POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE
E DELL'INFORMAZIONE

RAMS ENGINEERING, ADVANCEMENT OF SYSTEM SAFETY OF AVIONIC EQUIPMENT

TESI DI LAUREA MAGISTRALE IN
INGEGNERIA AERONAUTICA

Author: **Darren Scott FOSNIGHT**

Student ID: 962705
Advisor: Prof. Gianantonio MAGNANI
Co-advisor: Ing. Suelì ROJAS
Academic Year: 2021-22

Our greatest glory is not in never falling, but in rising every time we fall (Confucio)

Abstract

The purpose of this thesis is to show the importance and progress of RAMS engineering, denoted as the analysis of system safety, related, for this thesis, mainly on avionic equipment used on aircrafts and helicopters.

This thesis has been developed and conducted with Pariani SRL, a historical company based in Samarate that for over forty years has been designing and producing innovative products internally characterized by a strong integration between mechanics, hardware and software.

In the beginning, it will be given an overview of RAMS, its definition and highlight why it is so important for the safety of technical systems.

After describing the structure behind RAMS engineering, the standards which it is based on, and how it is implemented on technical system, a case study will be shown.

In the end, the future progress of RAMS will be shown and possible developments will be discussed.

Key-words: RAMS Engineering; Safety; Avionic equipment; Aircrafts; Technical system; Future progress.

Sommario

Lo scopo di questa tesi è di mostrare l’importanza e il progresso del ramo di ingegneria RAMS, denotata come l’analisi della sicurezza di un sistema, relativa, per questa tesi, principalmente alle apparecchiature avioniche utilizzate su aeromobili ed elicotteri.

Questa tesi è stata sviluppata e condotta con Pariani SRL, azienda storica con sede a Samarate che da oltre quarant’anni progetta e produce internamente prodotti innovativi caratterizzati da una forte integrazione tra meccanica, hardware e software.

All’inizio verrà fornita una panoramica dell’ingegneria RAMS, la sua definizione e si evidenzierà perché è così importante per la sicurezza dei sistemi tecnici.

Dopo aver descritto la struttura alla base dell’ingegneria RAMS, gli standard su cui si basa e come viene implementata nel sistema tecnico, verrà mostrato un caso di studio.

Infine, verrà mostrato il progresso futuro della RAMS e verranno discussi possibili sviluppi.

Parole chiave: Ingegneria RAMS; Sicurezza; Apparecchiature avioniche; Aeromobili; Sistema tecnico; Progressi futuri.

Nomenclature

AI	Artificial Intelligence
ALT	Accelerated Life Testing
AM	Additive Manufacturing
API	Application Programming Interfaces
ASA	Aircraft Safety Assessment
AR	Augmented Reality
CA	Criticality Analysis
CBPM	Condition Based Predictive Maintenance
CC	Cloud Computing
CCA	Common Cause Analysis
CD	Continuous Deployment
CI	Continuous Integration
CM	Corrective Maintenance
CMA	Common Mode Analysis
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
CMMS	Computerized Maintenance Management System
CMR	Certification Maintenance Requirements
COTS	Commercial Off the Shelf
CPS	Cyber Physical Systems
DOC	Document
DAL	Development Assurance Levels
DD	Dependence Diagram
DevOps	Development and Operations

DET	Dynamic Event Tree
DfM	Design for Maintainability
FC	Failure condition
FEM	Finite Element Method
FD	Fault Diagnosis
FH	Flight Hour
FHA	Functional Hazard Assessment
FIT	Failure in Time
FMECA	Failure Mode and Effect Criticality Analysis
FMES	Failure Mode Effects Summary
fpmh	Failures per million hours
FR	Failure Rate
FRACAS	Failure Reporting and Corrective Actions Systems
FT	Fault Tree
FTA	Fault Tree Analysis
GPRS	General Packet Radio Service
HA	Hazard Analysis
HEP	Human Error Probabilities
HMI	Human Machine Interface
ICT	Information and Communication Technologies
IDE	Integration Development Environment
IDPSA	Integrated Deterministic and Probabilistic Safety Assessment
IIOT	Industrial Internet of Things
IoS	Internet of Services
IoT	Internet of Things
IT	Information Technology

KLOC	Thousands of Lines Of Code
KPI	Key Performance Indicator
LRU	Line Replaceable Unit
MFE	Monitoring and Feature Extraction
ML	Machine Learning
MOOP	Multi-Objective Optimization Problem
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair/Restore
MTTF	Mean Time to Failure
O&M	Operations and Maintenance
OEE	Overall Equipment Effectiveness
OEMs	Original Equipment Manufacturers
OH	Operating Hours
P/N	Part Number
PCB	Printed Circuit Board
PDF	Probability Density Function
PFD	Probability of Failure on Demand
PLM	Product Lifecycle Management
PM	Preventive Maintenance
PMS	Performance Monitoring System
PRA	Particular Risk Analysis
PSA	Probabilistic safety assessment
PSSA	Preliminary System Safety Assessment
RAMS	Reliability, Availability, Maintainability and Safety
RAV	Replacement Asset Value
RBD	Reliability Block Diagram

REV	Revision
RFQ	Request For Quote
RIAC	Reliability Information Analysis Center
RPA	Reliability Prediction Analysis
RPR	Reliability Prediction Report
RTAD	Real Time Anomaly Detection
SaaS	Software as a Service
SFPS	Single Failure Points
SSA	System Safety Assessment
TCD	Technical Description
TCO	Total Cost of Ownership
TW	Time Window

Contents

1 Introduction

1.1. Scope and targets of the thesis

The main scope of this thesis is to show the state of the art of RAMS engineering analysis for avionic equipment and to discuss the most recent methods developed to improve the analysis and to ensure better and more precise results.

The motivation that led me to write this thesis concerns my current job role and the importance of understanding deeply the current methods to find out if they have any weaknesses and possible aspects that can be improved.

System safety is one of the key aspects that companies look at when they develop new products and finding ways to improve the analysis, to obtain more precise results, is one of their major concerning aspects.

This thesis has been organized in the following way.

It begins with an overview of RAMS engineering, regarding its definition, importance and state of the art in the aeronautical field.

The main part discusses in detail the current methods, to give an overview of how it works and it is implemented theoretically and practically.

Next, a case study is shown and analyzed, regarding a project in which I have been involved recently.

In the end, it is shown the obtained outcomes and the aspects that can be improved, discussing the most recent and innovative methods that can be implemented in the future to enhance RAMS engineering analysis.

1.2. RAMS Engineering

1.2.1. RAMS definition

RAMS stands for reliability, availability, maintainability and safety, important quality attributes of all technical systems. System safety is the systematic process of securing RAMS from a lifecycle perspective.

RAMS is a central element in many different application areas, ranging from manufacturing, transportation and process industries to nuclear and space industries.

Reliability denotes the ability of a product or system to perform a specific function and may be referred to as design reliability or operational reliability. For example, a product's design reliability is its ability to perform as intended after it leaves the factory. The operational reliability of the product denotes its ability to function in operation, throughout its life or for a specified period.

Availability denotes the ability of a system to be kept in a working state in a given environment. The availability of a system depends on the reliability of the system design, its maintainability and its maintenance support.

Maintainability is a design property of a product or system and is determined by the ease with which the product or system can be promptly repaired or maintained. It includes maintenance, inspection and control activities. The maintainability of a system depends, among other things, on the accessibility, standardization and modularization of the system.

Safety is also a property of the system. A system is said to have adequate safety if it does not cause harm to people, the environment or any other asset during its life cycle, during normal use and also through predictable misuse.

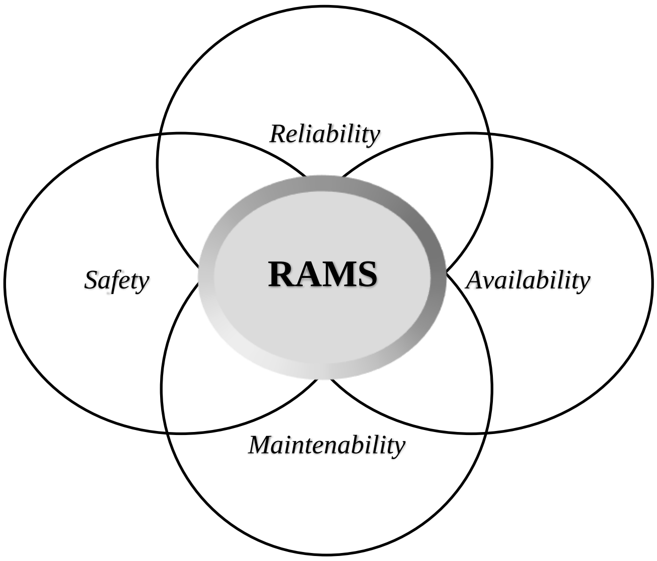


Figure 1. RAMS structure

1.2.2. RAMS importance

Engineering based on RAMS analysis is one of the technical methodologies that had the greatest interest and expansion in recent years.

Its use and implementation in the technical and quality departments allows the design and analysis of the reliability, availability, maintainability, safety and risk of complex installations, products or systems and where different technical areas converge: mechanics, electricity, chemistry, electronics, software, etc.

RAMS Engineering provides solutions, using analysis, prediction and demonstration to evaluate the system’s ability to perform as intended in the operational environment, and complete the defined mission. The interaction of software embedded systems with human constraints, environmental conditions, and the strict regulation requirements, challenge the performance and success of operation, and may result in catastrophic failures causing loss of human lives, and major financial damage. Products with low life cycle costs, high reliability, high availability and minimum required maintenance, are important contributors to the company’s reputation and competitive abilities, and the present predominant market demand. It is now unthinkable to carry out a complex project without RAMS analysis.

For more information, consult bibliography reference [1].

1.3. RAMS Analysis state of the art in the aeronautical field

For more information about this section, consult bibliography reference [2].

RAMS is a long-term operating characteristic of a system and is achieved through the application of data, concepts, methods, techniques and engineering tools throughout the lifecycle of the system. In the railway sector, the reference standard is EN 50126 [3], but it can be applied in any industrial sector: Aeronautics, Defense, Naval, Oil and Gas.

Many companies associate RAMS activities to a certification milestone in the aircraft's lifecycle. Indeed, RAMS engineering is largely used to design, validation, operations and maintenance activities for many actors in the supply chain, from OEMs to integrators, operators and maintainers. As we can see in the V-diagram below for the development of a technological product, RAMS assessments are developed throughout the whole lifecycle of technical products.

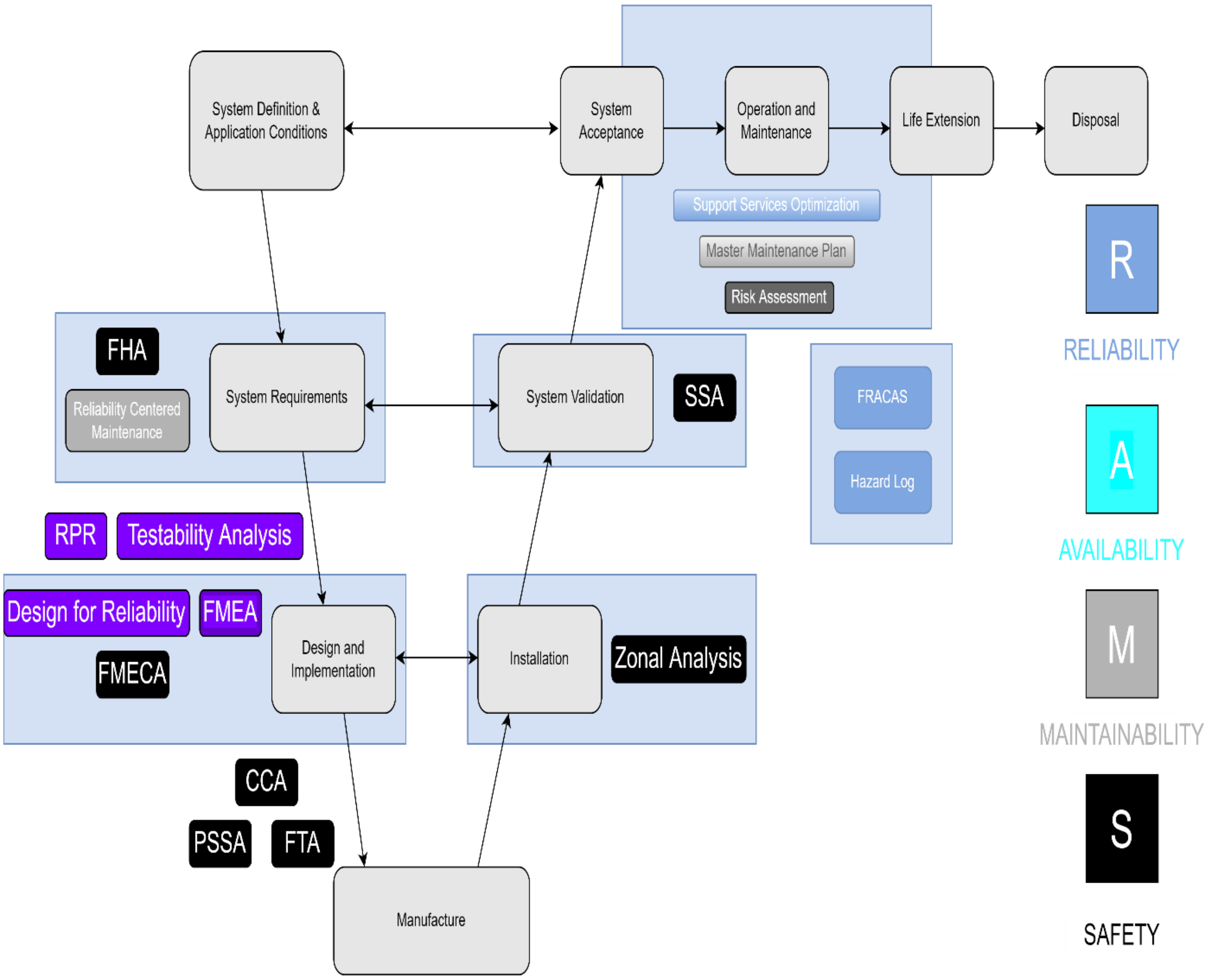
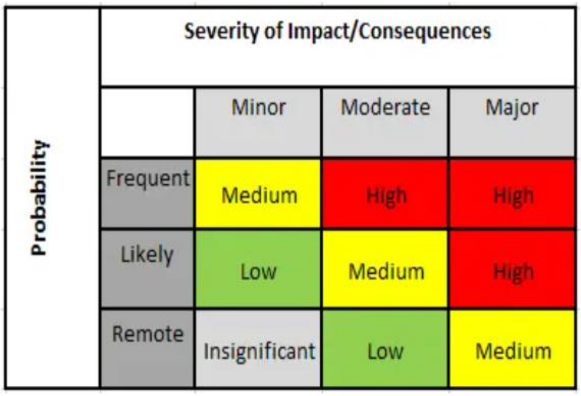


Figure 2. RAMS V-diagram

Take for example an aircraft integrator who intends to develop and bring to market a new type of aircraft. Early in the design phase, when product requirements are specified, the functions that the product should perform must be defined at both the integration and system levels.

The next step, after defining the system functions, is to perform a Functional Hazard Assessment (FHA). The FHA defines all the possible scenarios in which a hazard could have an effect on the safety of the aircraft. These scenarios are known as Failure Conditions and one of the RAMS engineer's job is to identify and classify them according to their severity. Each severity level will imply a specific safety objective for each fault condition.



Probability		Severity of Impact/Consequences		
		Minor	Moderate	Major
	Frequent	Medium	High	High
	Likely	Low	Medium	High
	Remote	Insignificant	Low	Medium

Figure 3. Risk matrix

While the preliminary aircraft architecture continues to develop and, possibly, a prototype is already under construction, several RAMS analyzes are performed to evaluate the compliance of the design with the safety objective derived from the FHA.

From the point of view of maintainability, once the preliminary architecture of the aircraft has been defined, the system engineer includes in the Aircraft Maintenance Manual those parts which are expected to require periodic maintenance. From there, the RAMS engineer performs a reliability-focused maintenance analysis, where maintenance tasks and intervals are defined for each item. This is only a preliminary list of maintenance actions, which is updated after the completion of the safety assessment and throughout the life of the aircraft, as new maintenance procedures may emerge.

On the reliability side, the Reliability Predictive Analysis (RPA) is one of the first analyzes to be performed, where the expected reliability of each component, assembly and system is calculated with the support of reliability prediction standards , historical reliability databases or , with reliability data extracted directly from the field. The latter, being the more desirable option, is usually unattainable due to inability to access OEM manufacturers data or simply because the items are being used for the first time. By performing an RPA, RAMS engineers can estimate the overall system reliability and make an initial estimate of the system's compliance with safety objectives and observe which elements need to be improved or replaced with more reliable parts. The results and conclusions of the analysis are reported in the Reliability Prediction Report (RPR).

One of the most known RAMS methodologies is the Failure Modes, Effects and Criticality Analysis (FMECA), performed for each system, where the failure modes of each component of the related system are identified. Each item can have multiple failure modes, each with specific causes and effects. The FMECA is used by RAMS engineers to link component failures to system failure conditions and more accurately estimate whether each failure condition will meet the safety objectives defined in the FHA. The link between the reliability prediction analysis and the FMECA is the failure rate of each component. While the RPA is used to estimate the failure rate of an item, the FMECA distributes this failure rate among the different failure modes of the item. In case the distribution is not known, the assumption of equally distributing the predicted failure rates is accepted.

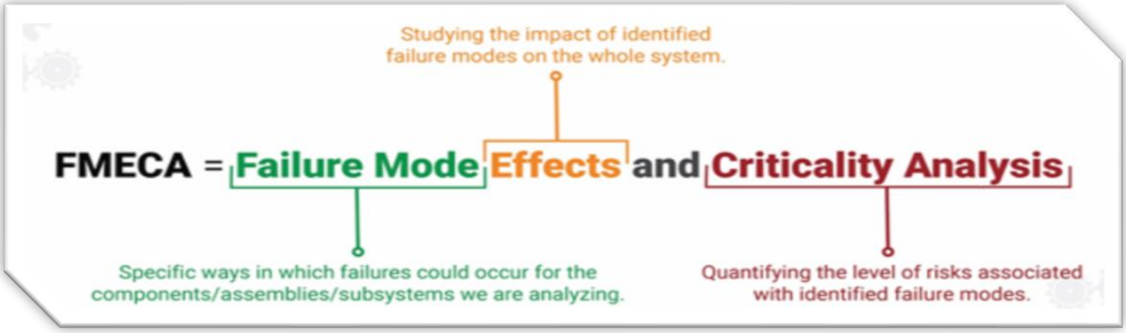

Studying the impact of identified failure modes on the whole system.
FMECA = Failure Mode Effects and Criticality Analysis
Specific ways in which failures could occur for the components/assemblies/subsystems we are analyzing.
Quantifying the level of risks associated with identified failure modes.

Figure 4. FMECA

Subsequently, a Fault Tree Analysis (FTA) will allow RAMS engineers to evaluate and determine the compliance of each fault condition with the safety objective. The FTA is usually performed only on those failure conditions that need to be quantitatively evaluated as the catastrophic, dangerous and possibly major failure conditions, using the output of the FMECA, from which the failure modes are identified for each item as failure events. basis which contribute to our top event which corresponds to our fail condition. In the Fault Tree Analysis the unavailability of each failure condition is calculated, a value strictly dependent on the average flight time. The longer our flight, the greater the unavailability, therefore the greater the difficulty of the system to meet the safety objective. In addition, Fault Tree Analysis is able to identify the single points of failure (SPoF) of the project, which are those failure modes that cause the failure of the entire system.

