ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΠΜΣ Κυβερνοασφαλεια
και Επιστημη Δεδομενων
MSc Cybersecurity
and Data Science
DEPT OF INFORMATICS
UNIVERSITY OF PIRAEUS

DEPENDABLE SYSTEMS AND CRITICAL INFRASTRUCTURES DESIGN

RELIABILITY ENGINEERING AND HARDWARE FAULT-TOLERANCE

DIMITRIS AGIAKATSIKAS, MIHALIS PSARAKIS

FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS (FMECA)

Objectives of this lecture

- To understand why Failure modes, effects, and criticality analysis (FMECA) is used
- To become aware of the different approaches to FMECA
- To learn the steps of an FMECA

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.
- A substantial portion of the product's total cost is determined in the early stages of development. This is why is it important of performing FMECA early in the design process, as it can help identify and mitigate the risks associated with potential failures, potentially reducing the locked-in costs by ensuring a more reliable and cost-effective design from the beginning.

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

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.

Boom-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.

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 MAIN STEPS

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

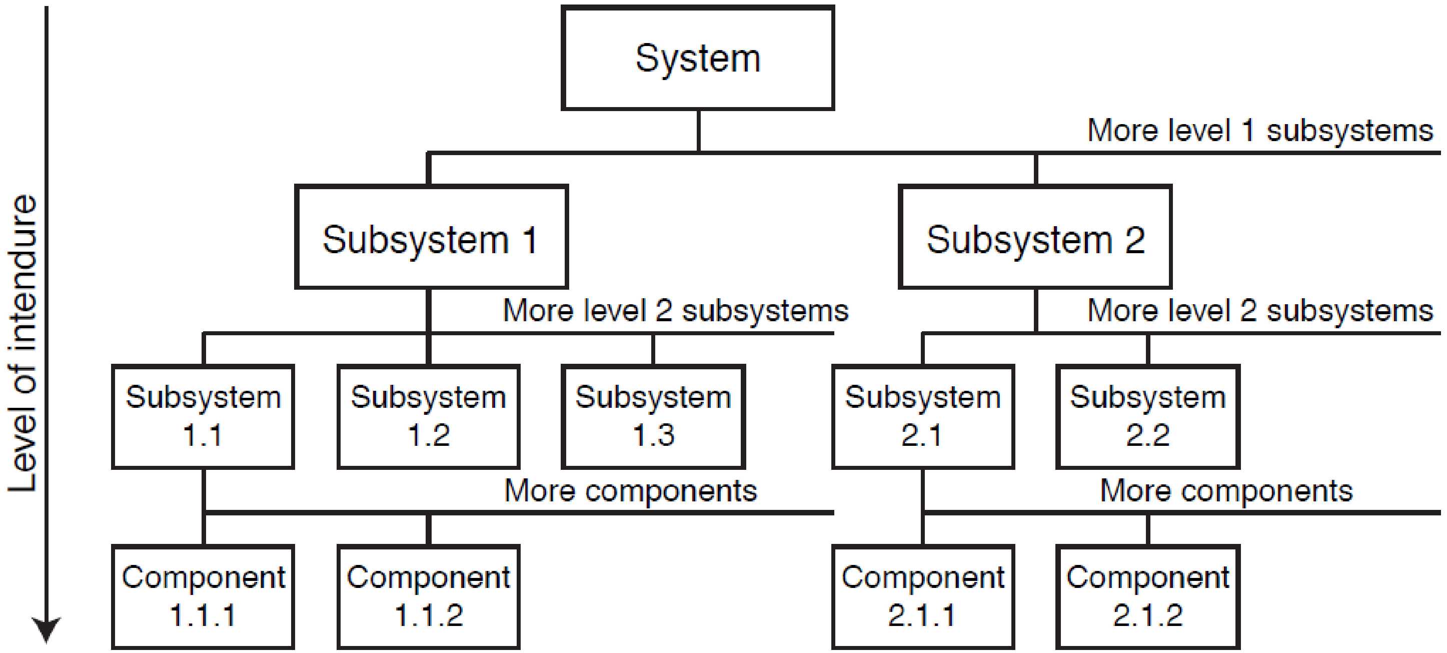
1. FMECA PREREQUISITES

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

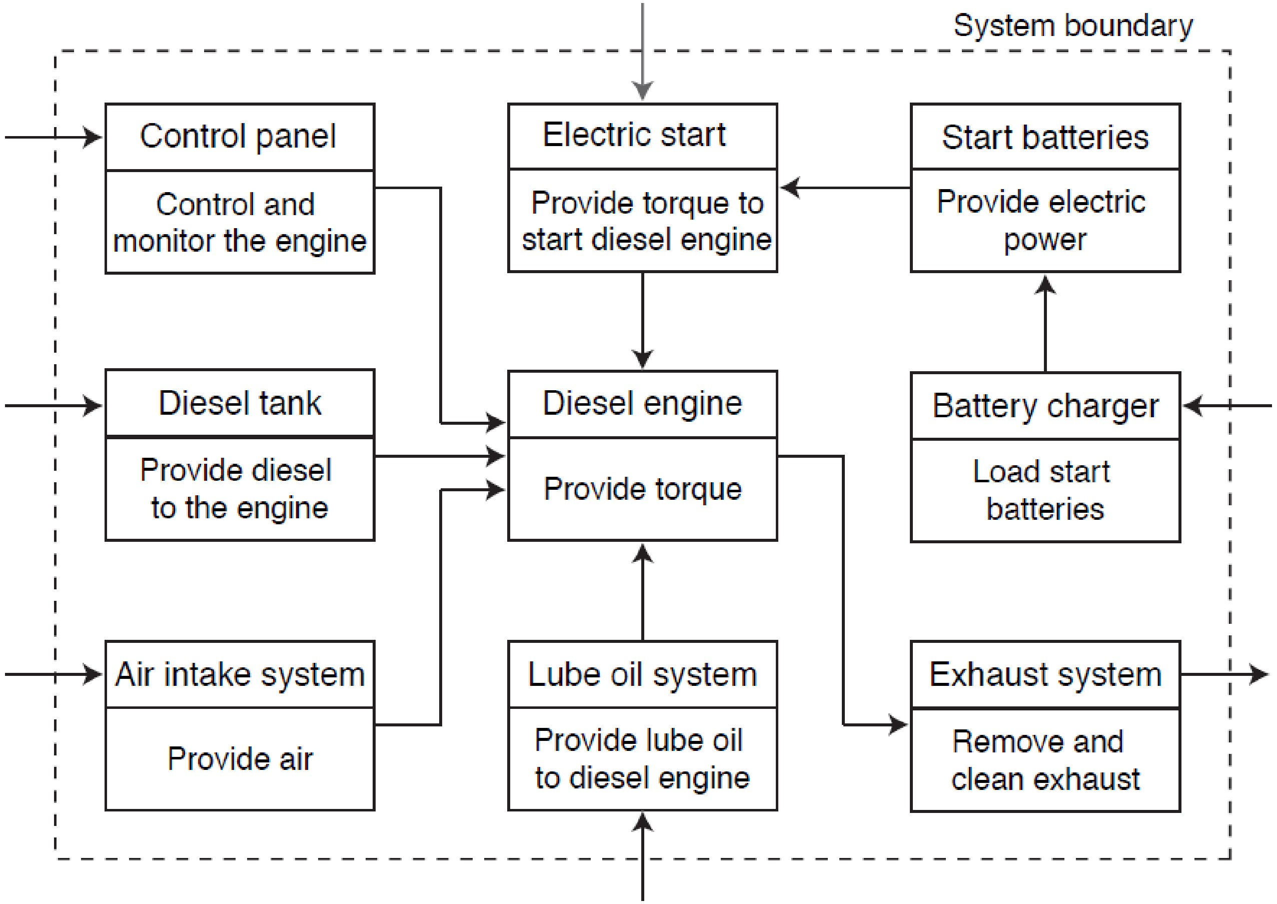
2A. SYSTEM STRUCTURE ANALYSIS

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:



