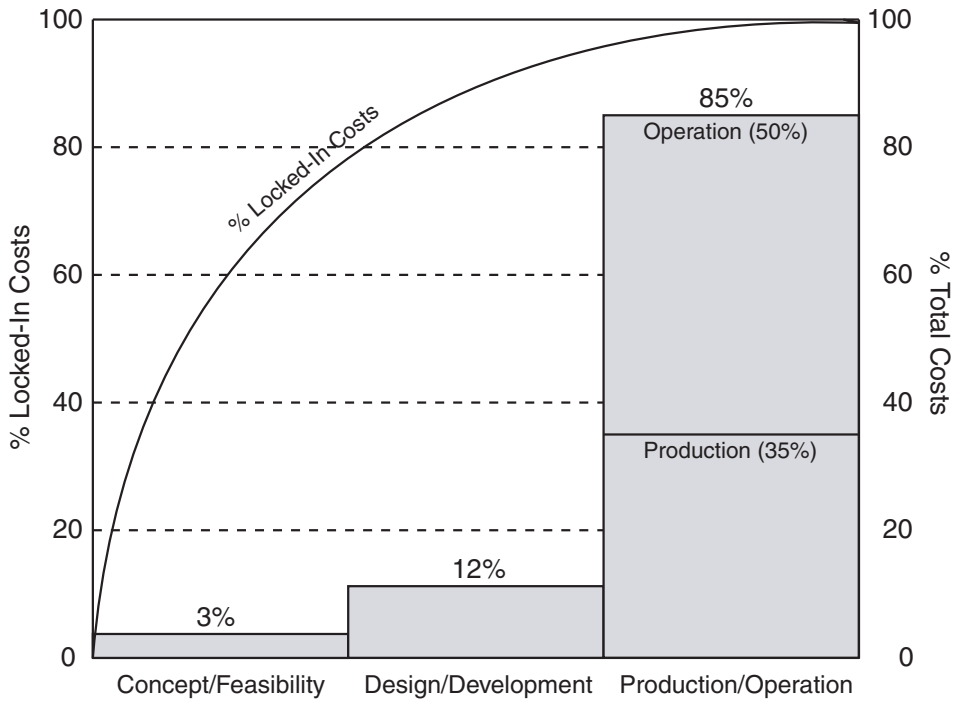
FMECA basic question

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

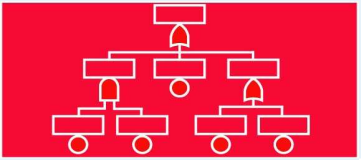


When to perform an FMECA

The FMECA should be initiated as 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:

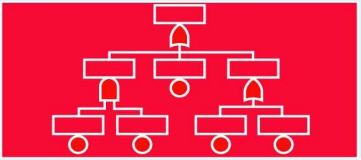


– Source: SEMATECH (1992)



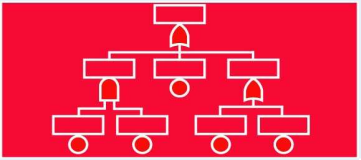
Types of FMECA

- *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



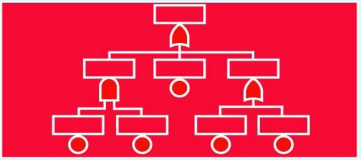
Two approaches to FMECA

- 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.

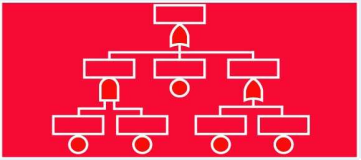


FMECA standards

- 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"

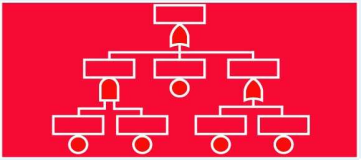


FMECA procedure



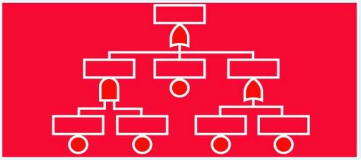
FMECA main steps

1. FMECA prerequisites
2. System structure analysis
3. Failure analysis and preparation of FMECA worksheets
4. Team review
5. Corrective actions