In the FTA, it is also important to carefully differentiate between obvious failures, dormant or latent failures, and hidden failures. Dormant faults are not detected when they occur and remain in this state until an inspection/revision is performed. In this context the aspect of maintainability occurs because if, for example, the planned time interval between two periodic inspections is too large, the probability increases that a dormant fault combines with another fault, thus leading to a system failure increase, and therefore the system may not comply with its safety objectives. If so, the RAMS engineer tries to find solutions that allow the system to become compliant and looks for the appropriate maintenance interval. These maintenance actions and time intervals are included as Certification Maintenance Requirements (CMR) in the aircraft maintenance manual.

Once the FTA is completed and before the first prototype aircraft is manufactured, a Zonal Safety Analysis, a Particular Risk Analysis (PRA) and a Common Mode Analysis (CMA) are developed. Common Cause Analysis (CCA) includes these three analyzes and is conducted to identify individual failure modes or external events that can lead to catastrophic or dangerous failure conditions.

In the Common Mode Analysis, RAMS engineer will verify that AND gates do not have faults which could cause simultaneous failures.

In the Particular Risk Analysis (PRA), the RAMS engineer identifies which external events may cause a system failure and affect the airworthiness of the aircraft. From this analysis derives a list of safety requirements.

In the Zonal Safety Analysis, the equipment installations in each zone of the aircraft will be checked for compliance with appropriate safety standards. Interference between systems is evaluated and design and installation guidelines are developed. Once the aircraft is manufactured, the ZSA is closed with an inspection of each zone to verify the implementation of corrective actions.

It is very important that reliability is monitored during the operational life of a technical system, as the theoretical values calculated during the design must be verified. Tracking reliability metrics allows manufacturing organizations to fully control the quality of suppliers and offer product customers integrated logistics support for spare parts and maintenance supplies. To track the reliability of each part, the most widely used tool is the FRACAS (Failure Reporting and Corrective Action Systems), which is able to derive important reliability metrics such as mean time between failures by collecting failure data from global operations. A consistent FRACAS system provides an in-depth overview of the reliability performance of fleets, products and individual subsystems and parts, while enabling a systematic approach for implementing corrective actions to improve aircraft reliability.

In the field of maintainability, the RAMS engineer can help operator organizations, such as fleet owners, airlines or charter flight companies, in building maintenance plan. A reorganization of all maintenance activities required for each aircraft into a structured Master Maintenance Plan can provide a global solution for fleets. The MMP includes the development of the process and tools for organizing and maintaining individual maintenance plans, as well as a structured process for introducing changes to the Scheduled Maintenance section of the Aircraft Maintenance Manual. The reorganization of the Maintenance Plan has effects of cost reduction, optimization of resources and manpower.

Safety engineers are needed at all levels of the operational life to monitor hazards. The Hazard Log is a tool required by all operators of aircraft fleets or equivalent technical systems. The Hazard Log is a collection of operational hazards and the corresponding Risk Assessment. Safety engineers study the risks of each operation, whether in service or maintenance, with the potential to cause harm to the staff health or damage to equipment. To bring the residual risk to an acceptable level, mitigations have to be applied as defined in the initial operational requirements.

2 RAMS structure and methods

2.1. Reliability

For more information about this section, consult bibliography reference [4].

2.1.1. Reliability Engineering

- ***Definition and objectives***

Reliability engineering concerns the ability of a system or component to function under stated conditions for a specified period of time without failure.

The reliability function is defined as the probability of success at time t, which is denoted as R(t) and estimated from detailed analysis, previous data sets or through reliability testing and reliability modelling.

It may be expressed mathematically as:

$$R(t) = \int_t^\infty f(x)dx \qquad (2.1)$$

In equation (2.1), $f(x)$ is the failure probability density function and t is the length of the period of time, which is assumed to start from time zero.

Reliability commonly related to failure-free operation. However, even if no single part of the system fails, but the system as a whole does not do what was expected, then it is still charged on the system reliability.

The system requirements specification is the criterion against which reliability is measured.

Reliability is limited to operation under stated or explicitly defined conditions. This constraint is necessary because it is impossible to design a system for unbounded conditions. The operating environment must be addressed during design and testing.

Reliability is often a major factor in system costs. It focuses on the costs of failures caused by system downtime, the cost of spare parts, repair equipment, personnel and the cost of warranty claims.

Reliability engineering deals with the prediction, prevention and management of lifecycle engineering uncertainty and failure risks. While stochastic parameters influence reliability, reliability is not achieved by mathematical and statistical models alone. The uncertainties involved largely influence quantitative methods for prediction and measurement.

Reliability engineering is closely related to quality engineering, safety engineering, and system safety because they use common methods for their analysis and may require input from each other.

The objectives of reliability engineering, in decreasing order of priority, are:

- To apply engineering knowledge and methods to prevent or to reduce the probability or frequency of failures.
- To identify and correct the causes of failures that do occur after trying to prevent them.
- To determine ways of facing failures that do occur, if their causes have not been corrected.
- To apply methods for estimating the reliability of new designs, and for analyzing reliability data.

Priority classification is used to achieve effective results in terms of cost minimization and generation of reliable products. It is important to understand and anticipate the possible causes of failures and to have the correct knowledge of how to prevent them.

➢ ***Reliability assessment basics***

The goal of reliability assessments is to provide qualitative and quantitative evidence that the use of a component or system will not be associated with unacceptable risk. The basic steps to take are:

- Fully identify relevant unreliability hazards, such as potential conditions, events, human errors, failure modes, interactions, failure mechanisms, and root causes, by specific analysis or testing.
- Evaluate the associated system risk, through specific analysis or tests.
- Propose mitigation measures, such as requirements, design changes, detection logic, maintenance, training, by which risks can be reduced and controlled to an acceptable level.
- Determine appropriate mitigation and agree acceptable levels of risk based on cost-benefit analysis.

Risk is the combination of likelihood and severity of the failure incident scenario occurring.

The severity of failures includes the cost of spare parts, man-hours, logistics, damage and machine downtime that can cause production losses. A failure can also lead to injury and death of people within the system. In this case, reliability engineering becomes system safety. Acceptable levels are determined by the authority, customers or interested parties. The risk that remains after all reliability activities have been completed is called residual risk and includes risk that is not identified and not fully quantifiable.

Improvements in the complexity of technical systems, such as design and material changes, scheduled inspections and backup redundancy, reduce risk and increase costs. The risk can be reduced to the lowest level reasonably achievable or practically achievable.

➢ ***Reliability program plan***

A reliability program is a complex structure based on learning and knowledge of system products and processes. It is sustained by team leadership, integrated into business processes and executed by proven standard working practices.

A reliability program plan is used to document exactly what activities, methods, tools, analysis and tests are required for a specific subsystem, as well as clarifying customer requirements for reliability assessment. Determining resource allocation and budgeting for testing and other activities are critical to a successful program. In general, the amount of work required for an effective program for complex systems is high. A reliability program plan is essential to achieving high levels of system reliability, testability, maintainability, and availability, and is developed early during system development and refined throughout the system lifecycle. It specifies the tasks of the reliability engineer and also the tasks performed by other interested parties. An effective reliability program plan must be approved by top program management, who is responsible for allocating sufficient resources for its implementation.

When reliability is not under control, more complicated issues can emerge, such as labor shortages, availability of spare parts, logistics delays, lack of repair facilities, and complex configuration management costs. The problem of unreliability can also be increased by the consequences of maintenance induced failures after repairs. Focusing only on maintainability is therefore not enough. Reliability must be evaluated and improved in relation to both availability and total cost of ownership (TCO) due to the cost of spare parts, man-hours for maintenance, transportation costs, storage costs and risks of obsolescence of the parts. But TCO also includes downstream costs when reliability calculations have not sufficiently or accurately addressed customers' personal risks, and a trade-off is often required in this case. The reliability plan should clearly provide a strategy for checking availability. The testability of a system should also be addressed in the plan, as this is the link between reliability and maintainability.

- ***Reliability requirements***

One of the first tasks of reliability engineering is to adequately specify reliability and maintainability requirements derived from overall availability needs and design failure analysis or preliminary prototype test results. Requirements must be clear to prevent designers from designing unreliable objects, constructions or interface systems. Reliability requirements apply to the system itself, including test and evaluation requirements and associated activities and documentation. Reliability requirements are included in system requirement specifications, test plans, and contractual statements. Creating appropriate lower-level requirements is critical. Providing only quantitative minimum targets such as mean time between failures (MTBF) values or failure rates is not sufficient for several reasons. One reason is that a full validation, related to correctness and verifiability in time, of a quantitative reliability allocation on lower levels for complex systems cannot be made as a consequence of the fact that the requirements are probabilistic for the extremely high level of uncertainties involved, and because reliability is a function of time, and accurate estimates of a probabilistic reliability number per item are available only very late in the project, sometimes even after many years of in-service use. Hence, quantitative reliability parameters, in terms of MTBF, are very uncertain design parameters.

Moreover, reliability design requirements should lead a system or part design to embody features that prevent failures or limit its consequences. A design requirement should be precise enough to ease the designer in the projecting phase and to help him proving, through analysis or testing, that the requirement has been achieved within some given confidence. Reliability requirements should be detailed and could be derived from failure analysis or testing, through systems risk assessment and mitigation logic. Hazard log systems must be created to collect detailed information on why and how systems could or have failed. Reliability engineers should also address requirements for various reliability tasks and documentation during system development, testing, production, and operation. These requirements are generally specified in the contract statement of work and depend on how much margin the customer provides to the contractor. Reliability tasks include various analyses, planning, and failure reporting. Failure reporting analysis and corrective action systems are a common approach for product and process reliability monitoring.

- ***Reliability design***

Reliability design begins with the development of a system model. To provide a graphical means of evaluating the relationships between different parts of the system, reliability models use block diagrams and Fault Tree Analysis.

A set of practical regulations is generally provided to designers so that they can project products that are protected against damage and excessive wear.

Redundancy is considered one of the most important design techniques. This means that if one part of the system fails, there is an alternate path that works as a backup system. The reason why redundancy is the most used choice is related to the fact that high level confidence reliability evidence for new parts or systems is often not available or is expensive to obtain. By combining redundancy, together with failure monitoring, and the avoidance of common cause failures, systems can be made highly reliable. In combination with redundancy, the use of different designs or manufacturing processes, through different suppliers of similar parts, can provide less sensitivity to quality issues, allowing high levels of reliability to be achieved through all the development cycle. Redundancy can also be applied in systems engineering by double checking requirements, data, designs, calculations, software, and tests to overcome systematic failures.

For electronic assemblies, a different approach, called physics of failure, is used. This technique is based on the analysis of the physical static and dynamic failure mechanisms. It accounts for variation in load, strength and stress that lead to failure with a high level of detail with the use of finite element method (FEM) software programs that can deal with complex geometries and failure mechanisms such as creep and fatigue. The component can be re-designed to reduce the probability of failure and to make it more robust against such variations. Derating is another common design technique which consists in selecting components whose specifications significantly exceed the expected stress levels.

- ***Human factors***

In practice, most failures can be traced back to some type of human error, for example in:

- Management decisions
- Requirement analysis and setting
- Configuration control
- Design
- Design drawings
- Assumptions
- Testing

- Calculations, simulations, FEM analysis
- Statistical analysis
- Manufacturing
- Quality control
- Maintenance
- Maintenance manuals
- Training
- Information classification
- Feedback of field information

However, policies that completely rule out human actions in design and production processes to improve reliability may not be effective because humans are also capable at detecting such failures, correcting them, and improvising when abnormal situations occur.

Moreover, human errors in management and the organization of data and information may also contribute to unreliability. This is the main reason why high levels of reliability for complex systems can only be achieved through a process with proper planning and execution of the validation and verification tasks. This also includes careful organization of data and information sharing and creating a reliability culture.

- ***Software reliability***

System reliability includes hardware, software, supporting infrastructure, operators and procedures. Generally, reliability engineering focuses on critical hardware parts of the system but nowadays, software has become an increasingly critical part of most electronics and nearly all systems due to the extensive use of digital integrated circuit technology.

However, there are huge differences in how software and hardware work. Most hardware unreliability is the result of a component failure that results in the system not performing its intended function. Repairing or replacing the hardware component restores the system to its original operating state. However, software does not fail in the same way that hardware fails. Instead, software unreliability is the result of unexpected results of software operations. Restoring software to its original state only works until the same combination of inputs and states results in the same unintended result.

Software reliability depends on clear requirements, design and implementation and depends strongly on a systematic process to anticipate and design against unintended consequences. A good software development plan is a key aspect of the software reliability program.

The software development plan describes the design and coding standards, configuration management, metrics and models to be used during development.

A common reliability metric is the number of software faults, usually expressed as faults per thousand lines of code, which, along with software execution time, is key to most software reliability models and estimates. The software reliability increases as the number of faults or fault density decreases. Because of the way software faults are distributed in the code, their severity, and the probability of the combination of inputs necessary to encounter the fault, establishing a direct connection between fault density and MTBF is difficult.

Testing is also very important, because even the best software development process results in some software faults that are nearly undetectable until tested. Software is tested at several levels through integration and system testing. During all phases of testing, software faults are discovered, corrected, and re-tested. Reliability estimates are updated based on the fault density and other metrics. At a system level, MTBF data can be collected and used to estimate reliability. Unlike hardware, performing exactly the same test on exactly the same software configuration does not provide increased statistical confidence. Instead, software reliability uses different metrics, such as code coverage.

2.1.2. Failure characteristics of embedded systems and Reliability parameters

- ***Failure characteristics***

Hardware failures

Hardware failures are typically characterized by a bathtub curve. An example curve is shown below. The chance of a hardware failure is high during the initial life of the module. The failure rate during the rated useful life of the product is low. Once the end of the life is reached, failure rate of modules increases again. Graph taken from bibliography reference [5].

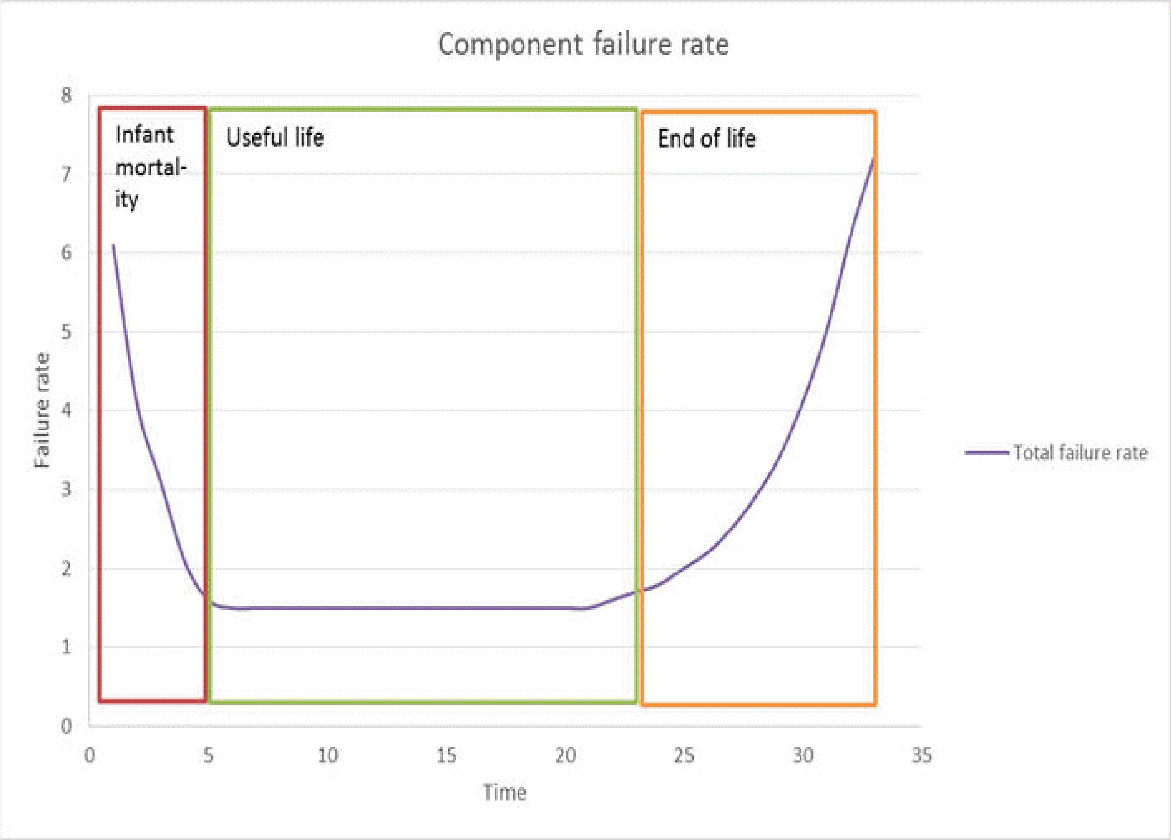


Figure 5. Component failure rate trend

Hardware failures during a products life can be attributed to the following causes:

- Design failures: this class of failures take place due to inherent design defects in the system. In a well-designed system this class of failures makes a very small contribution to the total number of failures.
- Infant Mortality: this class of failures cause newly manufactured hardware to fail. This type of failures can be attributed to manufacturing problems like poor soldering, leaking capacitor etc. These failures should not be present in systems leaving the factory as these faults will emerge in factory system burn in tests.
- Random Failures: random failures can occur during the entire life of a hardware module. These failures can lead to system failures. Redundancy is provided to recover from this class of failures.
- Wear Out: once a hardware module has reached the end of its useful life, degradation of component characteristics will cause hardware modules to fail. This type of faults can be eliminated by preventive maintenance.

The following graph shows the contribution of the different failure modes towards the overall failure rate. Graph taken from bibliography reference [5].