2B. SYSTEM STRUCTURE ANALYSIS

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



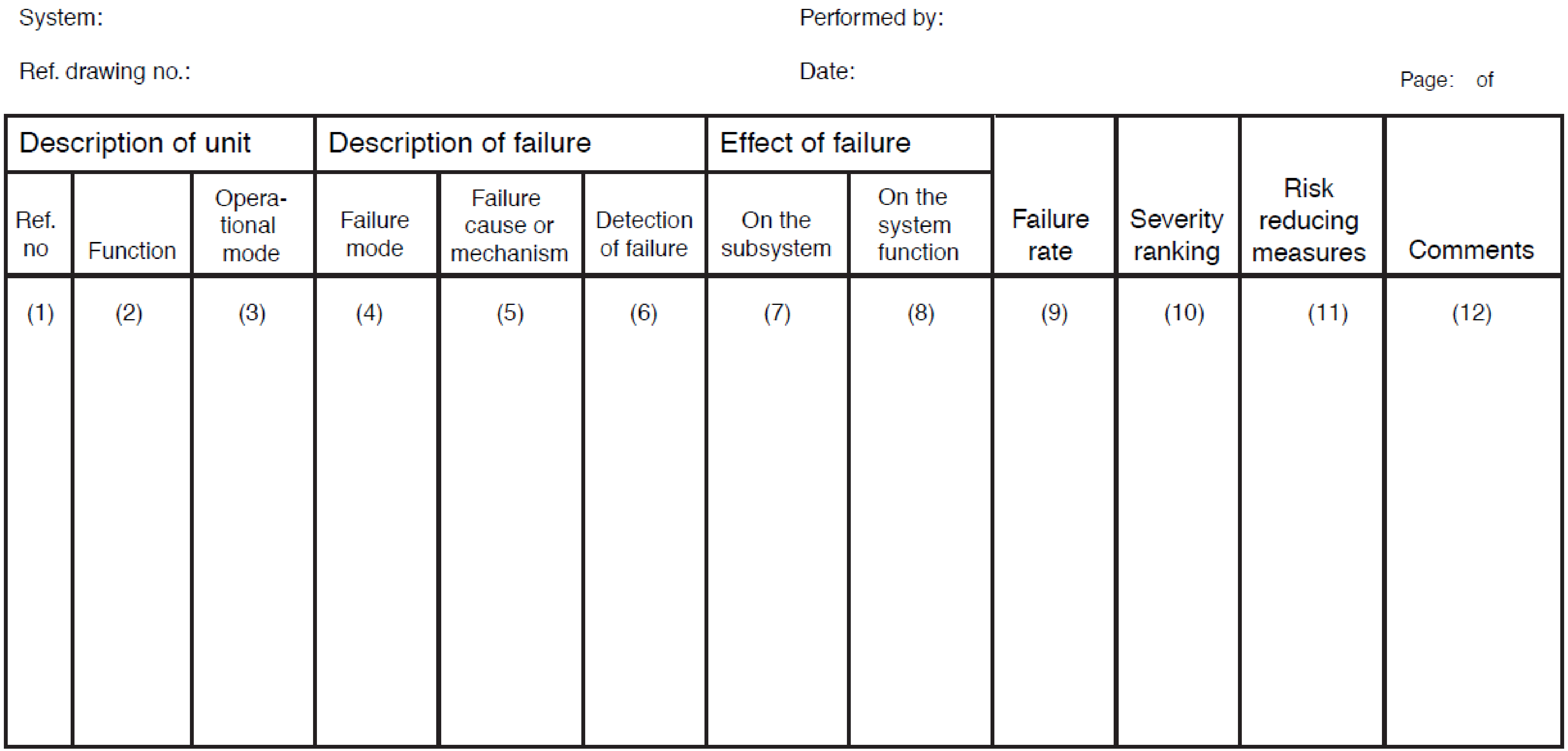
3. SYSTEM STRUCTURE ANALYSIS

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.

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	Opera-tional 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 now discuss the various columns in the FMECA worksheet.