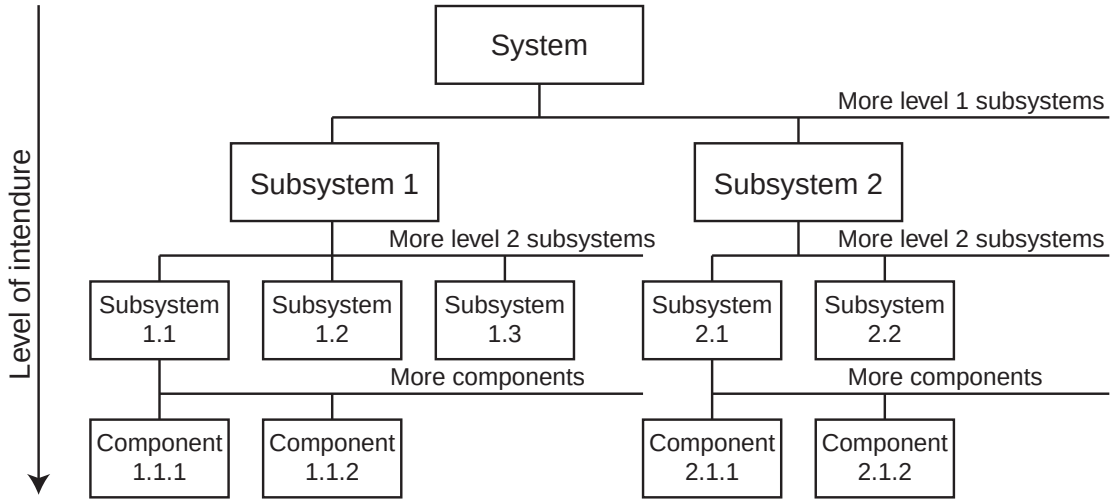
FMECA prerequisites

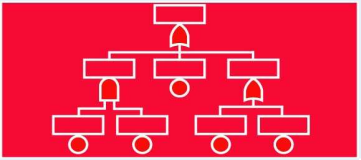
1. Define the system to be analyzed
   (a) System boundaries (which parts should be included and which should not)
   (b) Main system missions and functions (incl. functional requirements)
   (c) Operational and environmental conditions to be considered
   Note: Interfaces that cross the design boundary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

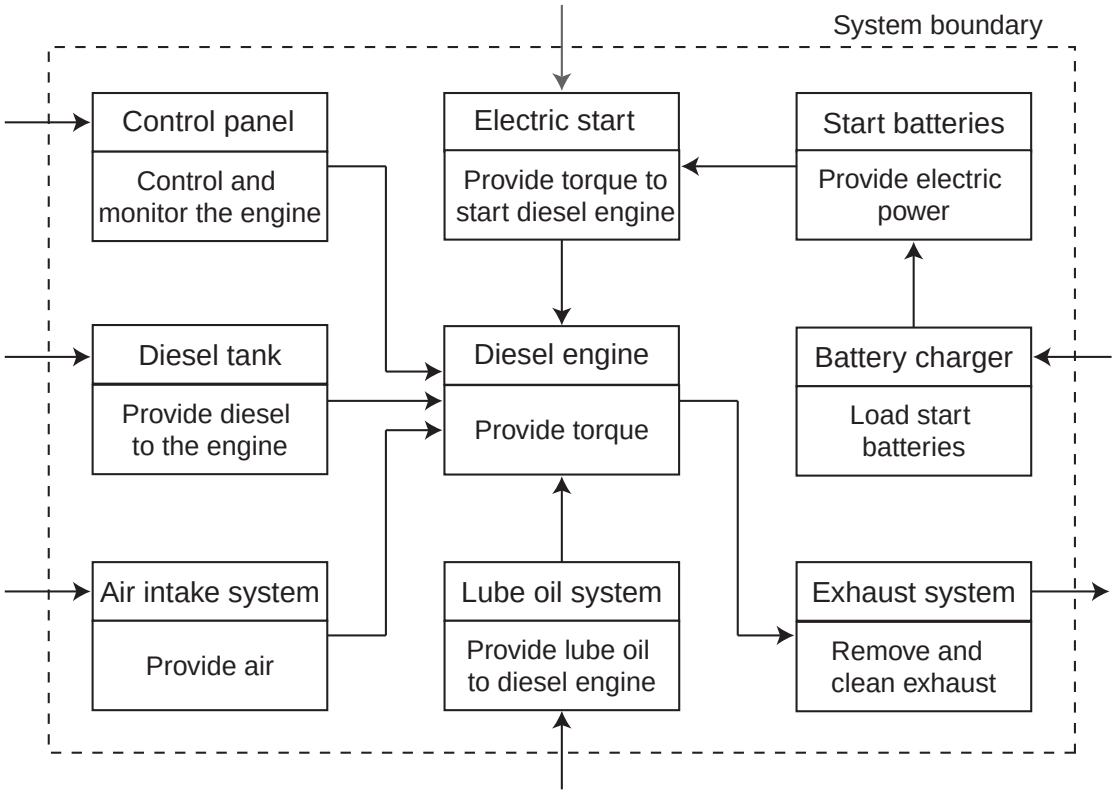
1. Divide the system into manageable units - typically functional elements. To what level of detail we should break down the system will depend on the objective of the analysis. It is often desirable to illustrate the structure by a hierarchical tree diagram:

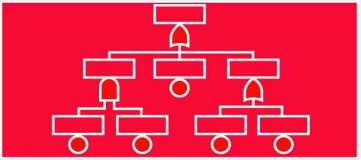




System structure analysis - (2)

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

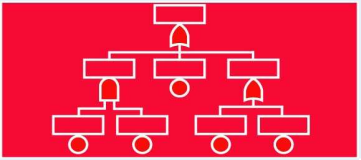




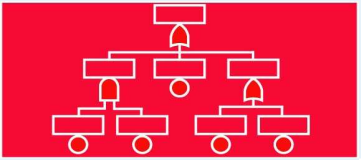
System structure analysis - (3)

The analysis should be carried out on an as high level in the system hierarchy as possible. 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.



Worksheet preparation



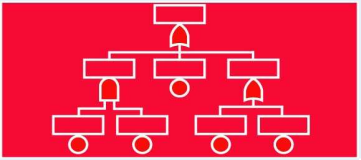
Preparation of FMECA worksheets

A suitable FMECA worksheet for the analysis has to be decided. In many cases the client (customer) will have requirements to the worksheet format - for example to fit into his maintenance management system. A sample FMECA worksheet covering the most relevant columns is given below.

System: Performed by:

Ref. drawing no.: Date: Page: of

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

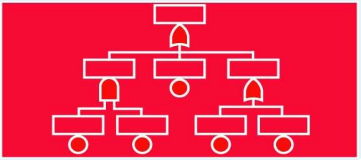


Preparation of FMECA worksheets - (2)

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.

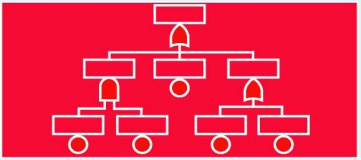
We will now discuss the various columns in the FMECA worksheet on the previous slide.

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.



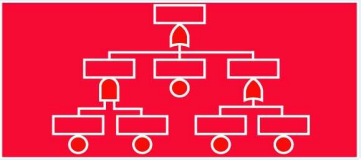
Preparation of FMECA worksheets - (3)

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.



Preparation of FMECA worksheets - (4)

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)
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.

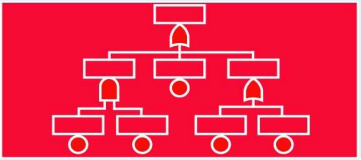


Preparation of FMECA worksheets - (4)

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.

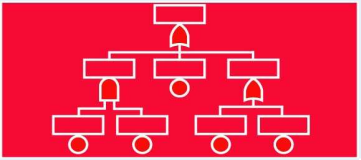
– Source: SEMATEC (1992)



Preparation of FMECA worksheets - (5)

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.

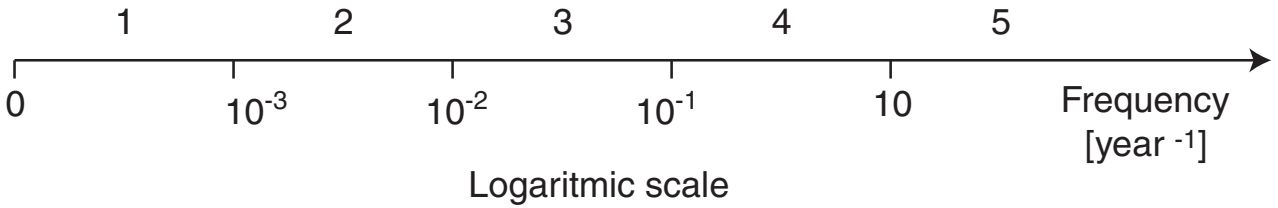
In some applications it may be relevant to include separate columns in the worksheet for *Effects on safety*, *Effects on availability*, etc.