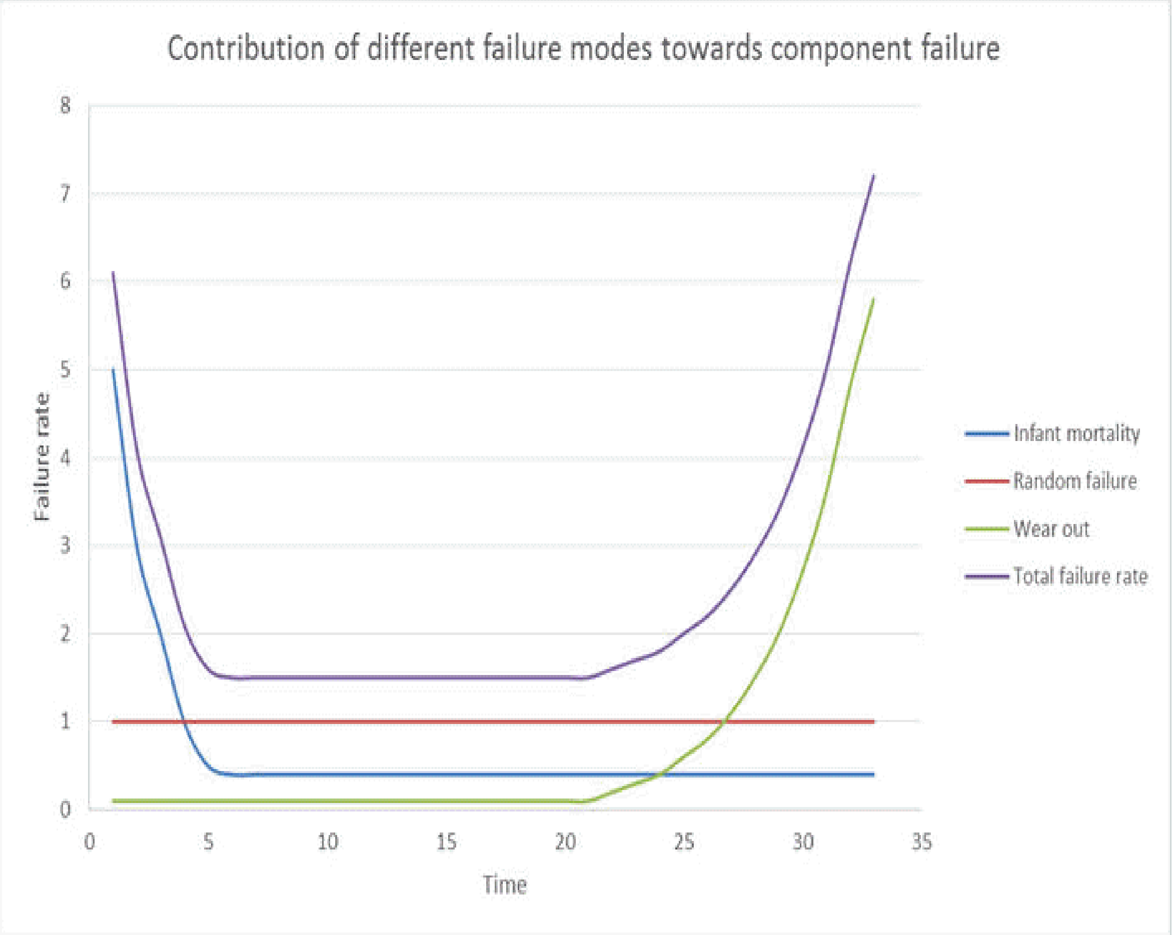


Figure 6. Failure modes contribution

Software failures

Software failures can be characterized by keeping track of software defect density in the system. This number can be obtained by keeping track of historical software defect history. Defect density will depend on the following factors:

- Software process used to develop the design and code
- Complexity of the software
- Size of the software
- Experience of the team developing the software
- Percentage of code reused from a previous stable project
- Rigor and depth of testing before product release

Defect density is typically measured in number of defects per thousand lines of code.

➢ ***Reliability parameters***

❖ *FAILURE RATE*

Failure rate is the frequency with which an engineered system or component fails, expressed in failures per unit of time. It is usually denoted by the Greek letter Lambda λ and is often used in reliability engineering.

The failure rate of a system usually depends on time, with the rate varying over the life cycle of the system.

In practice, the mean time between failures (MTBF = 1/λ) is often reported instead of the failure rate. This is valid and useful if the failure rate may be assumed constant, often used for complex units/systems, electronics, and is a general agreement in some Military and Aerospace reliability standards. It does in this case only relate to the flat region of the bathtub curve, which is also called the "useful life period". Because of this, it is incorrect to extrapolate MTBF to give an estimate of the service lifetime of a component, which will typically be much less than suggested by the MTBF due to the much higher failure rates in the "end-of-life wear out" part of the "bathtub curve".

The reason for the preferred use for MTBF numbers is that the use of large positive numbers is more intuitive and easier to remember than very small numbers.

❖ *MTBF*

Mean Time Between Failure (MTBF) is a reliability term used to provide the number of failures per million hours for a product. The MTBF is an important system parameter in systems where failure rate needs to be managed, in particular for safety systems. The MTBF appears frequently in the engineering design requirements, and governs frequency of required system maintenance and inspections. In special processes called renewal processes, where the time to recover from failure can be neglected and the likelihood of failure remains constant with respect to time, the failure rate is simply the multiplicative inverse of the MTBF.

Failure rates are important factors in the insurance, finance, commerce and regulatory industries and fundamental to the design of safe systems in a wide variety of applications.

MTBF is the most common inquiry about a product’s life span and is important in the decision-making process of the end user. MTBF is more important for industries and integrators than for consumers. Most consumers are price driven and will not take MTBF into consideration, neither is the data often readily available. On the other hand, when equipment such as media converters or switches must be installed into mission critical applications, MTBF becomes very important. In addition, MTBF may be an expected line item in an RFQ (Request For Quote). Without the proper data, a manufacturer’s piece of equipment would be immediately disqualified.

MTBF for hardware modules can be obtained from the vendor for off-the-shelf hardware modules. MTBF for in-house developed hardware modules is calculated by the hardware team developing the board.

MTBF for software can be determined by simply multiplying the defect rate for thousand lines of code executed per second.

❖ *MTTR*

Mean Time To Repair (MTTR) is the time needed to repair a failed hardware module. In an operational system, repair generally means replacing a failed hardware part. Thus, hardware MTTR could be viewed as mean time to replace a failed hardware module. Taking too long to repair a product drives up the cost of the installation in the long run, due to down time until the new part arrives, and the possible window of time required to schedule the installation. To avoid MTTR, many companies purchase spare products so that a replacement can be installed quickly. However, customers will usually ask about the turn-around time of repairing a product, and indirectly, that can fall into the MTTR category.

MTTR for a software module can be computed as the time taken to reboot after a software fault is detected.

❖ *MTTF*

Mean Time To Failure (MTTF) is a basic measure of reliability for non-repairable systems. It is the mean time expected until the first failure of a piece of equipment. MTTF is a statistical value and is meant to be the mean over a long period of time and a large number of units. Technically, MTBF should be used only in reference to a repairable item, while MTTF should be used for non-repairable items. However, MTBF is commonly used for both repairable and non-repairable items.

❖ *FIT*

Failure in time (FIT) is another way of reporting MTBF. FIT reports the number of expected failures per one billion hours of operation for a device. This term is used particularly by the semiconductor industry but is also used by component manufacturers. FIT can be quantified in several ways: 1000 devices for 1 million hours or 1 million devices for 1000 hours each, and other combinations. FIT and Confidence Limits (CL) are often provided together. In common usage, a claim to 95% confidence is normally taken as indicating virtual certainty.

2.1.3. Reliability for electronic equipment

Reliability is currently recognized as an essential need in electronic systems. It is looked upon as a mean for reducing costs from the factory, where rework of defective components adds a non-productive overhead expense, where repair costs include not only parts and labor but also transportation and storage. More importantly, reliability directly impacts force effectiveness, measured in terms of availability, and determines the size of the logistics inhibiting force utilization.

Reliability is based on the standard MIL-HDBK-217F [6], which purpose is to establish and maintain consistent and uniform methods for estimating the inherent reliability of electronic equipment and systems. It provides a common basis for reliability predictions during acquisition programs for military electronic systems and equipment. It also establishes a common basis for comparing and evaluating reliability predictions of related or competitive designs. The standards are intended to be used as a tool to increase the reliability of the equipment being designed.

The standards provide the models supporting a basic tool identified as reliability prediction and contains two methods of reliability prediction: “Part Stress Analysis” and “Parts Count”. These methods vary in degree of information needed to apply them.

The Part Stress Analysis Method requires greater amount of detailed information and is applicable during the later design phase when actual hardware and circuits are being designed.

The Parts Count Method requires less information, generally part quantities, quality level, and the application environment. This method is applicable during the early design phase and during proposal formulation. In general, the Parts Count Method will usually result in a more conservative estimate (i.e., higher failure rate) of system reliability than Parts Stress Method.

Every aspect of an electronic system, from the purity of materials used in its component devices to the operator’s interface, has an impact on reliability. Reliability engineering must, therefore, be applied throughout the system’s development diligently and be integrated with other engineering disciplines.

2.1.4. The Role of Reliability Prediction

Reliability prediction combines:

- creation of a proper reliability model
- estimation and justification of input parameters for this model
- estimation of output reliability parameters at system or part level

Reliability prediction provides the quantitative baseline needed to assess reliability analysis. A prediction made of a proposed design may be used in several ways. Reliability predictions for each design alternative provide one measure of relative value, which combined with other considerations, will aid in selecting the best of the available options. Once a design is selected, the reliability prediction may be used as a guide by showing the highest contributors to failure. If the part stress analysis method is used, it may also reveal other areas for change, as over stressed parts. The impact of proposed design changes on reliability can be determined only by comparing the reliability predictions of the existing and proposed designs. The ability of the design to maintain an acceptable reliability level under environmental extremes may be assessed through reliability predictions. The predictions may be used to evaluate the need for environmental control systems. The effects of complexity on the probability of mission success or the need for redundant, back-up systems may be determined with the aid of reliability predictions. A tradeoff of redundancy against other reliability enhancing techniques, as higher part quality, must be based on reliability predictions coupled with other pertinent considerations such as cost and space limitations. The prediction will also help evaluate the significance of reported failures. For example, if several failures of one type of component occur in a system, the predicted failure rate can be used to determine whether the number of failures is commensurate with the number of components used in the system, or, that it indicates a problem area.

Finally, reliability predictions results are also used to evaluate the probabilities of failure events described in a failure modes, effects and criticality analysis (FMECA).

2.1.5. Limitations of Reliability Predictions

Prediction of reliability from historic data can be very misleading, with comparisons only valid for identical designs, products, manufacturing processes, and maintenance with identical operating loads and usage environments. Even minor changes in any of these could have major effects on reliability. Furthermore, the most unreliable and important items are most likely to be modified and re-engineered since historical data was gathered, making the standard re-active or pro-active statistical methods and processes used, less effective.

For existing systems, any attempt by a responsible program to correct the root cause of discovered failures may render the initial MTBF estimate invalid, as new assumptions of the effect of this correction must be made. Another practical issue is the general unavailability of detailed failure data, with those available often featuring inconsistent filtering of failure feedback data, and ignoring statistical errors, which are very high for rare events like reliability related failures. Very clear guidelines must be present to count and compare failures related to different type of root-causes, such as manufacturing, maintenance, transport, system-induced or inherent design failures. Comparing different types of causes may lead to incorrect estimations and incorrect business decisions about the focus of improvement.

Standards provides a common basis for reliability predictions, based on analysis of the best available data at the time of issue. It is intended to make reliability prediction as good a tool as possible. However, like any tool, reliability prediction must be used intelligently, with due consideration or its limitations.

The first limitation is that the failure rate models are point estimates which are based on available data. Hence, they are valid for the conditions under which the data was obtained, and for the devices covered. Some extrapolation during model development is possible, but the inherently empirical nature of the models can be severely restrictive.

Even when used in similar environments, the differences between system applications can be significant. Predicted and achieved reliability have always been closer for ground electronic systems than for avionic systems, because the environmental stresses vary less from system to system on the ground and hence the field conditions are in general closer to the environment under which the data was collected for the prediction model. However, failure rates are also impacted by operational scenarios, operator characteristics, maintenance practices, measurement techniques and differences in definition of failure. Hence, a reliability prediction should never be assumed to represent the expected field reliability as measured by the user.

Electronic technology is known for its dynamic nature. New types of devices and new processes are continually introduced, compounding the difficulties of predicting reliability.

Another limitation of reliability predictions is the mechanics of the process. The part stress analysis method requires a significant amount of design detail. This naturally imposes a time and cost penalty. More significantly, many of the details are not available in the early design stages. For this reason, standards contain both the part stress analysis method and a simpler parts count method which can be used in early design and bid formulation stages.

Finally, a basic limitation of reliability prediction is its dependence on correct application by the user. Those who correctly apply the models and use the information in a conscientious reliability program will find the prediction a useful tool.

2.1.6. Part Stress Analysis Prediction

2.1.6.1. Applicability

This method is applicable when most of the design is completed and a detailed parts list including part stresses is available. It can also be used during later design phases for reliability trade-offs versus part selection and stresses. The standards contain failure rate models for a broad variety of parts used in electronic equipment. The parts are grouped by major categories and, where appropriate, are sub grouped within categories. The failure rates presented apply to equipment under normal operating conditions, i.e., with power on and performing its intended functions in its intended environment. Extrapolation of any of the base failure rate models beyond the tabulated values or extrapolation of any associated model modifiers is completely invalid. The general procedure for determining a system level failure rate is to sum individually calculated failure rates for each component. This summation is then added to a failure rate for the circuit board, which includes the effects of soldering parts. Finally, the effects of connecting circuit boards together are accounted by adding in a failure rate for each connector.

2.1.6.2. Part Quality

The quality of a part has a direct effect on the part failure rate and appears in the part models as a factor, π_Q. Many parts are covered by specifications that have several quality levels. Hence, the part models have values of π_Q that are keyed to these quality levels. Such parts with their quality designators are shown in table 1. The detailed requirements for these levels are clearly defined in the applicable specification.

Part	***Quality designators***
Microcircuits	S, B, B-1, Other: Quality judged by screening level
Discrete Semiconductors	JANTXV, JANTX, JAN
Capacitors, Established Reliability (ER)	D, C, S, R, B, P, M, L
Resistors, Established Reliability (ER)	S, R, P, M
Coils, Molded, Reliability (ER)	S, R, P, M
Relays, Established Reliability (ER)	R, P, M, L

Table 1. Parts with Multi-Level Quality Specifications

Some parts are covered by older specifications, usually referred to as Non-Established Reliability (Non-ER), that do not have multi-levels of quality. These part models generally have two quality levels designated as ‘MIL-SPEC.”, and “Lower”. If the part is procured in complete accordance with the applicable specification, the π_Q value for MIL-SPEC should be used. If any requirements are renounced, or if a commercial part is procured, the π_Q value for Lower should be used.

Poor equipment design, production, and testing facilities can degrade part quality. The use of the higher quality parts requires a total equipment design and quality control process commensurate with the high part quality. It would make little sense to procure high quality parts only to have the equipment production procedures damage the parts or introduce latent defects. Nevertheless, when a proposed equipment development is pushing the state of the art and has a high reliability requirement needing high quality parts, the total equipment program should be given careful scrutiny and not just the parts quality. Otherwise, the low failure rates as predicted by the models for high quality parts will not be realized.

2.1.6.3. Environment

All part reliability models include the effects of environmental stresses through the environmental factor, π_E. The description of these environments is shown in table 2. The π_E factor is quantified within each part failure rate model. These environments encompass the major areas of equipment use. Some equipment will experience more than one environment during its normal use, such as equipment in a spacecraft. In such a case, the reliability analysis should be segmented, namely, missile launch (M_L) conditions during boost into and return from orbit and space flight (S_F) while in orbit.

Environment	π_E	***Description***
Ground, Benign	G_B	Nonmobile, temperature and humidity-controlled environments readily accessible to maintenance; includes laboratory instruments and test equipment, medical electronic equipment, business and scientific computer complexes, and missiles and support equipment in ground silos.
Ground, Fixed	G_F	Moderately controlled environments such as installation in permanent racks with adequate cooling air and possible installation in unheated buildings; includes permanent installation of air traffic control radar and communications facilities.
Ground, Mobile	G_M	Equipment installed on wheeled or tracked vehicles and equipment manually transported; includes tactical missile ground support equipment, mobile communication equipment, tactical fire direction systems, handheld communications equipment, laser designations and range finders.
Naval, Sheltered	N_S	Includes sheltered or below deck conditions on surface ships and equipment installed in submarines.
Naval, Unsheltered	N_U	Unprotected surface shipborne equipment exposed to weather conditions and equipment immersed in salt water. Includes sonar equipment and equipment installed on hydrofoil vessels
Airborne, Inhabited, Cargo	A_{IC}	Typical conditions in cargo compartments which can be occupied by an aircrew. Environment extremes of pressure, temperature, shock and vibration are minimal. Examples include long mission aircraft such as the C130, C5, B52, and C141. This category also applies to inhabited areas in lower performance smaller aircraft such as the T38.

Airborne, Inhabited, Fighter	A_{IF}	Same as A_{IC} but installed on high performance aircraft such as fighters and interceptors. Examples include the F15, F16, F111, F/A 18 and A1O aircraft.
Airborne, Uninhabited, Cargo	A_{UC}	Environmentally uncontrolled areas which cannot be inhabited by an aircrew during flight. Environmental extremes of pressure, temperature and shock may be severe. Examples include uninhabited areas of long mission aircraft such as the C130, C5, B52 and C141. This category also applies to uninhabited area of lower performance smaller aircraft such as the T38.
Airborne, Uninhabited, Fighter	A_{UF}	Same as A_{UC} but installed on high performance aircraft such as fighters and interceptors. Examples include the F15, F16, F111 and A1O aircraft.
Airborne, Rotary Winged	A_{RW}	Equipment installed on helicopters. Applies to both internally and externally mounted equipment such as laser designators, fire control systems, and communications equipment.
Space, Flight	S_F	Earth orbital. Approaches benign ground conditions. Vehicle neither under powered flight nor in atmospheric reentry; includes satellites and shuttles.
Missile, Flight	M_F	Conditions related to powered flight of air breathing missiles, cruise missiles, and missiles in unpowered free flight.
Missile, Launch	M_L	Severe conditions related to missile launch (air, ground and sea), space vehicle boost into orbit, and vehicle re-entry and landing by parachute. Also applies to solid rocket motor propulsion powered flight, and torpedo and missile launch from submarines.
Cannon, Launch	C_L	Extremely severe conditions related to cannon launching of 155 mm and 5-inch guided projectiles. Conditions apply to the projectile from launch to target impact.

Table 2. Environmental Symbolism and Description

2.1.6.4. Thermal Aspects

The use of this prediction method requires the determination of the temperatures to which the parts are subjected. Since parts reliability is sensitive to temperature, the thermal analysis of any design should fairly accurately provide the ambient temperatures needed in using the part models. Of course, lower temperatures produce better reliability but also can produce increased penalties in terms of added loads on the environmental control system, unless achieved through improved thermal design of the equipment. The thermal analysis should be part of the design process and included in all the trade-off studies covering equipment performance, reliability, weight, volume, environmental control systems, etc.

2.1.6.5. Part Failure Rate Models

Part failure rate models for microelectronic parts are significantly different from those for other parts. A typical example of the type of model used for most other part types is the following one for a bipolar transistor:

$$\lambda_p = \lambda_b \pi_T \pi_A \pi_R \pi_S \pi_Q \pi_E \tag{2.2}$$

Where, in equation (2.2):

- λ_p is the part failure rate,
- λ_b is the base failure rate usually expressed by a model relating the influence of electrical and temperature stresses on the part,
- π_E and the other π factors modify the base failure rate for the category of environmental application and other parameters that affect the part reliability.

The π_E and π_Q factors are used in most all models and other π factors apply only to specific models. The applicability of π factors is identified in each section.

The base failure rate (λ_b) models and tables of calculated values are provided in the standards along with identification of the applicable model factors.

The model equations can, of course, be incorporated into computer programs for machine processing. The tabulated values of λ_b are cut off at the part ratings with regard to temperature and stress, hence, use of parts beyond these cut off points will overstress the part. The use of the λ_b models in a computer program should take the part rating limits into account. The λ_b equations are mathematically continuous beyond the part ratings but such failure rate values are invalid in the overstressed regions.

All the part models include failure data from both catastrophic and permanent drift failures and are based upon a constant failure rate.