- 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

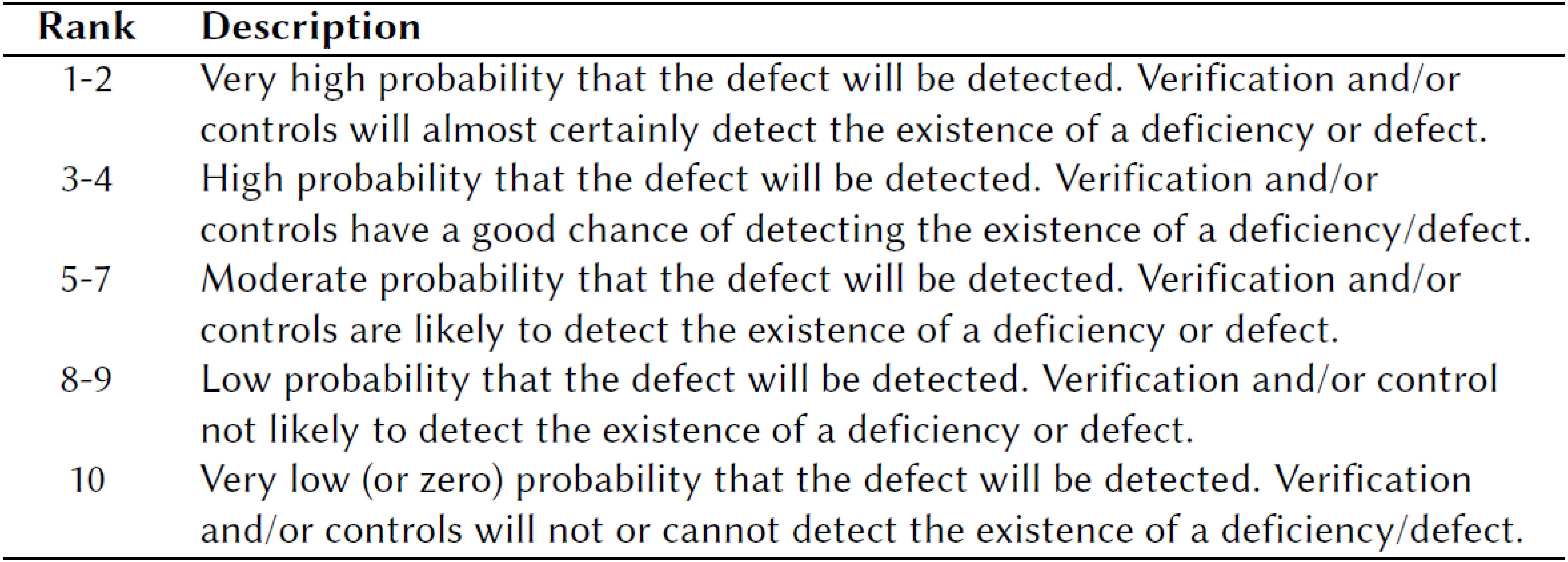
- 5. The failure modes identified in column 4 are studied one-by-one. The failure mechanisms (e.g., SEU, SET, TID) that may produce or contribute to a failure mode are identified and listed. Other possible causes of the failure mode should also be listed. If may be beneficial to use a checklist to secure 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.

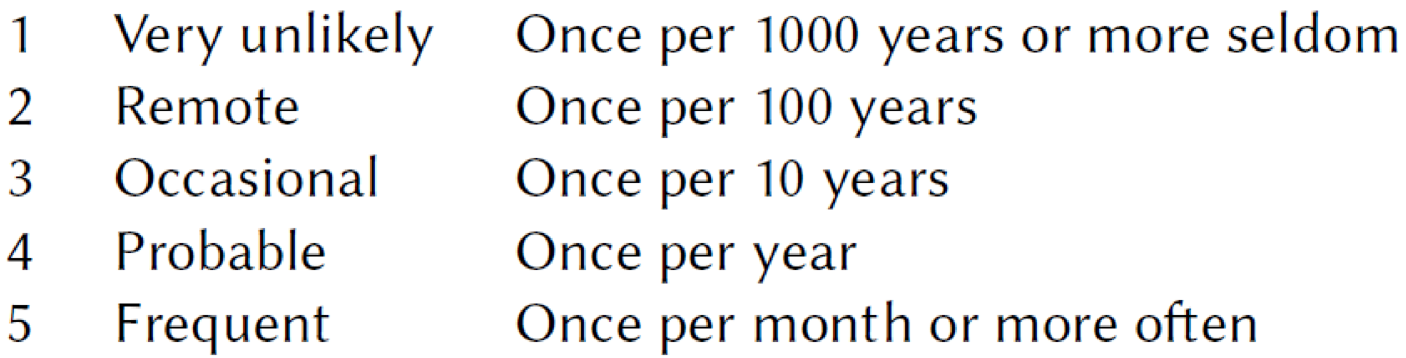
FMECA WORKSHEET – 8

- 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.