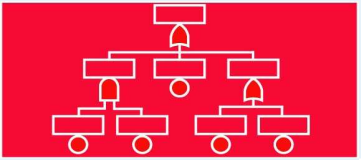
Preparation of FMECA worksheets - (6)

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



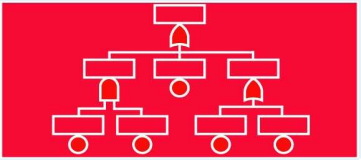
In some applications it is common to use a scale from 1 to 10 where 10 denotes the highest rate of occurrence



Preparation of FMECA worksheets - (8)

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

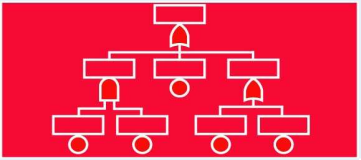


Preparation of FMECA worksheets - (8)

In some application the following severity classes are used

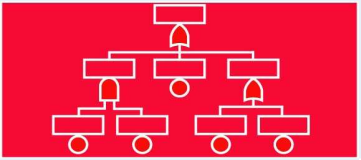
Rank	Description
10	Failure will result in major customer dissatisfaction and cause non-system operation or non-compliance with government regulations.
8-9	Failure will result in high degree of customer dissatisfaction and cause non-functionality of system.
6-7	Failure will result in customer dissatisfaction 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)

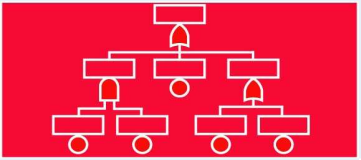


Preparation of FMECA worksheets - (9)

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.



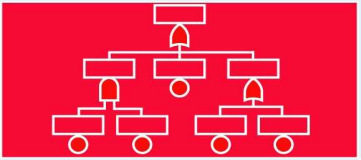
Risk ranking and team review



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

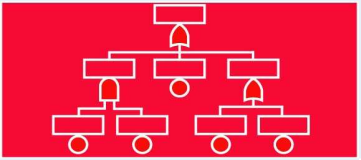
The risk associated to failure mode is a function of the frequency of the failure mode and the potential end effects (severity) of the failure mode. The risk may be illustrated in a so-called risk matrix.

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

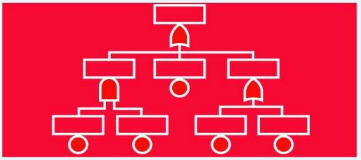
An alternative to the risk matrix is to use the ranking of:

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

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

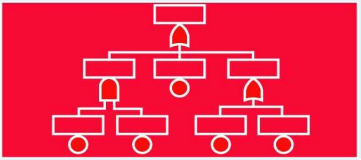
The smaller the RPN the better – and – the larger the worse.



RPN has no clear meaning

- 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

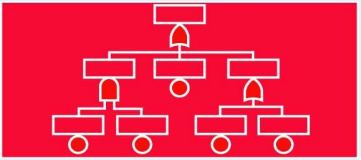
POTENTIAL
FAILURE MODE AND EFFECTS ANALYSIS
Front Door L.H.

___ System 1 - Automobile
___ Subsystem 2 - Body Closures
X Component 3 - Front Door L.H.
Design Responsibility Body Engineering
Model Year(s)/Program(s) 199X/Lion 4dr/Wagon
Key Date 3/3/2003
Core Team T. Fender - Car Product Dev., C. Childers - Manufacturing, J. Ford - Assy Ops (Dalton, Fraser, Henley Assembly Plants)

FMEA Number 1234
Page 4 of 9
Prepared By A. Tate - X6412 - Body Engr
FMEA Date (Orig.) 2/28/2003 (Rev) 3/3/2003

Item / Function	Potential Failure Mode	Potential Effect(s) of Failure	Sev	Class	Potential Cause(s)/Mechanism(s) of Failure	Occur	Current Design Controls	Detec	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Action Results: Actions Taken	Sev	Occ	Det
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
					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
										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
					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
					Wax application plugs door drain holes.	3	Laboratory test using "worst case" wax application and hole size. - Detection	1	21				7	3	1
					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

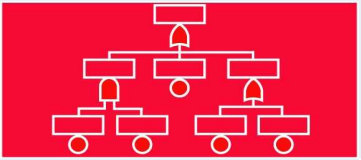
– ReliaSoft Xfmea printout, from www.reliasoft.com



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



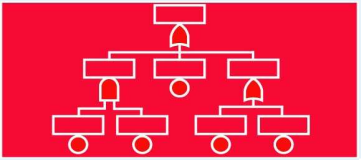
Review objectives

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

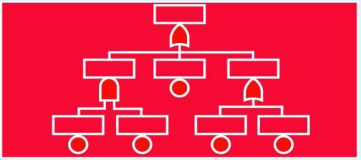
1. To decide whether or not the system is acceptable
2. To identify feasible improvements of the system to reduce the risk. This may be achieved by:
   (a) Reducing the likelihood of occurrence of the failure
   (b) Reducing the effects of the failure
   (c) Increasing the likelihood that the failure 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.