2.1.6.6. Part Failure Rate Methods

The reliability prediction of the equipment is carried out in accordance with the method presented in the standard MIL-HDBK-217F [6], where each category of electronic components is assigned a model for the failure rate calculation. Furthermore, ANSI VITA 51.1 [7] standard is used to adjust the models, by taking into account the most recent developments in electronics.

The standard MIL-HDBK-217F [6] specifies that the basic failure rate of each component must be multiplied by several corrective factors, which depend, for example, on the operative conditions, on the type of working environment, on the quality of the manufacturing etc.

In the following tables are reported the models that are used for the failure rate calculation of the equipment and the list of coefficients with relative description. The failure rates are indicated with λ and the corrective factors with π.

Component	***Failure rate model***	***Notes***
Microcircuits	$\lambda_p = (C_1\pi_T + C_2\pi_E)\pi_Q\pi_L$	ANSI VITA 51.1 specifies that the manufacturers' failure rates may be used instead of a prediction based on the MIL standard, if provided. However, these must be corrected to take into account the differences in temperature and environment between the operative and testing conditions.
Diodes	$\lambda_p = \lambda_b\pi_T\pi_S\pi_C\pi_Q\pi_E$	/
Bipolar Transistors	$\lambda_p = \lambda_b\pi_T\pi_A\pi_R\pi_S\pi_Q\pi_E$	/
Transistors (Si FET)	$\lambda_p = \lambda_b\pi_T\pi_A\pi_Q\pi_E$	/
Optoelectronics (Emitters)	$\lambda_p = \lambda_b\pi_T\pi_Q\pi_E$	/
Resistors	$\lambda_p = \lambda_b\pi_T\pi_P\pi_S\pi_Q\pi_E$	/
Capacitors	$\lambda_p = \lambda_b\pi_T\pi_C\pi_V\pi_{SR}\pi_Q\pi_E$	/
Coils (Inductive Devices)	$\lambda_p = \lambda_b\pi_T\pi_Q\pi_E$	/
Switches	$\lambda_p = \lambda_b\pi_L\pi_C\pi_Q\pi_E$	/
Connectors (General)	$\lambda_p = \lambda_b\pi_T\pi_K\pi_Q\pi_E$	As specified in the standard, this failure rate model is valid for a mated pair of connectors; therefore, it is necessary to divide by two to obtain the failure rate for a single connector.
Connectors (Sockets)	$\lambda_p = \lambda_b\pi_P\pi_Q\pi_E$	/
Electronic Filters	$\lambda_p = \lambda_b\pi_Q\pi_E$	/

Table 3. Electric Component's failure rate models

Coefficient	***Description***
λ_p	Failure rate
λ_b	Basic failure rate
π_Q	Quality factor
π_E	Environment factor
π_T	Temperature factor
π_P	Active pins factor
π_K	Mating factor
π_L	Load stress factor
π_C *(For switches)*	Contact configuration factor
π_C *(For Capacitors)*	Capacitance factor
π_C *(For Diodes)*	Construction factor
π_V	Voltage stress factor
π_{SR}	Series resistance factor
π_P	Power dissipation factor
π_S	Stress factor
π_A	Application factor
π_R	Power rating factor
π_L	Learning factor
C_1	Die complexity failure rate
C_2	Package failure rate

Table 4. Coefficient’s description

2.1.7. Parts Count Reliability Prediction

This prediction method is applicable during bid proposal and early design phases when insufficient information is available to use the part stress analysis models shown before. The information needed to apply the method are:

1) generic part types (including complexity for microcircuits) and quantities
2) part quality levels
3) equipment environment.

The equipment failure rate is obtained by looking up a generic failure rate in standard's tables, multiplying it by a quality factor, and then summing it with failure rates obtained for other components in the equipment. The general mathematical expression for equipment failure rate with this method is given by equation (2.3):

$$\lambda_{EQUIP} = \sum_{i=1}^{n} N_i \left(\lambda_g \pi_Q\right)_i \tag{2.3}$$

for a given equipment environment where:

- λ_{EQUIP} = Total equipment failure rate (Failures/10^6 Hours)
- λ_g = Generic failure rate for the i^{th} generic part (Failures/10^6 Hours)
- π_Q = Quality factor for the i^{th} generic part
- N_i = Quantity of the i^{th} generic part
- n = Number of different generic part categories in the equipment

The equation (2.3) above applies if the entire equipment is being used in one environment. If the equipment comprises several units operating in different environments (such as avionics systems with units in airborne inhabited (A_I) and uninhabited (A_U) environments), then the equation should be applied to the portions of the equipment in each environment. These "environment-equipment" failure rates should be added to determine total equipment failure rate. The quality factors to be used with each part type are shown with the applicable λ_g tables and are not necessarily the same values that are used in the Part Stress Analysis. Microcircuits have an additional multiplying factor, π_L, which accounts for the maturity of the manufacturing process. For devices in production two years or more, no modification is needed. For those in production less than two years, λ_g should be multiplied by the appropriate π_L factor. It should be noted that no generic failure rates are shown for hybrid microcircuits. Each hybrid is a fairly unique device. Since none of these devices have been standardized, their complexity cannot be determined from their name or function. Identically or similarly named hybrids can have a wide range of complexity that contrasts categorization for purposes of this prediction method. If hybrids are anticipated for a design, their use and construction should be thoroughly investigated on an individual basis.

2.2. Availability

For more information about this section, consult bibliography reference [8].

Availability is the likelihood of an item performing satisfactorily at any given time when used under stated conditions in an ideal support environment and is generally defined as uptime divided by total time (uptime plus downtime).

Availability is also the proportion of planned operating time that is available for production and the time lost is downtime.

Downtime consists of planned and unplanned stops.

Unplanned shutdowns occur when machines are planned for production but unplanned events occur. Examples include equipment failure, unplanned maintenance, lack of operators or materials, etc.

Planned shutdowns happen when you schedule your equipment for production, but various planned events prevent that from happening. Examples include product changeovers, tool adjustments, cleaning, scheduled maintenance and quality inspection. Rest breaks and meetings also fall into this category.

Reliability block diagrams or fault tree analysis are developed to calculate the availability of a system. These methods can identify the most critical elements and failure modes or events that affect availability.

2.2.1. Availability representation

The simplest representation of availability (A) is a ratio of the expected value of the uptime of a system to the aggregate of the expected values of up and down time (that results in the "total amount of time" C of the observation window), as defined in the equation (2.4) below:

$$A = \frac{E[uptime]}{E[uptime]+E[downtime]} = \frac{E[uptime]}{C} \tag{2.4}$$

Another equation (2.5) for availability is the ratio between the Mean Time To Failure (MTTF) and the aggregate of the MTTF with the Mean Time To Repair (MTTR), that results in the Mean Time Between Failure (MTBF), as defined below:

$$A = \frac{MTTF}{MTTF+MTTR} = \frac{MTTF}{MTBF} \tag{2.5}$$

The average availability is the proportion of time during a mission or time period that the system is available for use. It represents the mean value of the instantaneous availability function over the period [0, c] and is given by equation (2.7):

$$A_c = \frac{1}{c}\int_0^c A(t)\,dt \qquad (2.6)$$

The steady state availability of the system is the limit of the availability function as time tends to infinity. Steady state availability is also called asymptotic availability. It is represented by equation (2.8):

$$A = \lim_{C\to\infty} A_c \qquad (2.7)$$

Limiting average availability is also defined on an interval [0,c] as in equation (2.9),

$$A_\infty = \lim_{c\to\infty} A_c = \lim_{c\to\infty}\frac{1}{c}\int_0^c A(t)dt, \quad c > 0 \qquad (2.8)$$

2.2.2. Definitions within systems engineering

Different classifications of availabilities can be used to present different conclusions about system's availability. The difference can be potentially large and availability measurements can be misused or misleading based on the usage made by the company and its customers. If a company uses a different classification from the one used by the customer, these two could have very different impressions of the system. Therefore, the choice of availability classification to use should be made carefully, taking into account the system and industry and how the company and its customers perceive availability. Hence, availability must be clearly defined in contracts. It is necessary to make sure that the company and its customers have the same understanding of availability and agree on the classification to use.

Three different types of availability are reported below.

- ***Inherent Availability, A_I***

Inherent availability is the steady state availability when considering only the corrective maintenance (CM) downtime of the system. This classification is sometimes referred to as the availability as seen by maintenance staff. This classification excludes preventive maintenance downtime, logistic delays, supply delays and administrative delays. Since these other causes of delay can be minimized or eliminated, an availability value that considers only the corrective downtime is the inherent property of the system. Many times, this is the type of availability that companies use to report the availability of their products because they see downtime other than actual repair time as out of their control and too unpredictable.

The corrective downtime reflects the efficiency and speed of the maintenance staff, as well as their expertise and training level. It also reflects characteristics that should be of importance to the engineers who design the system, such as the complexity of necessary repairs, ergonomics factors and whether ease of repair was adequately considered in the design.

For a single component, the inherent availability can be computed by equation (2.10):

$$A_I = \frac{MTTF}{MTTF+MTTR} \qquad (2.9)$$

It is slightly more complicated for a system. In this case, you have to consider the mean time between failures, or MTBF, and compute it as the following equation (2.11):

$$A_I = \frac{MTBF}{MTBF+MTTR} \qquad (2.10)$$

- MTBF = Uptime / Number of System Failures
- MTTR = CM Downtime / Number of System Failures

Until steady state is reached, the MTBF calculation may be a function of time. In such cases, before reaching steady state, the calculated MTBF changes as the system ages and more data are collected. Thus, the above formulation should be used cautiously.

- ***Achieved Availability, A_A***

Achieved availability is very similar to inherent availability with the exception that preventive maintenance (PM) downtimes are also included. Specifically, it is the steady state availability when considering corrective and preventive downtime of the system. The achieved availability is sometimes referred to as the availability seen by the maintenance department. It includes both corrective and preventive maintenance but does not include logistic delays, supply delays or administrative delays.

Achieved availability can be computed by looking at the mean time between maintenance actions, MTBM, and the mean maintenance downtime, $\overline{M}$, using the following equation (2.12):

$$A_A = \frac{MTBM}{MTBM+\overline{M}} \qquad (2.11)$$

- MTBM = Uptime / (Number of System Failures + Number of System Downing PMs)
- $\overline{M}$ = (CM Downtime + PM Downtime) / (Number of System Failures + Number of System Downing PMs)

System Downing PMs are PMs that cause the system to go down or require a shutdown of the system.

- ***Operational Availability, A_O***

Operational availability is a measure of the real average availability over a period of time and includes all experienced sources of downtime, such as administrative downtime, logistic downtime, etc. The operational availability is the availability that the customer actually experiences. It is essentially the availability based on actual events that happened to the system. The previously discussed availability classifications are a prior estimate based on models of the system failure and downtime distributions. In many cases, operational availability cannot be controlled by the manufacturer due to variation in location, resources and other factors.

Operational availability is the ratio of the system uptime to total time. Mathematically, it is given by the following equation (2.13):

$$A_O = \frac{Uptime}{Operating\ Cycle} \qquad (2.12)$$

where the operating cycle is the overall time period of operation being investigated and uptime is the total time the system was functioning during the operating cycle. The operational availability is a function of time, t, or operating cycle.

The concept of operational availability is closely related to the concept of operational readiness. In military applications, this means that the assigned numbers of operating and maintenance personnel, the supply chain for spare parts and training are adequate. In the case the manufacturer, for example, has a poor distribution and transportation system or does not stock the parts needed or provide enough service personnel to support the systems in the field, then, the readiness of this manufacturer to go to market with the product is low.

Logistic planners, design engineers and maintainability engineers can collaboratively estimate the repair needs of the system, required personnel, spares, maintenance tasks, repair procedures, support equipment and other resources. A realistic overview of the system's availability in actual operation can be made only when all downtime causes are addressed.

2.2.3. Availability in Series and in Parallel

System Availability is calculated by modeling the system as an interconnection of parts in series and parallel. The following rules are used to decide if components should be placed in series or parallel:

- If failure of a part leads to the combination becoming inoperable, the two parts are considered to be operating in series
- If failure of a part leads to the other part taking over the operations of the failed part, the two parts are considered to be operating in parallel.

➢ ***Availability in Series:***

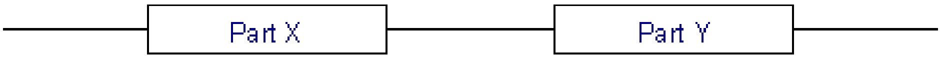


Figure 7. Availability in series

As stated above, two parts X and Y are considered to be operating in series if failure of either of the parts results in failure of the combination. The combined system is operational only if both Part X and Part Y are available. From this it follows that the combined availability is a product of the availability of the two parts. The combined availability is shown by the equation (2.14) below:

$$A = Ax * Ay \tag{2.13}$$

The implications of the above equation (2.14) are that the combined availability of two components in series is always lower than the availability of its individual components. Consider the system in the figure above. Part X and Y are connected in series. The table 5 below shows the availability and downtime for individual components and the series combination.

Component	***Availability***	***Downtime***
X	99%	3.65 days/year
Y	99.99%	52 minutes/year
X and Y combined in series	98.99%	3.69 days/year

Table 5. Availability in series outcome

➢ ***Availability in Parallel:***

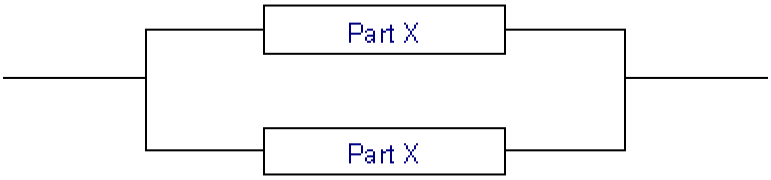


Figure 8. Availability in parallel

As stated above, two parts are considered to be operating in parallel if the combination is considered failed when both parts fail. The combined system is operational if either is available. The combined availability is shown by the equation (2.15) below:

$$A = 1 - (1 - A_x)^2 \qquad (2.14)$$

The implications of the above equation (2.15) are that the combined availability of two components in parallel is always much higher than the availability of its individual components. Consider the system in the figure above. Two instances of Part X are connected in parallel. The table 6 below shows the availability and downtime for individual components and the parallel combination.

Component	***Availability***	***Downtime***
X	99%	3.65 days/year
Two X components operating in parallel	99.99%	52 minutes/year

Table 6. Availability in parallel outcome

➢ ***Partial Operation Availability***

In systems where failure of a component leads to some users losing service, system availability has to be defined by considering the percentage of users affected by the failure.

Consider a system with N components where the system is considered to be available when at least N-M components are available and no more than M components can fail. The availability of such a system is denoted by $A_{N,M}$ and is calculated as in the equation (2.16) below:

$$A_{N,M} = \sum_{i=0}^{M} \frac{N!}{i! \times (N-i)!} \times A^{(N-i)} \times (1-A)^{i}$$

(2.15)

2.3. Maintainability

For more information about this section, consult bibliography reference [9].

Maintainability is one of the key concepts for equipment manufacturers, operators and asset managers. There are two types of maintainability analysis: preventive maintenance analysis and corrective maintenance analysis. The purpose of the preventive maintenance analysis is to examine all the maintenance actions that allow to prevent the occurrence of failures of the parts constituting the system, through the search and removal of incipient failures, or the scheduled replacement of components subject to wear whose useful life is reasonably known, or whose deterioration is particularly difficult to verify. The purpose of the corrective maintenance analysis is to examine the procedures and actions aimed at restoring the functionality of a device or part of it, identifying and replacing the faulty LRU (Line Replaceable Unit), exploiting the diagnostic indications as well as the accessibility and extractability of the equipment design.

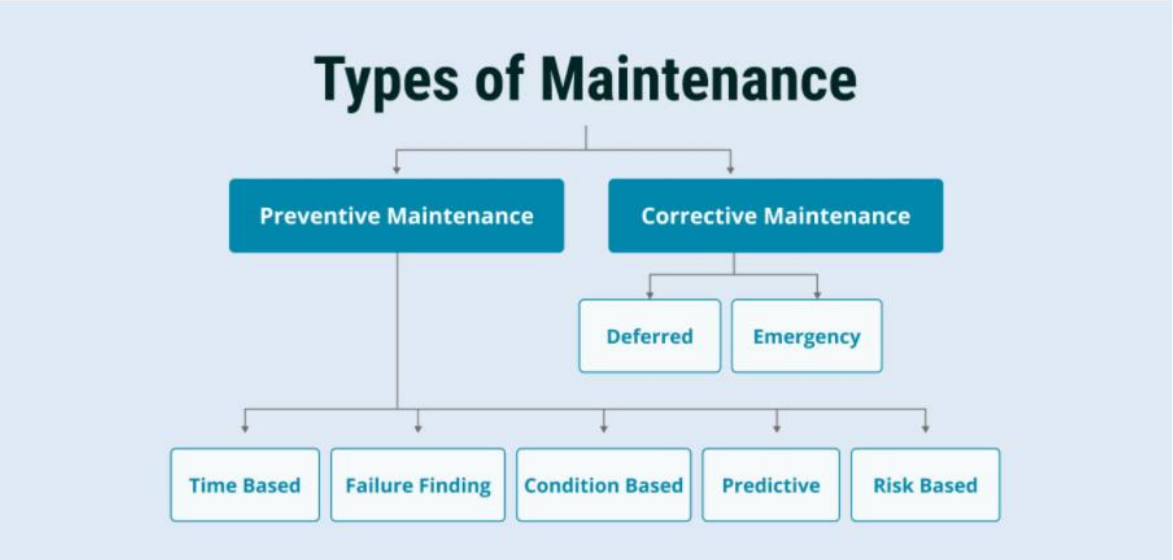


Figure 9. Types of Maintenance

The maintenance analysis provides indications in terms of human resources, time and materials, spare parts and equipment necessary for maintenance, through:

- Evaluation of the Mean Time To Repair (MTTR) or the average time required to perform the maintenance operation considered. The lower the MTTR, the higher the maintainability of the asset.
- Compilation of preventive and corrective maintenance schedules, which is a support for the drafting of a technical manual useful for maintenance technicians in which the operations necessary for maintenance are described in detail;
- Definition of the type and number of spare parts, which means drafting of a list of spare parts that must be present in the warehouse in order to minimize downtime necessary for component replacement.

The analysis of corrective and preventive maintenance times must be evaluated by providing the times of isolation, localization, accessibility, replacement of parts, reassembly of components and functional test according to the standard MIL-HDBK472 [10].

The goal of maintainability is to get equipment up and running as quickly as possible, with the lowest possible cost of maintenance. The easier it is to perform repairs and maintenance on an asset, the higher its maintainability.

The concepts of reliability, availability, and maintainability are closely related and together provide asset managers with the tools to evaluate the performance of any asset management program. Maintainability is considered inherent in the building system design, ensuring ease, accuracy, safety, and economy of maintenance activities within that system. The purpose of maintainability is to improve the effectiveness and efficiency of maintenance. One of the main desired products of this activity is the optimization of the life cycle costs of the building. Design for maintainability (DfM) is the first step of an effective maintenance program, linking maintenance objectives to the design process.