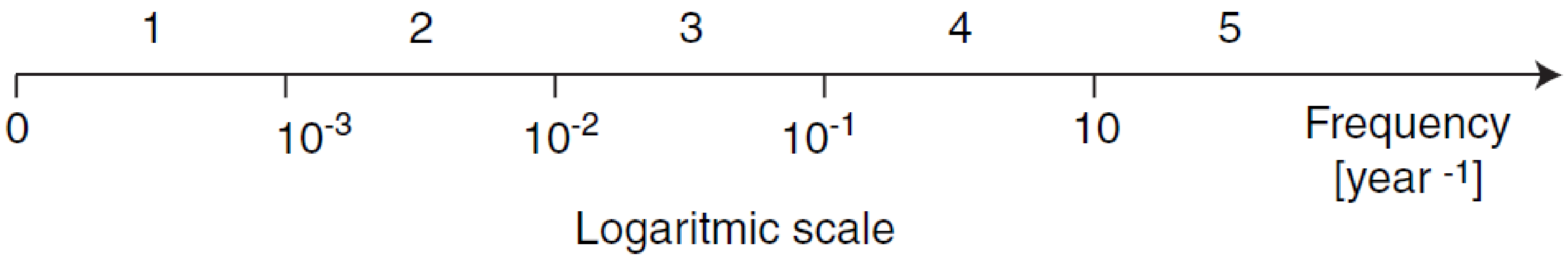
Additional columns: In some applications it may be beneficial to consider each category of effects separately, like: safety effects, environmental effects, production availability effects, economic effects, and so on.

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:



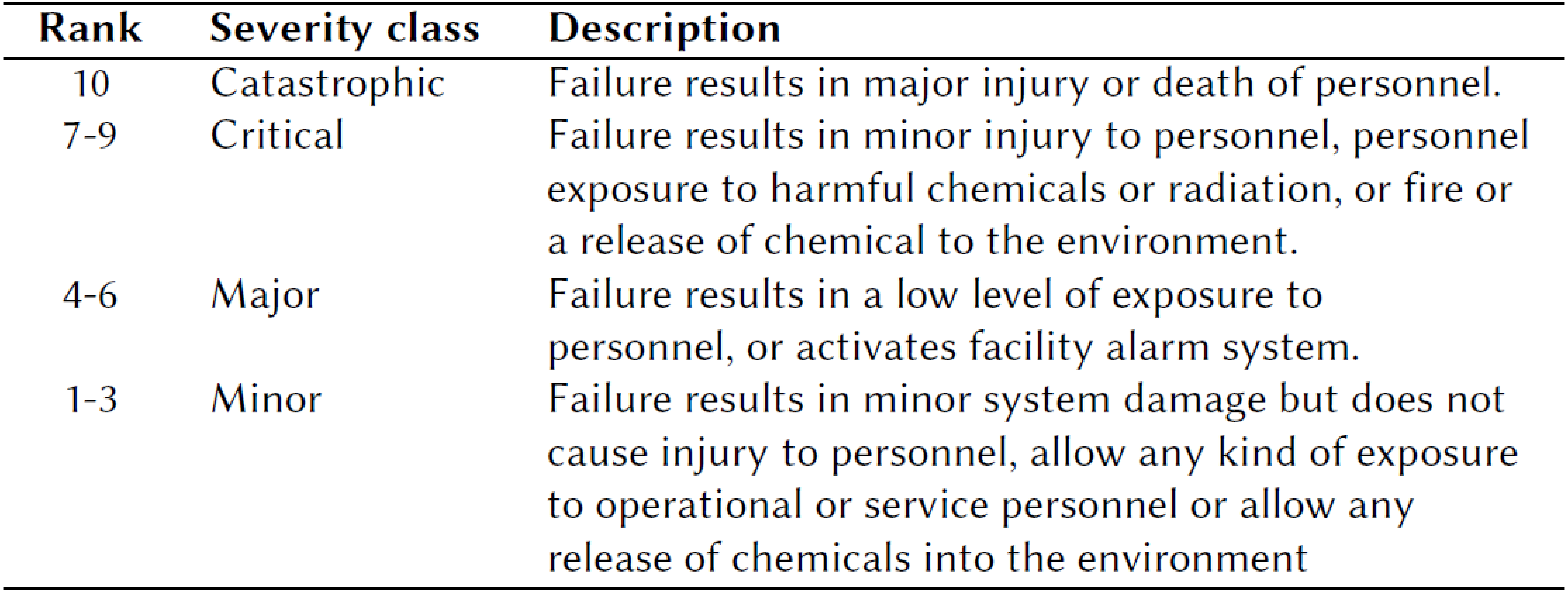
1	Very unlikely	Once per 1000 years or more seldom
2	Remote	Once per 100 years
3	Occasional	Once per 10 years
4	Probable	Once per year
5	Frequent	Once per month or more often