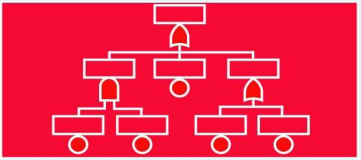
Corrective actions



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.

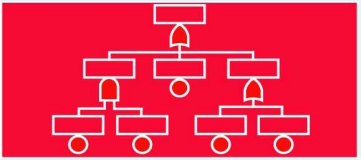
Xfmea

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.	

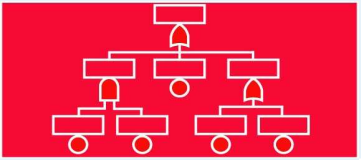
– ReliaSoft Xfmea printout, from www.reliasoft.com



RPN reduction

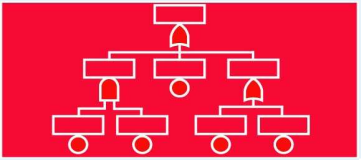
The risk reduction related to a corrective action may be comparing the RPN for the initial and revised concept, respectively. A simple example is given in the following table.

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

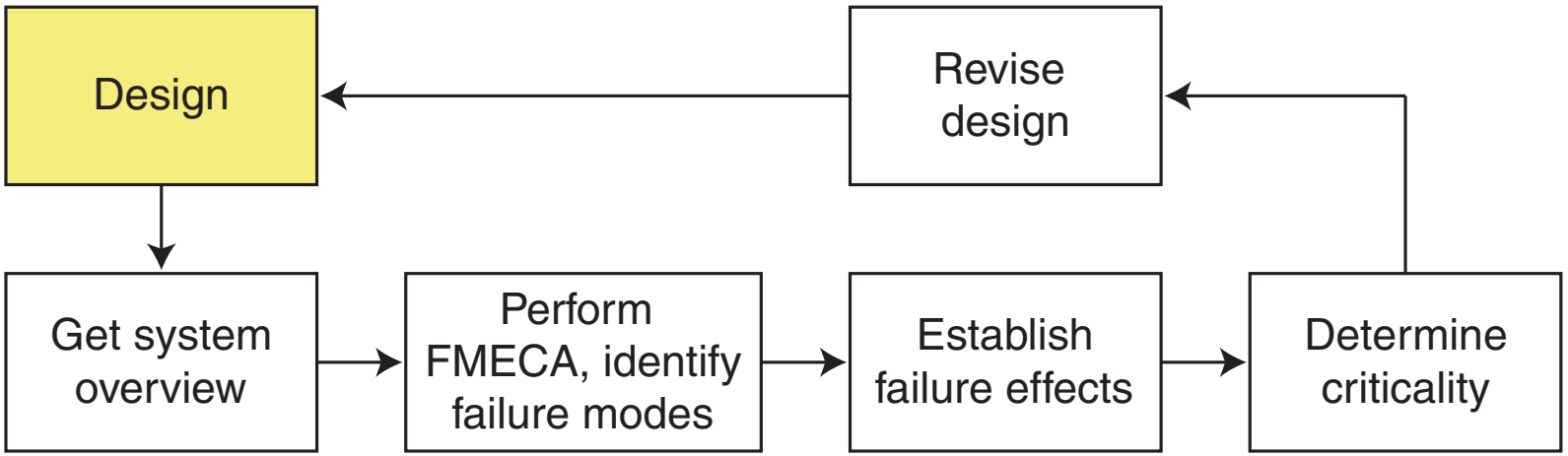


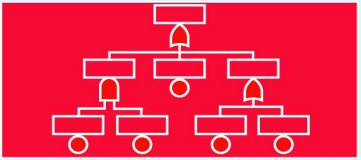
Application areas

- **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.

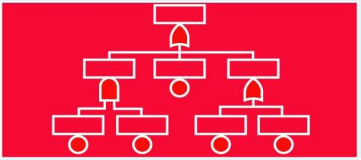


FMECA in design





Conclusions

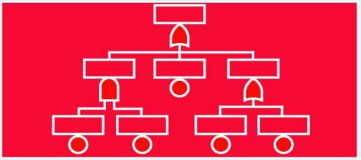


Summing up

The FMECA process comprises three main phases:

Phase	Question	Output
Identify	What can go wrong?	Failure descriptions Causes $\longrightarrow$ Failure modes $\longrightarrow$ Effects
Analyze	How likely is a failure? What are the consequences?	Failure rates RPN = Risk priority number
Act	What can be done? How can we eliminate the causes? How can we reduce the severity?	Design solutions, Test plans, manufacturing changes, Error proofing, etc.

– Based on Kmenta (2002)



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