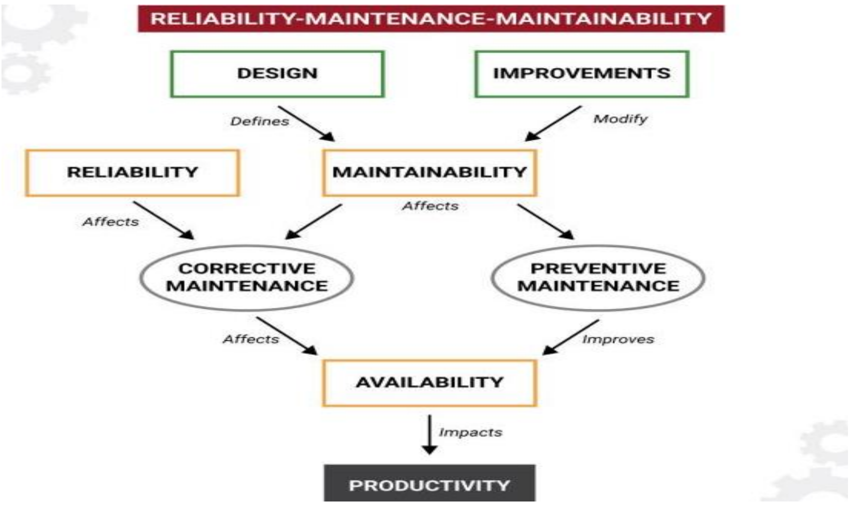


Figure 10. Reliability-Maintenance-Maintainability scheme

2.3.1. Track and measure maintainability

An important metric for measuring maintainability is the cost spent maintaining an asset. The cost of maintenance as a percentage of replacement asset value (RAV) is usually monitored to ensure that costs are within ranges obtained from the industry benchmark. Lower maintenance costs spent on an asset mean higher maintainability. It is evident that high maintainability is synonymous with low MTTR and low maintenance costs. To ensure that an asset has the desired levels of maintainability, a complete maintainability analysis is required for the equipment design phase. It involves considerations such as:

- using readily available materials and components
- utilizing standard fitting and bolting connections
- enabling fault identification
- ensuring the ease of assembly and disassembly

These considerations are discussed in detail in the next section.

2.3.2. Maintainability factors and cost associated

➢ ***Maintainability factors***

In engineering, maintainability is the ease with which a product can be maintained in order to:

- correct defects or their cause
- repair or replace faulty or worn-out components without having to replace still working parts
- prevent unexpected working conditions
- maximize a product’s useful life
- maximize efficiency, reliability, and safety
- meet new requirements
- make future maintenance easier, or cope with a changing environment

In some cases, maintainability involves a system of continuous improvement, learning from the past in order to improve the ability to maintain systems, or improve the reliability of systems based on maintenance experience.

To obtain satisfactory maintainability the following factors must be considered:

- The equipment or machine could fail at some time or other.
- The positioning of maintenance displays, check points, gauges, meters and the position of one assembly with respect to others.
- The limitations imposed by the human frame.
- The environment in which maintenance or repairs will be carried out.
- The design of test equipment.
- The presentation of information in the maintenance and repair manual.

➢ ***Costs associated with maintainability***

Maintainability is an important factor in the total cost of equipment. An increase in maintainability can lead to reduction in operation and support costs. For example, a more maintainable product lowers maintenance time and operating costs. Furthermore, more efficient maintenance means a faster return to operation or service, decreasing downtime.

There are many components of investment cost related to maintainability. These include, as shown in figure 11, the costs of prime equipment, system engineering management, repair parts, support equipment, data, training, system test and evaluation, and new operational facilities.

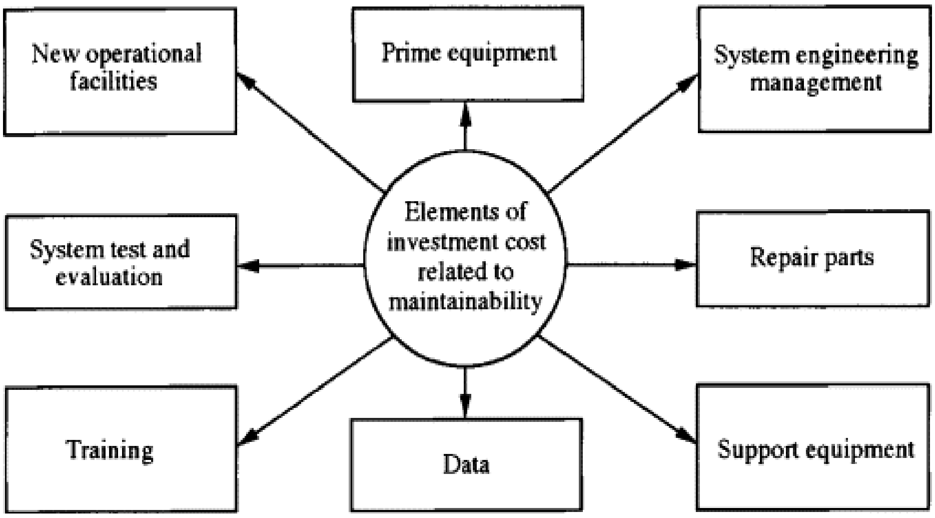

New operational facilities
Prime equipment
System engineering management
System test and evaluation
Elements of investment cost related to maintainability
Repair parts
Training
Data
Support equipment

Figure 11. Elements of investment cost related to maintainability

2.3.3. Design for maintainability

Most of several standards, best practices, and maintainability requirements that can be followed to ensure an asset is highly maintainable, can be mainly grouped under the following six categories:

- Standardization
- Modularization
- Interchangeability
- Malfunction annunciation
- Fault isolation
- Identification and tagging

Figure 12. Maintainability Design

- ***Standardization***

Instead of using multiple different types of parts and components, it is recommend minimizing the variety between parts in order to minimize inventory, equipment, and training requirements.

A common implementation of this rule is the use of standard connections in electronic devices.

The practice of standardization is commonly employed in the industrial space to minimize the types and sizes of bolts and fasteners within any asset assembly.

- ***Modularization***

Modularization refers to designing complicated machines from smaller blocks, modules, or subassemblies so that each block can be maintained independently of each other. This improves maintainability in the following ways:

- Facilitating easy disassembly and reassembly of machines, thus improving accessibility to the part requiring maintenance or replacement.
- It is often cheaper to replace the subassembly than to repair the damaged part. The damaged group can later be repaired and used as a spare. These practices significantly reduce the MTTR for any asset.
- System level upgrades are usually possible by upgrading one or more sub-assemblies rather than changing the entire equipment.

- ***Interchangeability***

The use of commonly available generic components instead of custom parts allows the user to use alternative spares from the market if the original spares are not available or have longer lead times. It is an easily achievable optimization of maintenance activities.

- ***Malfunction annunciation***

Whenever an asset fails to perform its intended function, this defective condition of the asset should be apparent to the operator in real time so that the required maintenance activity can be planned and undertaken before a catastrophic failure occurs.

Complicated machinery in heavy industries have elaborate monitoring systems installed on them. These systems include temperature sensors, pressure sensors, vibration monitors and other condition monitoring equipment used as part of predictive maintenance.

Any deviation from the set limits generates alarms for the operator who can then take the necessary measures and warn the personnel concerned. They can use this information to allocate necessary resources and to schedule maintenance work, usually through a computerized maintenance management system (CMMS).

- ***Fault isolation***

Whenever an asset fails or malfunctions, the first step is to diagnose the root cause of the problem. If the root cause is not obvious, the inspection and diagnosis of the defective component requires a lot of effort and therefore time and costs.

This waste of time and resources can easily be avoided by incorporating design features that limit the influence of human factors, make the problem apparent and consequently simplify the necessary corrective maintenance.

- ***Identification and tagging***

Assets, equipment, groups and sub-groups should be identifiable from one another to facilitate communication and record keeping. Resource operators achieve this by assigning unique and meaningful tags to resources and components.

Components within the equipment are assigned specific part numbers by the manufacturer so that questions regarding specific parts can be made without any confusion.

Asset management professionals use this elaborate identification system to improve maintainability in a variety of different ways.

Assigning unique part numbers ensures that the correct parts are set up for a service job avoiding unnecessary downtime. Equipment-specific history records and maintenance instructions can be made readily available using the equipment tagging system that helps maintenance personnel identify the right asset during field activities.

- ***Other ways for improving maintainability***

There are several small improvements that can be made to simplify maintenance work on complex assets:

- Purchasing easy-to-maintain goods is an important factor to consider during the procurement process.
- Provide quick access to preventive maintenance checklists, drawings, records and procedures. The easiest way to do this is to store them in a CMMS database.
- Maintenance workers and upper-level operators. The maintenance department should ensure adequate maintenance training, especially if new requirements are put in place.
- Standardize equipment and inventory. The organization should try to stick to the same types of equipment and tools whenever possible and appropriate to minimize the need for additional training and misuse.
- Standardize routine work. One way to reduce operating and maintenance costs is to increase employee productivity and reduce the number of human errors. In addition to training programs, standardizing operating procedures is the way to do this.
- Focus on proactive maintenance. More proactive maintenance leads to fewer major failures, requiring far more resources and expertise to resolve.

2.3.4. Maintainability prediction

Maintainability prediction is the estimate of the preventive and corrective maintenance workload associated with the proposed project. The quantification and monitoring of maintenance activities is a fundamental component to guarantee the reliability and achievement of the objectives of the quality system. This is the core capability of maintainability prediction, providing detailed analysis and measurement of the most vital maintenance actions. It is used to analyze a system to determine repair and maintenance measures, such as MTTR and other metrics. Maintainability prediction should be done immediately after defining the base system. This is the earliest time that sufficient data is available to perform a meaningful quantitative assessment of the performance and maintenance characteristics of the design. At this early stage in the system design process, maintainability predictions can still influence the design approach. As system design advances to the detailed level, more comprehensive design information becomes available and consequently the estimation of system maintainability characteristics becomes more accurate. The estimate should be updated continuously as the project progresses to provide the visibility needed to ensure that the specified requirements have a high probability of realization. The predictions are applicable to all programs and to all types of systems and equipment. However, they are especially pertinent in programs where risks are high or unknown and failure to meet maintainability requirements is highly undesirable.

Running maintainability predictions also allows you to focus on reviewing repair and maintenance procedures. By providing an organized and efficient approach to system maintainability analysis, you gain more insights and can work proactively for improvement.

➢ ***Benefits of performing maintainability predictions***

There are many benefits to performing maintainability prediction analysis. The main objective is to optimize repair and maintenance policies and procedures. It is difficult to achieve this without measurable statistics. It can be particularly difficult in the design phase of the product lifecycle to evaluate repair metrics when actual production has not yet begun. In this case, maintainability predictions are useful because they allow you to complete a product evaluation before production, while design changes that improve repair times have significantly less impact.

Maintainability Predictive analysis can also be performed once a system is up and running. By evaluating all corrective and preventive maintenance actions in the system, a predictive maintainability analysis can provide insight into the activities or components causing long system downtime. Unacceptable downtime could be caused by a variety of problems such as inadequate repair procedures, inability to properly isolate a fault, or inefficiencies that make it difficult to carry out the repair process. Maintainability forecasts can help evaluate all of these factors and provide insights to enable improvement.

Maintainability predictions can be used starting from early-stage design concept all the way through manufacturing and production. In fact, maintainability predictions are very useful when used throughout the entire product lifecycle and even in next generation product development. You can start your forecast with all the information you have, get a quick and early assessment, then refine your analysis as your project matures to get an increasingly accurate assessment. In this way, maintainability predictions become a key element in the continuous improvement process.

- ***Four elements of maintainability prediction***

There are four elements in performing a Maintainability Prediction analysis based on the standard MIL-HDBK-472 [10] methodology: Maintenance Tasks, Maintenance Task Groups, FD&I Outputs, and Maintainability Groups.

They can be considered the building blocks of predictive maintainability analysis. Once these are defined, it is possible to begin with the components of the system and describe the process and procedures required to repair and replace the failed elements.

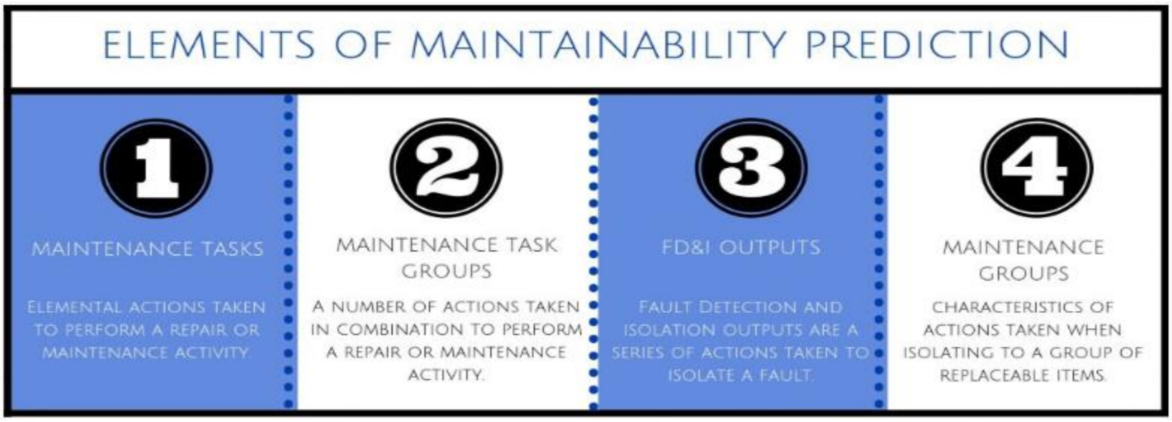

ELEMENTS OF MAINTAINABILITY PREDICTION
1
MAINTENANCE TASKS
ELEMENTAL ACTIONS TAKEN TO PERFORM A REPAIR OR MAINTENANCE ACTIVITY
2
MAINTENANCE TASK GROUPS
A NUMBER OF ACTIONS TAKEN IN COMBINATION TO PERFORM A REPAIR OR MAINTENANCE ACTIVITY.
3
FD&I OUTPUTS
FAULT DETECTION AND ISOLATION OUTPUTS ARE A SERIES OF ACTIONS TAKEN TO ISOLATE A FAULT.
4
MAINTENANCE GROUPS
CHARACTERISTICS OF ACTIONS TAKEN WHEN ISOLATING TO A GROUP OF REPLACEABLE ITEMS.

Figure 13. Four elements of Maintainability Prediction

- ***Maintenance Tasks and Maintenance Task Groups***

Maintenance actions are defined by a list of basic Maintenance Tasks that define the procedure for repair or maintenance action. Along with these task, it is assigned the time it takes to perform them. A library of basic tasks can be built up and then reuse them within your analysis.

Also, you can define a task group or run multiple tasks together to complete a repair action. All those Maintenance Tasks can be combined into a single Maintenance Task Group to use in the analysis for quick and consistent measurement.

- ***FD&I Outputs***

FD&I Outputs, or Fault Detection and Isolation Outputs, are the activities performed to detect and isolate a failed item. Similar to Maintenance Task Groups, FD&I Outputs are typically defined as a group of tasks performed together as a unit.

- ***Maintenance Groups***

Maintenance groups define how a repair action is performed on a group of items, rather than on an individual item. Some of the data required to define a maintenance group includes access to the repairable item, replacement methodology, and whether unit reassembly is required for checkout.

2.3.5. Maintainability management

Maintainability management is commonly conducted in accordance with custom program standards. The objective of maintainability program management is to integrate maintainability requirements with system requirements and equipment design, thereby ensuring that the system and equipment are easily maintainable at designated maintenance levels at the lowest system life-cycle cost (LCC) possible. Maintainability program management is designed to provide the required maintainability activities throughout the system lifecycle to ensure that the desired maintainability characteristics are achieved and maintained.

An effective maintainability program emphasizes the integration of maintainability attributes into the system and its components. The integration management procedure must ensure that there is a concurrent development condition between maintainability, design, system safety, reliability, LCC, manufacturing engineering and logistics engineering personnel during the program effort to achieve maximum information exchange common to all parts.

Maintenance planning provides the necessary integration input to the logistics engineering function to identify the support requirements and resources for individual end items, subsystems, assemblies and components. These requirements are then summarized in maintenance plans for the entire system and outline maintenance functions, flows, responsibilities and actions. Initial maintenance plans identify system-level service requirements, equipment repairs, and planned maintenance levels. The resulting plans describe the functional system design in sufficient detail to identify the configuration, construction, interfaces, and repairable characteristics. Maintenance plans can be developed for a variety of operations, including test support, contractor support, logistics support for contractors, warehouse, organization, and automatic and intermediate test equipment.

The initial iteration of the Maintenance Analysis task provides the management framework for detailed analysis of the tasks within the logistics support analysis task. Subsequent iterations will identify maintenance actions on removed serviceable assemblies and define appropriate levels of repair related to specific program requirements.

The maintainability program plan, if required, will identify the management activities necessary for the integration of maintainability features into the system design, otherwise the system engineering management plan, the system effectiveness program plan or the Logistics Support Plan may contain this information.

Examples of nine common maintainability tasks are summarized below.

- ***<u>Task 1, Maintainability Analysis</u>***

The maintainability analysis includes all maintainability activities addressed in the program plan. Translates overall system support and operational requirements into detailed quantitative and qualitative maintainability requirements and evaluates how many established maintainability requirements have been met. It is an iterative process that begins with preliminary concepts, progresses through the development of a preferred maintainability model for Preliminary Design Review (PDR), and culminates in a detailed design with well-defined quantitative and qualitative maintenance support requirements to the lowest level repairable item.

- ***Task 2, Document Maintainability Requirements and Criteria***

Maintainability engineers provide input to designers to identify and integrate specified maintainability requirements. The design criteria constitute specific maintainability goals, such as modularization, standardization, accessibility, interchangeability, guidance to repair versus disposal, quantity and placement of test points, and degree of self-test capabilities. These criteria are expressed qualitatively or quantitatively and are used as guidelines by the design engineer. A maintainability project checklist can be provided to designers and used by maintainability engineers to record their assessments of maintainability characteristics within the project.

Allocations and predictions are made using one or more of the maintainability parameters. These metrics are commonly measured in hours, but the time range can be selected based on the system's time scale. It is important to clearly understand with the customer which parameter they want to use as a basis for maintainability requirements.

These and other parameters can be included in a maintainability model that allows for the manipulation of maintainability data into analyzes useful for solving maintainability problems by adjusting the values and consuming maintainability margins in alternative ways.

The maintainability engineer should develop and maintain a maintainability requirements model that can also produce a content-driven report from the customer's data needs expressed in a description of the data item. Typically, detailed corrective maintenance data and a summary of mean time to repair (MTTR) should be reported in addition to preventive or turnaround maintenance data.

There are many ways to measure maintainability and many ways to count time in maintenance events, so corrective maintenance times must be defined very carefully and agreed with the customer. These times may include removal and replacement time for Online Replaceable Units only, or they may include access times, checkout times, and logistics delays. The maintainability engineer should keep a tabular list of corrective maintenance times allocated for each item accepted into the maintainability plan, if possible, in a computer database model.

- ***Task 3, Maintainability Quantitative Analysis to Assure Requirements Are Met***

Maintainability allocations are allocated in a top-down trend from higher-level quantitative maintainability data to provide a quantitative goal that the designer must meet and allow cost-effective alternatives to be evaluated in integrating maintainability and other requirements into the system, subsystem, and component concepts and designs.