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

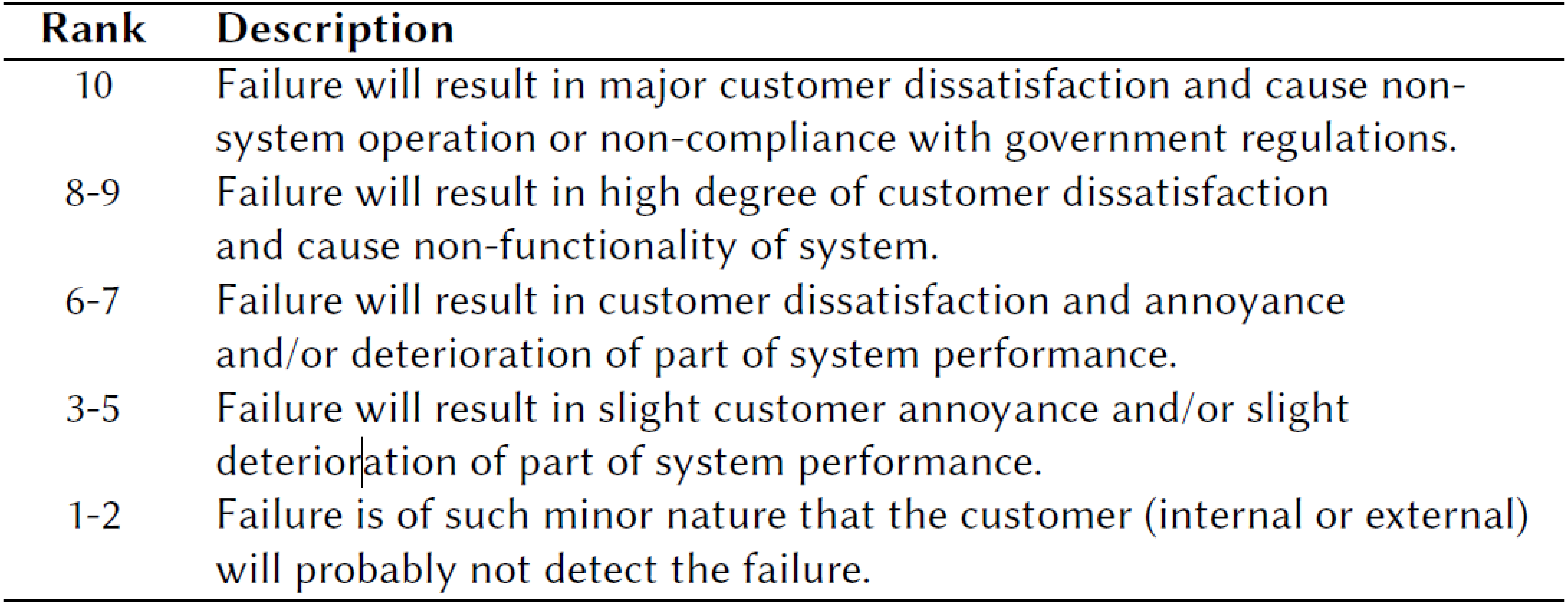
- 10. The severity of a failure mode is the worst potential (but realistic) effect of the failure considered on the system level (the global effects). The following severity classes for health and safety effects are sometimes adopted:



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.

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.
- 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

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

- RPN = S x O x D

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

BIBLIOGRAPHY

- Rausand, Marvin, and Arnljot Høyland. System Reliability Theory: Models, Statistical Methods, and Applications. Wiley, 2004.
- https://www.ntnu.edu/ross/books/sis/slides