As the project matures so that it is possible to imagine the maintenance actions that need to be performed, the maintainability engineer adds the predicted failure rate and maintenance time columns to the data table and calculates the predicted MTTR. If the system-wide MTTR is within the required value, all is fine. If not, you need to identify the elements contributing to the excess maintenance time and discuss with the designer how to reduce the time.

Later, when actual failure rate and maintenance time data becomes available from reliability and maintainability testing, production or user testing, the engineer can develop the achieved MTTR data.

The planned maintenance time of the system or end item is calculated from the detailed planned maintenance activities by combining them in accordance with the process flow diagram and time sequence diagram. In a deterministic environment, estimated times are simply added where they run serially, and critical path times are added where parallel tasks are involved. In a probabilistic environment, mean and variation numbers are required and are fed into a model to determine aggregated values. In both the deterministic and probabilistic approaches, margins should be used to provide risk management opportunities.

As the design concept matures, maintainability engineers study the evolving design and make forecasts of scheduled maintenance in the context of the planned maintenance concept. Where forecasts suggest a failure to meet assigned values, the maintainability engineer must first determine which area of the project offers the best avenue for mitigation.

There may be several alternatives that may need to be studied in a commercial format. The maintenance engineer then works with the selected item's principal engineer to reduce scheduled maintenance time. As a last option, maintainability figures can be reallocated and maintainability margins attached or margin values swapped to other parts of the architecture.

- ***Task 4, Design Surveillance/Assessment***

Maintainability design inputs are formally passed on to designers via conversation, maintainability tabular data, and design specs where downward flow is applicable. Design effort is monitored by attending design meetings, reviewing preliminary design data, such as sketches and drawings, and through concurrent engineering discussions with the design engineer. Issues that cannot be resolved informally are addressed by engineering management in internal reviews.

- ***Task 5, Participate in Design Trade-off Studies***

Maintainability engineering provides input for alternative design concepts, supporting concepts, subcontractor/supplier proposals, and analysis of the effect of alternative manufacturing processes on maintainability. The usual criteria for evaluating the compatibility of concepts or alternatives include relative MTTR, entry requirements, skill levels and number of staff, special tools and test equipment, impact on facilities and their life cycle maintenance cost.

- ***Task 6, Participate in Design Reviews***

Maintainability Engineering actively participates in all formal and informal internal reviews and is also included in the distribution of all proposed design changes. Each change is evaluated for the impact on quantitative and qualitative maintainability requirements. Upon approval of a design change, forecast parameter values, design criteria, or maintenance procedure documentation are updated as appropriate.

- ***Task 7, Subcontractor and Supplier Control***

Subcontractors and suppliers providing newly developed equipment are subject to the maintainability constraints assigned to them by the main contractor. Based on the results of the maintainability analysis, quantitative parameters are assigned and incorporated into the subcontractor's or supplier's specifications. Vendor progress is tracked and maintainability issues are highlighted for resolution.

- ***Task 8, Failure Reporting, Analysis, and Corrective Action***

Management can review failure trends, significant failures, default actions, and corrective actions at a program reliability review committee. A maintainability engineer participates in the review committee in the maintainability analysis process. In-plant corrective action data can provide useful maintainability data, including information on the timeline of maintainability actions.

- ***Task 9, Conduct Maintainability Demonstration***

Achievement of system maintainability requirements is assessed through formal and/or informal maintainability analyzes and demonstrations. Demonstration tests are conducted to support verification of contract requirements. Often the contractor will be required to demonstrate the MTTR of the system, which includes time for fault detection, fault isolation, removal and replacement, and repair verification.

2.4. Safety

For more information about this section, consult bibliography reference [11].

Safety is the state of being safe, the condition of being protected from harm or other dangers. Safety can also refer to the control of recognized hazards in order to achieve an acceptable level of risk.

System safety is an engineering discipline. Constant changes in technology, environmental regulation, and public safety concerns make analyzing complex safety-critical systems more and more challenging.

Safety engineering ensures that engineered systems provide acceptable levels of safety. Safety engineering ensures that a life-critical system performs as intended, even when components fail.

Analytical techniques can be divided into two categories: qualitative and quantitative methods. Both approaches share the goal of finding causal dependencies between a hazard on system level and individual component failures. Qualitative approaches focus on the causes of system hazards while quantitative methods aim to provide estimates of the probabilities, rates and severity of consequences.

The complexity of technical systems such as design and material improvements, planned inspections, fail-safe design and backup redundancy reduce risk and increase costs. The risk may be reduced to the lowest level that is reasonably achievable or practically achievable.

Traditionally, safety analysis techniques have relied solely on the skill and experience of the safety engineer. In the last decade, model-based approaches have gained prominence. Contrary to traditional methods, model-based techniques try to derive the relationships between causes and consequences from some sort of model of the system.

- ***Safety certification***

Typically, security guidelines prescribe a set of steps, deliverables, and exit criteria that focus on planning, analysis and design, implementation, testing and validation, configuration management, and quality assurance activities for developing a safety critical system. They also typically formulate expectations regarding the creation and use of traceability in the project. Higher quality traceability information can streamline the certification process and help build confidence in the maturity of the applied development process.

Failure in safety-certified systems is usually acceptable if, on average, less than one life is lost for every 10^9 hours of continuous operation. Most commercial aircraft are certified at this level. Cost versus loss of life was considered appropriate at this level by the FAA for aircraft systems under Federal Aviation Regulations.

- ***Preventing Failure***

Once a failure mode is identified, it can usually be mitigated by adding additional or redundant equipment to the system. Safety-critical systems are commonly required not to allow a single event or component failure to result in a catastrophic failure mode.

For any given failure, it is almost always possible to design and incorporate redundancy into a system.

There are two categories of techniques to reduce the probability of failure:

- Failure prevention techniques increase the reliability of individual elements.
- Fault-tolerant techniques, such as redundancies and barriers, increase overall system reliability.

- ***Traditional methods for safety analysis***

The two most common fault modeling techniques are called failure mode and effects analysis and fault tree analysis. They will be described in the next sections. These techniques are just ways of finding problems and of making plans to cope with failures, as in probabilistic risk assessment.

2.4.1. FMEA

Failure mode and effect analysis (FMEA) is the process of reviewing as many components, assemblies, and subsystems as possible to identify potential failure modes in a system and their causes and effects. For each component, the failure modes and their effects on the rest of the system are recorded in a specific FMEA worksheet. There are many variations of such worksheets. An FMEA can be a qualitative analysis, but it can be placed on a quantitative basis when mathematical models of the failure rate are combined with a statistical database of failure mode ratios. It was one of the first highly structured systematic techniques for failure analysis. An FMEA is often the first step of a system reliability study.

A few different types of FMEA analyses exist, such as:

- Functional
- Design
- Process

Sometimes FMEA is extended to FMECA (failure mode, effects, and criticality analysis) to indicate that criticality analysis is also performed.

FMEA is bottom-up inductive analytical reasoning, direct logic, single point of failure analysis and is a fundamental task in reliability engineering, safety engineering, and quality engineering.

FMEA can be performed both functionally or piece-part level. For functional FMEA, failure modes are identified for each function in a system or equipment item, usually with the help of a functional block diagram. For piece-part FMEA, failure modes are identified for each piece-part component such as a connector, resistor, or diode. Failure mode effects are described and a probability is assigned based on the failure rate and failure mode ratio of the function or component.

Failure modes with identical effects can be combined and resumed in a Failure Mode Effects Summary.

A successful FMEA activity helps identify potential failure modes based on experience with similar products and processes, or based on the common physics of failure logic. It is widely used in the development and manufacturing industries at various stages of the product life cycle. Effects analysis refers to studying the consequences of such failures on different system levels.

Functional analyses are needed as an input to determine correct failure modes, at all system levels, both for functional FMEA or piece-part FMEA. An FMEA is used to structure mitigation for risk reduction based on either failure mode effect severity reduction or based on lowering the probability of failure or both. The FMEA is in principle a full inductive, forward logic, analysis, however the failure probability can only be estimated or reduced by understanding the failure mechanism. Hence, FMEA may include information on causes of failure to reduce the possibility of occurrence by eliminating identified root causes.

FMEA is a design tool used to systematically analyze postulated component failures and identify the resulting effects on system operations. The analysis is sometimes characterized as consisting of two sub-analyses, the first being the failure mode and effects analysis (FMEA) and the second being the criticality analysis (CA). Successful development of an FMEA requires that the analyst include all significant failure modes for each contributing element or part of the system. FMEAs can be performed at the system, subsystem, assembly, subassembly, or part level. The FMECA should be scheduled and completed concurrently with the planning. If completed in a timely manner, the FMECA can help guide design decisions. The usefulness of the FMECA as a design tool and in decision making process depends on how effectively and promptly design problems are identified. Timeliness is probably the most important consideration. In the extreme case, the FMECA would be of little value to design decision making if the analysis is done after the hardware is built. While the FMECA identifies all failure modes of parts, its primary benefit is the early identification of all critical and catastrophic system or subsystem failure modes so that they can be eliminated or minimized through modification of the project in the first phase of the development. Therefore, the FMECA should be performed at the system level as soon as preliminary design information is available and extended to lower levels as the detailed design progresses.

- ***Functional failure mode and effects analysis***

The analysis should always begin by listing the functions that the project must fulfill. Functions are the starting point of a well-crafted FMEA, and using functions as a baseline provides the best performance of an FMEA. A project is just a one possible solution to perform functions that need to be fulfilled. In this way it is possible to perform an FMEA on conceptual designs and detailed designs, on hardware and software and regardless of the complexity of the project.

In addition to the FMEAs performed on systems to evaluate the impact that lower-level failures have on system operation, many other FMEAs are performed. Particular attention is paid to the interfaces between systems and all functional interfaces. The purpose of these FMEAs is to ensure that irreversible physical and functional damage does not propagate across the interface as a result of a failure in one of the interface units. These analyzes are performed at the part level for circuits that interface directly with other units. FMEA can be performed without a criticality analysis, but a criticality analysis requires that the FMEA has previously identified critical system-level failures.

- ***Types of analysis***

- Functional: before design solutions are provided, the functions can be evaluated on the potential effects of functional failure. General mitigations may be proposed to limit the consequences of functional failures or limit the likelihood of them occurring in this early development. It is based on a functional breakdown of a system.
- Concept hardware design: analysis of systems or subsystems in the early stages of the design concept to analyze failure mechanisms and lower-level functional failures. It can be used in trade-off studies.
- Detailed hardware design: analysis of products before production. These are the most detailed FMEAs, called Piece-Part or Hardware FMEA, and used to identify any possible hardware failure modes down to the lowest part level. It should be based on hardware breakdown, such as Bill of Materials (BoM). Any severity of failure effect, failure prevention, mitigation, failure detection and diagnostics can be fully analyzed in this FMEA.
- Process: analysis of manufacturing and assembly processes. Both quality and reliability can be affected by process errors. The input for this FMEA is among other things a work process breakdown.

- ***Ground rules***

The ground rules of each FMEA include a set of project selected procedures, the assumptions on which the analysis is based, the hardware that has been included and excluded from the analysis and the motivations for the exclusions. The ground rules also describe the level of the analysis, the basic hardware status and the criteria for system and mission success. Every effort should be made to define all ground rules before the FMEA begins. However, the ground rules may be expanded and clarified as the analysis proceeds. A typical set of ground rules follows:

- Only one failure mode exists at a time.
- All inputs to the item being analyzed are present and at nominal values.
- All consumables are present in sufficient quantities.
- Nominal power is available.

➢ ***Benefits***

Major benefits derived from a properly implemented FMECA effort are as follows:

- It provides a documented method for selecting a design with a high probability of successful operation and safety.
- A documented uniform method of assessing potential failure mechanisms, failure modes and their impact on system operation, resulting in a list of failure modes ranked according to the seriousness of their system impact and likelihood of occurrence.
- Early identification of single failure points and system interface problems, which may be critical to mission success and safety. They also provide a method of verifying that switching between redundant elements is not compromised by presumed single failures.
- An effective method for evaluating the effect of proposed changes to the design and operational procedures on mission success and safety.
- A basis for in-flight troubleshooting procedures and for locating performance monitoring and fault-detection devices.
- Criteria for early planning of tests.
- From the above list, early identifications of single failure points, input to the troubleshooting procedure and locating of performance monitoring, fault detection devices are probably the most important benefits of the FMECA. In addition, the FMECA procedures are straightforward and allow methodic evaluation of the design.

➢ ***Basic terms***

The following terms are the basics of FMEA terminology.

- Action priority (AP)

The AP replaces the former risk matrix and RPN in some standards. It makes a statement about the need for additional improvement measures.

- Failure

The loss of a function under stated conditions.

- Failure mode

The specific manner or way by which a failure occurs in terms of failure of the part, component, function, equipment, subsystem, or system under investigation. Depending on the type of FMEA performed, failure mode may be described at various levels of detail. A piece-part FMEA will focus on detailed part or component failure modes.

A functional FMEA will focus on functional failure modes. These may be general or more detailed and specific to the equipment being analyzed.

- Failure cause

Defects in requirements, design, process, quality control, handling or part application, which are the underlying cause or sequence of causes that initiate a process that leads to a failure mode over a certain time. A failure mode may have more causes.

- Failure effect

Immediate consequences of a failure on operation, or more generally on the needs for the user that should be fulfilled by the function but now is not fully fulfilled

- Indenture levels

An identifier for system level and thereby item complexity based on the bill of material or functional breakdown. Complexity increases as levels are closer to one.

- Local effect

The failure effect as it applies to the item under analysis.

- Next higher-level effect

The failure effect as it applies at the next higher indenture level.

- End effect

The failure effect at the highest indenture level or total system.

- Detection

The means of detection of the failure mode by maintainer, operator or built-in detection system, including estimated dormancy period (if applicable)

- Probability

The likelihood of the failure occurring.

- Risk priority number (RPN)

Severity of the event multiplied by the probability of the event occurring and by detection, assumed as the probability that the event would not be detected before the user was aware of it.

- Severity

The consequences of a failure mode. Severity considers the worst potential consequence of a failure, determined by the degree of injury, property damage, system damage and time lost to repair the failure.

- Remarks / mitigation / actions

Additional info, including the proposed mitigation or actions used to lower a risk or justify a risk level or scenario.

- ***Probability (P)***

It is necessary to look at the cause of a failure mode and the likelihood of occurrence. This can be done by analysis, calculations or FEM analysis, looking at similar items or processes and the failure modes that have been documented for them in the past. A failure cause is looked upon as a design weakness. All the potential causes for a failure mode should be identified and documented. This should be in technical terms. A failure mode may give a Probability Ranking with a defined number of levels.

Ratings

1) Extremely unlikely: virtually impossible or no known occurrences on similar products or processes, with many running hours
2) Remote: relatively few failures
3) Occasional: occasional failures
4) Reasonably possible: repeated failures
5) Frequent: failure is almost inevitable

- ***Severity (S)***

Each end effect is given a severity number from no effect to a catastrophic one, based on cost and loss of life or quality of life. These numbers prioritize the failure modes together with probability and detectability. Below a typical classification is given.

Ratings

1) No relevant effect on reliability or safety
2) Very minor, no damage, no injuries, only results in a maintenance action
3) Minor, low damage, light injuries
4) Critical: causes a loss of primary function or loss of all safety margins
5) Catastrophic: product becomes inoperative and the failure may result in complete unsafe operation and possible multiple deaths

- ***Detection (D)***

The means or method by which a failure is detected, isolated by operator and the time it may take. This is important for maintainability control and it is especially important for multiple failure scenarios. This may involve dormant failure modes that have no direct system effect, while a redundant system automatically takes over or when the failure only is problematic during specific system states, or latent failures, such as deterioration failure mechanisms. It should be made clear how the failure mode or cause can be discovered by an operator under normal system operation or if it can be discovered by the maintenance crew by some diagnostic action or automatic built in system test. A dormancy and latency period may be entered.

Ratings

1) Certain – fault will be caught on test –
2) Almost certain
3) High

4) Moderate
5) Low
6) Fault is undetected by operators or maintainers

- ***Dormancy or latency period***

The average time that a failure mode may be undetected may be entered if known. For example:

- Seconds, auto detected by maintenance computer
- 8 hours, detected by turn-around inspection
- months, detected by scheduled maintenance block
- years, detected by overhaul task

- ***Indication***

If the undetected failure allows the system to remain in a safe, working state, a second failure situation should be explored to determine whether or not an indication will be evident to all operators and what corrective action they may or should take.

Indications to the operator should be described as follows:

- Normal - An indication that is evident to an operator when the system or equipment is operating normally.
- Abnormal - An indication that is evident to an operator when the system has malfunctioned or failed.
- Incorrect - An erroneous indication to an operator due to the malfunction or failure of an indicator.

- ***Detection coverage analysis***

This type of analysis is useful to determine how effective various test processes are at the detection of latent and dormant faults. The method used to accomplish this involves an examination of the applicable failure modes to determine whether or not their effects are detected, and to determine the percentage of failure rate applicable to the failure modes which are detected. The possibility that the detection means may itself fail latently should be accounted for in the coverage analysis as a limiting factor.

Another way to include detection coverage is for the FTA to conservatively assume that no holes in coverage due to latent failure in the detection method affect detection of all failures assigned to the failure effect category of concern. The FMEA can be revised if necessary for those cases where this conservative assumption does not allow the top event probability requirements to be met.

- ***Risk level (P×S) and (D)***

Risk is the combination of end effect probability and severity where probability and severity include the effect on non-detectability. The exact calculation may not be easy in all cases, such as those where multiple scenarios with multiple events are possible and detectability plays a crucial role. In that case fault tree analysis may be needed to determine exact probability and risk levels. The higher the risk level, the more justification and mitigation is needed to provide evidence and lower the risk to an acceptable level. High risk should be indicated to higher level management, who are responsible for final decision-making.

- ***Timing***

The FMEA should be updated whenever:

- A new product or process cycle begins
- Changes are made to the operating conditions
- A change is made in the design
- New regulations are instituted
- Customer feedback indicates a problem

- ***Uses***

- Development of system requirements that minimize the likelihood of failures
- Development of designs and test systems to ensure that the failures have been eliminated or the risk is reduced to acceptable level
- Development and evaluation of diagnostic systems
- To help with design choices in trade-off analysis

- ***Advantages***

- Catalyst for teamwork and idea exchange between functions
- Collect information to reduce future failures, capture engineering knowledge
- Early identification and elimination of potential failure modes
- Emphasize problem prevention
- Fulfill legal requirements
- Improve company image and competitiveness
- Improve production yield
- Improve the quality, reliability, and safety of a product/process
- Increase user satisfaction
- Maximize profit
- Minimize late changes and associated cost
- Reduce impact on company profit margin
- Reduce system development time and cost
- Reduce the possibility of same kind of failure in future
- Reduce the potential for warranty concerns

- ***Limitations***

While FMEA identifies important hazards in a system, its results may not be comprehensive and the approach has limitations. FMEA and other risk assessment methods and retrospective approaches, have been found to have limited validity when used in isolation. Challenges around scoping and organizational boundaries appear to be a major factor in this lack of validity. If used as a top-down tool, FMEA may only identify major failure modes in a system. Fault tree analysis is better suited for top-down analysis. When used as a bottom-up tool FMEA can complement FTA and identify many more causes and failure modes. It is not able to discover complex failure modes involving multiple failures within a subsystem, or to report expected failure intervals of particular failure modes up to the upper-level subsystem or system. Additionally, the multiplication of the severity, occurrence and detection rankings may result in rank reversals, where a less serious failure mode receives a higher RPN than a more serious failure mode. The reason for this is that the rankings are ordinal scale numbers, and multiplication is not defined for ordinal numbers. The ordinal rankings only say that one ranking is better or worse than another, but not by how much.

The FMEA worksheet is hard to produce, hard to understand and read, as well as hard to maintain. An alternative approach is to combine the traditional FMEA table with set of bow-tie diagrams. The diagrams provide a visualization of the chains of cause and effect, while the FMEA table provides the detailed information about specific events.

2.4.2. FMECA

FMECA extends FMEA by including a criticality analysis, which is used to track the probability of failure modes against the severity of their consequences. The result highlights failure modes with relatively high probability and severity of consequences, allowing direct corrective efforts to where they will produce the best value. FMECA tends to be preferred over FMEA in space and military applications, while various forms of FMEA predominate in other industries.

- ***Methodology***

The FMECA analysis procedure typically consists of the following logical steps:

1. Define the system
2. Define ground rules and assumptions in order to help drive the design
3. Construct system block diagrams
4. Identify failure modes at piece-part level or functional
5. Analyze failure effects/causes
6. Feed results back into design process
7. Classify the failure effects by severity
8. Perform criticality calculations
9. Rank failure mode criticality
10. Determine critical items
11. Feed results back into design process
12. Identify the means of failure detection, isolation and compensation
13. Perform maintainability analysis

14. Document the analysis, summarize uncorrectable design areas, identify special controls necessary to reduce failure risk
15. Make recommendations
16. Follow up on corrective action implementation and effectiveness

FMECA may be performed at the functional or piece-part level. Functional FMECA considers the effects of failure at the functional block level. Piece-part FMECA considers the effects of individual component failures, such as resistors, transistors or microcircuits. A piece-part FMECA requires far more effort, but provides the benefit of better estimates of probabilities of occurrence. However, Functional FMEAs can be performed much earlier and may help to better structure the complete risk assessment and provide other type of insight in mitigation options.

The criticality analysis may be quantitative or qualitative, depending on the availability of supporting part failure data.

❖ ***System Definition***

In this step, the major system to be analyzed is defined and partitioned into an indented hierarchy such as systems, subsystems or equipment, units or subassemblies, and piece-parts. Functional descriptions are created for the systems and allocated to the subsystems, covering all operational modes and mission phases.

❖ ***Ground rules and assumptions***

Before detailed analysis takes place, ground rules and assumptions are usually defined and agreed to. This might include, for example:

- Standardized mission profile with specific fixed duration mission phases
- Sources for failure rate and failure mode data
- Fault detection coverage that system built-in test will realize
- Whether the analysis will be functional or piece-part
- Criteria to be considered
- System for uniquely identifying parts or functions
- Severity category definitions

❖ ***Failure mode identification***

For each piece-part or each function covered by the analysis, a complete list of failure modes is developed. For functional FMECA, typical failure modes include:

- Untimely operation
- Failure to operate when required
- Loss of output
- Intermittent output
- Erroneous output
- Invalid output

For piece-part FMECA, failure mode data may be obtained from databases such as FMD–91 [12]. These databases provide not only the failure modes, but also the failure mode ratios. For example:

DEVICE FAILURE MODES AND FAILURE MODE RATIOS (FMD–91)

DEVICE TYPE	Failure Mode	Ratio (α)
RELAY	Fails to trip	.55
	Spurious trip	.26
	Short	.19
RESISTOR, COMPOSITION	Parameter change	.66
	Open	.31
	Short	.03

Table 7. Device failure modes

Each function or piece-part is then listed in matrix form with one row for each failure mode. Because FMECA usually involves very large data sets, a unique identifier must be assigned to each item and to each failure mode of each item.

- ***Failure effects analysis***

Failure effects are determined and entered for each row of the FMECA matrix, considering the criteria identified in the ground rules. Effects are separately described for the local, next higher, and end system levels. System level effects may include:

- System failure
- Degraded operation
- System status failure
- No immediate effect

- ***Severity classification***

Severity classification is assigned for each failure mode of each unique item and entered on the FMECA matrix, based upon system level consequences. A small set of classifications, usually having 3 to 10 severity levels, is used. Current FMECA severity categories for U.S. Federal Aviation Administration (FAA), NASA and European Space Agency space applications are derived from MIL-STD-882 [13].

SEVERITY CATEGORIES (MIL–STD–882)

CATEGORY	Description	Criteria
I	Catastrophic	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
II	Critical	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
III	Marginal	Could result in injury or occupational illness resulting in one or more lost work day(s), loss exceeding $10K but less than $200K, or environmental damage without violation of law or regulation where restoration activities can be accomplished.
IV	Negligible	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

Table 8. Severity categories

- ***Criticality ranking***

Failure mode criticality assessment may be qualitative or quantitative. For qualitative assessment, a probability code or number is assigned and entered on the matrix. For example, MIL-STD-882 [13] uses five probability levels:

FAILURE PROBABILITY LEVELS (MIL–STD–882)

DESCRIPTION	Level	Individual Item	Fleet
FREQUENT	A	Likely to occur often in the life of the item	Continuously experienced
PROBABLE	B	Will occur several times in the life of an item	Will occur frequently
OCCASIONAL	C	Likely to occur sometime in the life of an item	Will occur several times

REMOTE	D	Unlikely but possible to occur in the life of an item	Unlikely, but can reasonably be expected to occur
IMPROBABLE	E	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur, but possible

Table 9. Failure probability levels

The failure mode may then be charted on a criticality matrix using severity code as one axis and probability level code as the other. For quantitative assessment, modal criticality number is calculated for each failure mode of each item, and item criticality number is calculated for each item. The criticality numbers are computed using the following values:

- Basic failure rate λ_p
- Failure mode ratio α
- Conditional probability β
- Mission phase duration t

The basic failure rate λ_p is usually fed into the FMECA from a failure rate prediction based on reliability standards. For functional level FMECA, engineering judgment may be required to assign failure mode ratio. The conditional probability number β represents the conditional probability that the failure effect will result in the identified severity classification, given that the failure mode occurs. It represents the analyst's judgment as to the likelihood that the loss will occur.

❖ ***Critical item/failure mode list***

Once the criticality assessment is completed for each failure mode of each item, the FMECA matrix may be sorted by severity and qualitative probability level or quantitative criticality number. This enables the analysis to identify critical items and critical failure modes for which design mitigation is desired.

❖ ***Recommendations***

After performing FMECA, recommendations are made to design to reduce the consequences of critical failures. This may include selecting components with higher reliability, reducing the stress level at which a critical item operates, or adding redundancy or monitoring to the system.

❖ ***Maintainability analysis***

FMECA usually feeds into both Maintainability Analysis and Logistics Support Analysis, which both require data from the FMECA. FMECA is the most popular tool for failure and criticality analysis of systems for performance enhancement. In the present era of Industry 4.0, the industries are implementing a predictive maintenance strategy for their mechanical systems and FMECA is widely used for the failure mode identification and prioritization.

- ***FMECA report***

A FMECA report consists of system description, ground rules and assumptions, conclusions and recommendations, corrective actions to be tracked, and the attached FMECA matrix which may be in spreadsheet, worksheet, or database form.

- ***Advantages and disadvantages***

Strengths of FMECA include its comprehensiveness, the systematic establishment of relationships between failure causes and effects, and its ability to point out individual failure modes for corrective action in design. Weaknesses include the extensive labor required, the large number of trivial cases considered, and inability to deal with multiple-failure scenarios or unplanned cross-system effects.

- ***Failure detection methods***

For each component and failure mode, the ability of the system to detect and report the failure in question is analyzed. One of the following will be entered on each row of the FMECA matrix:

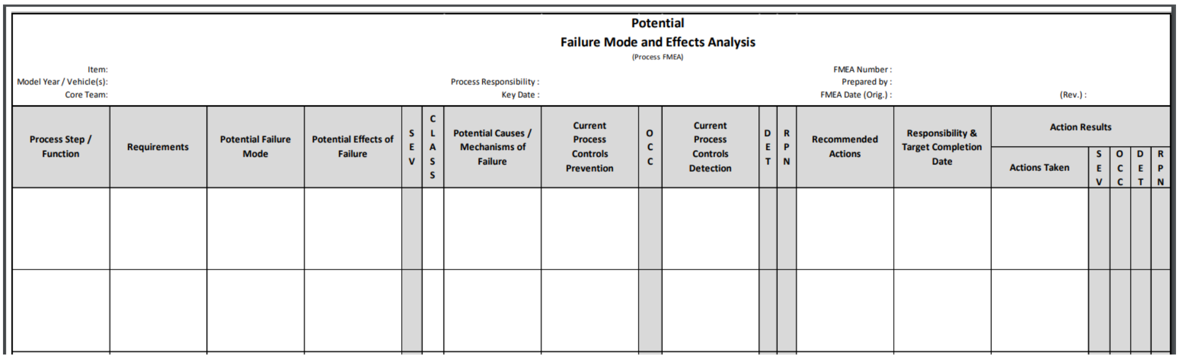
- Normal: the system correctly indicates a safe condition to the crew
- Abnormal: the system correctly indicates a malfunction requiring crew action
- Incorrect: the system erroneously indicates a safe condition in the event of malfunction, or alerts the crew to a malfunction that does not exist (false alarm)

2.4.3. How to perform FMEA and FMECA analysis

FMEA and FMECA aim to provide a list of potential failure modes ranked by:

- Importance
- Effect
- Probability

FMEA table or worksheet are generally used to guide decisions about changes that could prevent failure from spreading.



Potential
Failure Mode and Effects Analysis
(Process FMEA)

Item:
Model Year / Vehicle(s):
Core Team:
Process Responsibility :
Key Date :
FMEA Number :
Prepared by :
FMEA Date (Orig.) :
(Rev.) :

Process Step / Function	Requirements	Potential Failure Mode	Potential Effects of Failure	SEV	CLASS	Potential Causes / Mechanisms of Failure	Current Process Controls Prevention	OCC	Current Process Controls Detection	DET	RPN	Recommended Actions	Responsibility & Target Completion Date	Action Results				
														Actions Taken	SEV	OCC	DET	RPN

Figure 14. FMEA worksheet example

- ***FMEA type and information gathering***

As said before, there are different types of FMEA:

Design FMEA takes the entire life span of the component into consideration at the design stage. It regards material properties, interface between components, geometry, and engineering requirements.

Process FMEA considers all the steps that lead to the final product and is popular in manufacturing. It regards processing methods, machinery, and maintenance strategies.

Lastly, Functional FMEA thinks about the whole system rather than focusing on individual parts.

Once you have decided which type of FMEA to perform, the next phase is to gather as much information as possible to describe the product and process in detail. This can be done with the help of drawings, schematics, component lists, and interface information.

- ***Identify potential failure modes***

Refer back to the block diagram. For each item on the chart and each of its connections, write down all the ways it could break down. Approach it from a variety of angles.

There are many ways in which an asset can malfunction:

- part/system performs an unintended function
- poor performance
- reduced functionality
- failure to complete the intended function

This step is time-consuming. The goal is to be as complete as possible.

- ***Do a failure effect and cause analysis***

Failures propagate, so for each component/step, think about its impact on the environment and customers/users both internal and external. The more you invest early on in creating a robust, detailed diagram, the easier this step will be.

As the FMEA worksheet is filled out, think about each failure in two directions: What it affects downstream, as well as what upstream could cause such an issue in the first place like:

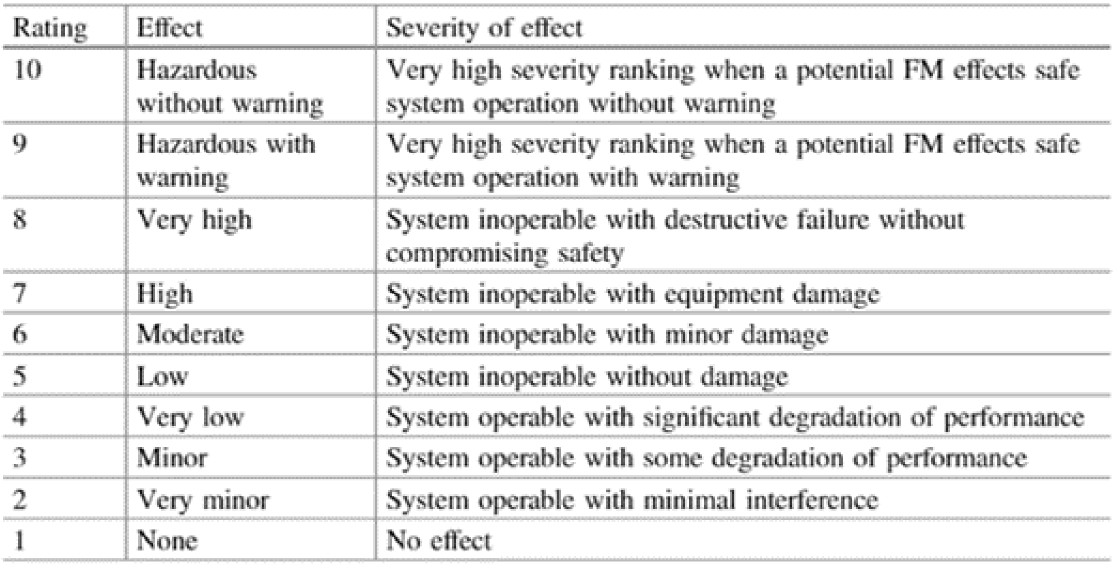
- Human error
- Material defects
- Incorrect engineering requirements

- ***Assign severity rankings***

Rank each failure on a scale of 0 to 10 where:

- 0: This failure has no measurable impact.
- 10: This failure would be dangerous and requires immediate intervention.

You are looking at the impact on users, downstream operations, the environment, and anyone or anything else that could be affected. Consider it in terms of costs, physical safety, time loss and damage to equipment.



Rating	Effect	Severity of effect
10	Hazardous without warning	Very high severity ranking when a potential FM effects safe system operation without warning
9	Hazardous with warning	Very high severity ranking when a potential FM effects safe system operation with warning
8	Very high	System inoperable with destructive failure without compromising safety
7	High	System inoperable with equipment damage
6	Moderate	System inoperable with minor damage
5	Low	System inoperable without damage
4	Very low	System operable with significant degradation of performance
3	Minor	System operable with some degradation of performance
2	Very minor	System operable with minimal interference
1	None	No effect

Table 10. Failure mode severity ranking

- ***Assign occurrence rankings***

In this step, consider how often this failure is likely to happen.

Once again, you rank possible failures on a scale of 0 to 10 where:

- 0: This failure is unlikely to ever happen.
- 10: This failure is virtually guaranteed.

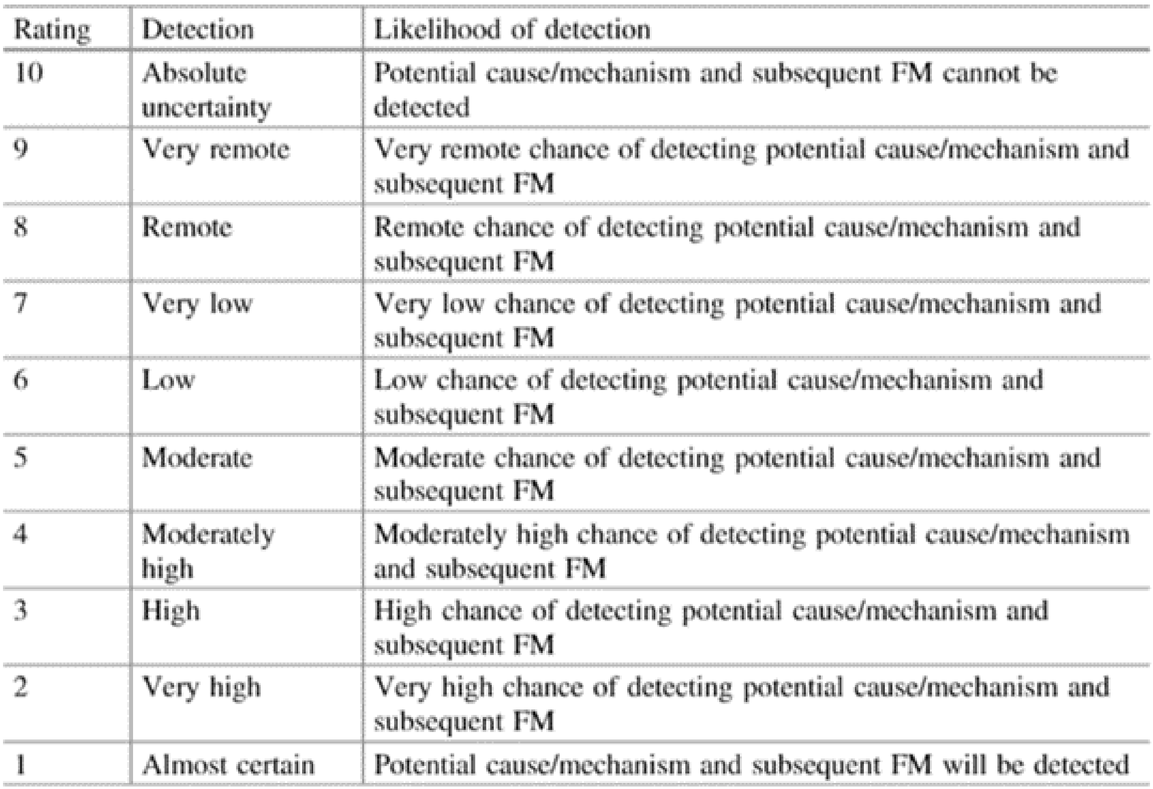
- ***Evaluate and assign failure detection rating***

Consider how easy or difficult it will be to detect this failure with the control systems you currently have in place. The control system could be a complex array of custom sensors, or it could be a quick visual inspection.

Ideally, the problem will be detected before it results in a complete failure for either the component or the whole system. Think about all of the positions you could put process control systems to catch the issue before it aggravates.

Rank each failure on a scale of 0 to 10 where:

- 0: You are almost guaranteed to detect the failure early.
- 10: Neither the failure nor its possible causes can be detected.



Rating	Detection	Likelihood of detection
10	Absolute uncertainty	Potential cause/mechanism and subsequent FM cannot be detected
9	Very remote	Very remote chance of detecting potential cause/mechanism and subsequent FM
8	Remote	Remote chance of detecting potential cause/mechanism and subsequent FM
7	Very low	Very low chance of detecting potential cause/mechanism and subsequent FM
6	Low	Low chance of detecting potential cause/mechanism and subsequent FM
5	Moderate	Moderate chance of detecting potential cause/mechanism and subsequent FM
4	Moderately high	Moderately high chance of detecting potential cause/mechanism and subsequent FM
3	High	High chance of detecting potential cause/mechanism and subsequent FM
2	Very high	Very high chance of detecting potential cause/mechanism and subsequent FM
1	Almost certain	Potential cause/mechanism and subsequent FM will be detected

Table 11. Detection rankings

- ***Calculate RPN***

RPN stands for risk priority number. RPN is calculated by multiplying the three rankings you obtained previously.

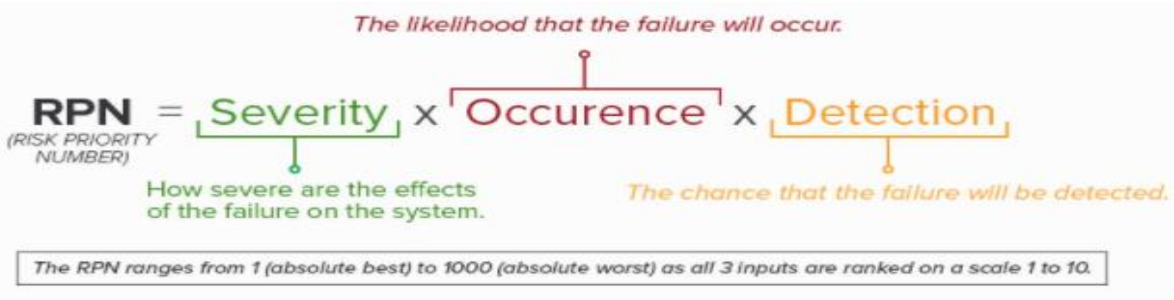

The likelihood that the failure will occur.
RPN
(RISK PRIORITY NUMBER)
=
Severity
x
Occurence
x
Detection
How severe are the effects of the failure on the system.
The chance that the failure will be detected.
The RPN ranges from 1 (absolute best) to 1000 (absolute worst) as all 3 inputs are ranked on a scale 1 to 10.

Figure 15. RPN

Do this calculation for every failure on your worksheet, and order the failures from high risk to low risk. Consult with your team to determine a critical level.

Some failures that seem minor could be triggers for other malfunctions that are downright catastrophic, so you have to be careful in perform correctly each step above.

➢ ***Take action***

Starting at the top of the list, look for ways that you could lower the RPN by adjusting at least one of the three factors that contribute to it:

- Occurrence: make the potential failure causes more robust, so they fail less often.
- Detection: add more control plans. There are innumerable sensors available, many of them with alarms or IoT integrations. These condition monitoring systems are an integral part of condition-based monitoring and predictive maintenance.
- Severity: put controls in place so that the consequences are not so significant.

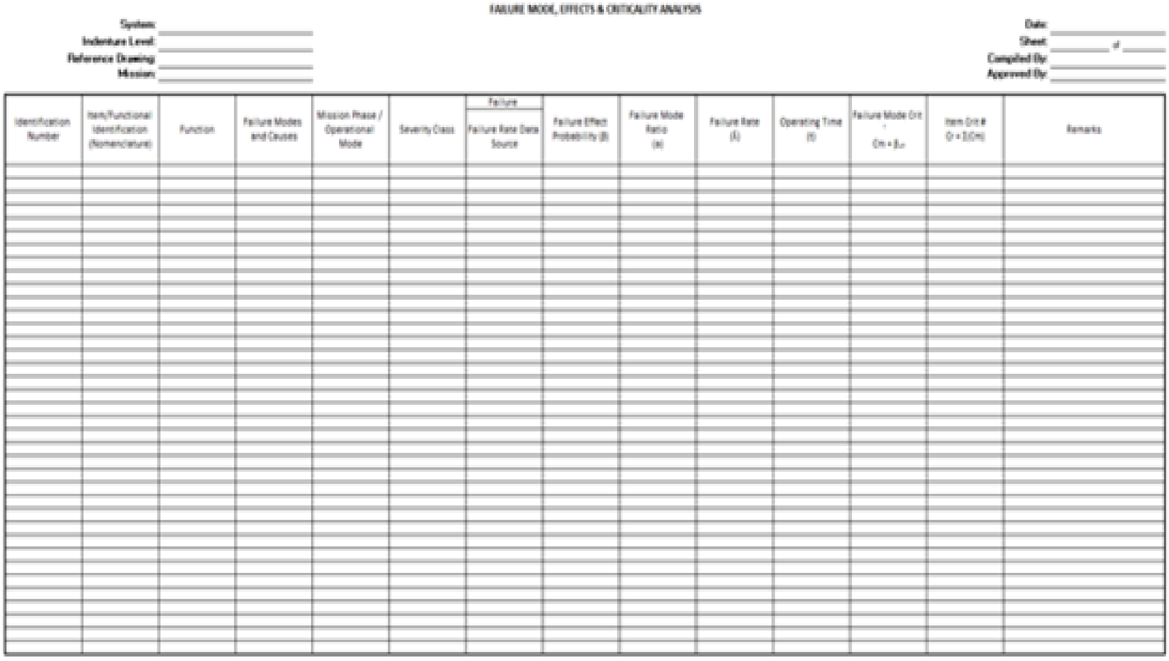
➢ ***Recalculate RPN***

When you have implemented your improvements, remake your occurrence, detection, and severity rankings, and recalculate your RPN. If you are still above the critical threshold, look for more ways to mitigate the failure.

If you are below your critical threshold, you are free to move on to the next failure.

➢ ***How to perform FMECA analysis***

As I mentioned previously, FMECA is an FMEA plus criticality. Just like FMEA, it has a worksheet:



FAILURE MODE, EFFECTS & CRITICALITY ANALYSIS

System: ____________
Indenture Level: ____________
Reference Drawing: ____________
Mission: ____________

Date: ____________
Sheet: ______ of ______
Compiled By: ____________
Approved By: ____________

Identification Number	Item/Functional Identification (Nomenclature)	Function	Failure Modes and Causes	Mission Phase / Operational Mode	Severity Class	Failure	Failure Effect Probability (β)	Failure Mode Ratio (α)	Failure Rate (λ)	Operating Time (t)	Failure Mode Crit # $C_m = \beta\alpha\lambda t$	Item Crit # $C_r = \Sigma(C_m)$	Remarks
						Failure Rate Data Source							

Figure 16. FMECA worksheet

- ***Perform FMEA***

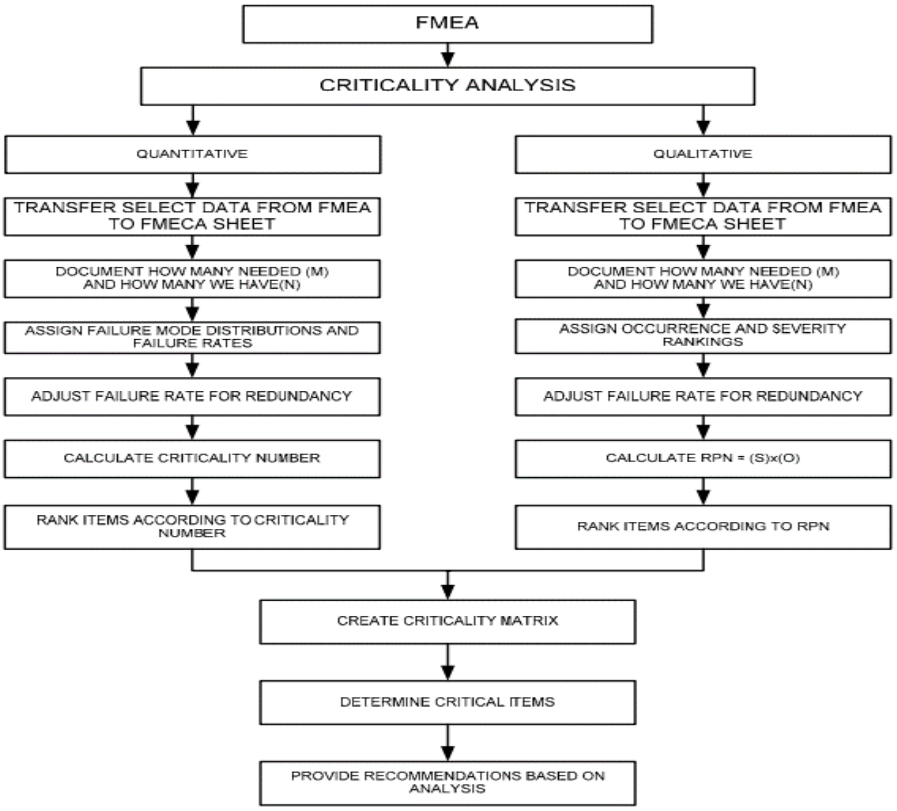

FMEA
CRITICALITY ANALYSIS
QUANTITATIVE
QUALITATIVE
TRANSFER SELECT DATA FROM FMEA TO FMECA SHEET
TRANSFER SELECT DATA FROM FMEA TO FMECA SHEET
DOCUMENT HOW MANY NEEDED (M) AND HOW MANY WE HAVE(N)
DOCUMENT HOW MANY NEEDED (M) AND HOW MANY WE HAVE(N)
ASSIGN FAILURE MODE DISTRIBUTIONS AND FAILURE RATES
ASSIGN OCCURRENCE AND SEVERITY RANKINGS
ADJUST FAILURE RATE FOR REDUNDANCY
ADJUST FAILURE RATE FOR REDUNDANCY
CALCULATE CRITICALITY NUMBER
CALCULATE RPN = (S)x(O)
RANK ITEMS ACCORDING TO CRITICALITY NUMBER
RANK ITEMS ACCORDING TO RPN
CREATE CRITICALITY MATRIX
DETERMINE CRITICAL ITEMS
PROVIDE RECOMMENDATIONS BASED ON ANALYSIS

Figure 17. FMECA flow

At this point, you have to choose between the top-down approach or the bottom-up approach.

The top-down approach, also known as the “functional method”, looks at the design requirements. It is usually invoked when creating a new product or new process.

The bottom-up approach is used most often on products or processes that already exist. It looks at each component individually, then as a part of bigger and bigger systems. The first steps outlined for the FMEA approach are inherently bottom-up. They say to list all your components and assess their potential failures one by one.

- ***Determine your parameters***

You get to choose whether to make this a qualitative or quantitative analysis. If you have large historical data a quantitative analysis is the right choice.

- ***Qualitative parameters***

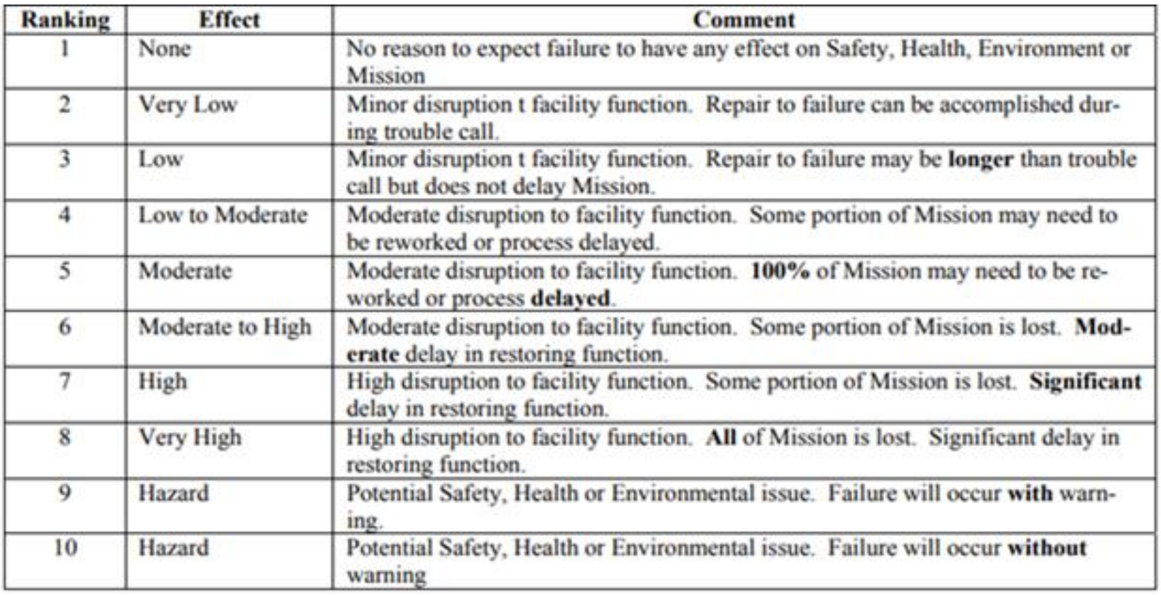
As in the FMEA, you will look at severity and occurrence.

The goal is to label the failure:

- Catastrophic: considerable losses to the environment, human life, and business operations.

- Harmful: the system is compromised and cannot perform its intended function. Trying to use the system causes additional damage.
- Marginal: there is some level of degradation, but it can still perform its functions.
- Minor: although there is degradation, the component/step continues to function optimally.
- No impact: you do not know whether a failure has occurred.

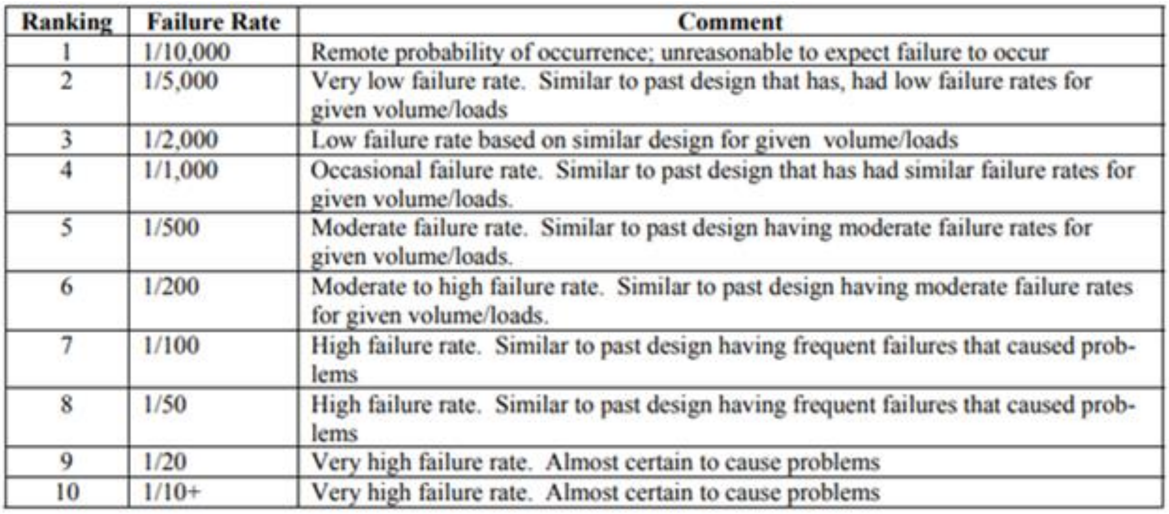
The official military standard for criticality analysis uses a specific 1 to 10 ranking:



Ranking	Effect	Comment
1	None	No reason to expect failure to have any effect on Safety, Health, Environment or Mission
2	Very Low	Minor disruption t facility function. Repair to failure can be accomplished during trouble call.
3	Low	Minor disruption t facility function. Repair to failure may be **longer** than trouble call but does not delay Mission.
4	Low to Moderate	Moderate disruption to facility function. Some portion of Mission may need to be reworked or process delayed.
5	Moderate	Moderate disruption to facility function. **100%** of Mission may need to be reworked or process **delayed**.
6	Moderate to High	Moderate disruption to facility function. Some portion of Mission is lost. **Moderate** delay in restoring function.
7	High	High disruption to facility function. Some portion of Mission is lost. **Significant** delay in restoring function.
8	Very High	High disruption to facility function. **All** of Mission is lost. Significant delay in restoring function.
9	Hazard	Potential Safety, Health or Environmental issue. Failure will occur **with** warning.
10	Hazard	Potential Safety, Health or Environmental issue. Failure will occur **without** warning

Table 12. Severity ranking

In other cases, there are four severity levels for FMECA instead of five. It is different in about every industry. After that, rank the chances of occurrence according to your team's designated FMECA procedure, such as the table 13 below:



Ranking	Failure Rate	Comment
1	1/10,000	Remote probability of occurrence; unreasonable to expect failure to occur
2	1/5,000	Very low failure rate. Similar to past design that has, had low failure rates for given volume/loads
3	1/2,000	Low failure rate based on similar design for given volume/loads
4	1/1,000	Occasional failure rate. Similar to past design that has had similar failure rates for given volume/loads.
5	1/500	Moderate failure rate. Similar to past design having moderate failure rates for given volume/loads.
6	1/200	Moderate to high failure rate. Similar to past design having moderate failure rates for given volume/loads.
7	1/100	High failure rate. Similar to past design having frequent failures that caused problems
8	1/50	High failure rate. Similar to past design having frequent failures that caused problems
9	1/20	Very high failure rate. Almost certain to cause problems
10	1/10+	Very high failure rate. Almost certain to cause problems

Table 13. Failure rates for FMECA

- ***Quantitative parameters***

This step allows you to fall back on hard data. Looking at known failure rates, use specific mathematical formulas with specific variables to calculate the failure mode criticality number.

In the end, you will have a failure mode criticality number representing how often a particular failure node occurs. It quantifies the consequences of that failure by summing up all the failure criticality numbers.

- ***Adjust failure rate for redundancy***

During the FMEA process, you discovered potential failures and took corrective action. One of those recommended actions may have been introducing redundancy, backup systems that correct for the same failure but in different ways.

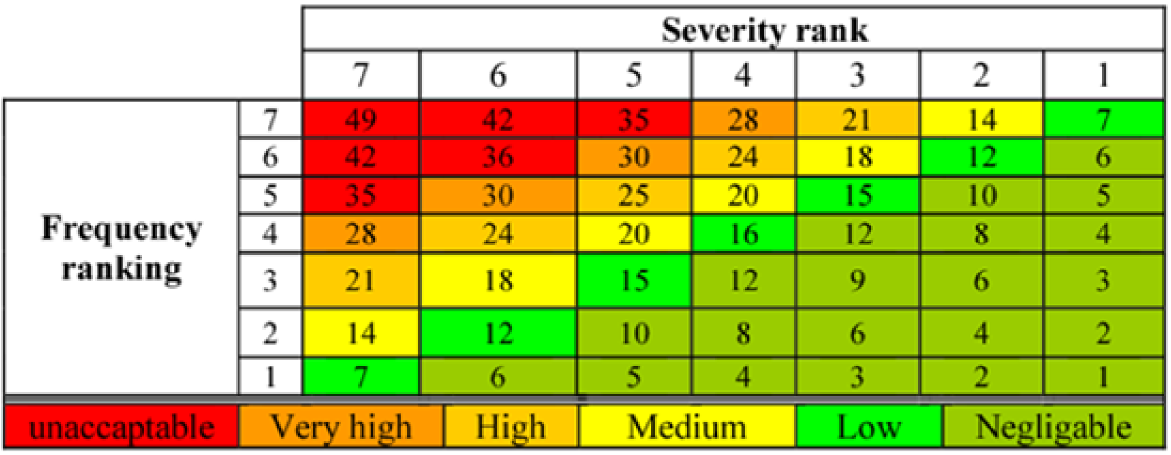
Accounting for those redundancies requires complex mathematics, but MIL-STD-1629 [14] is an excellent reference.

- ***Calculate criticality number or RPN***

If this is a quantitative case, you use the criticality number. For qualitative analysis, you have to calculate the risk priority number.

- ***Create a criticality matrix***

A criticality matrix is a visual representation of failure modes ranked by their likelihood and severity.



		Severity rank						
		7	6	5	4	3	2	1
Frequency ranking	7	49	42	35	28	21	14	7
	6	42	36	30	24	18	12	6
	5	35	30	25	20	15	10	5
	4	28	24	20	16	12	8	4
	3	21	18	15	12	9	6	3
	2	14	12	10	8	6	4	2
	1	7	6	5	4	3	2	1

unaccaptable	Very high	High	Medium	Low	Negligable

Figure 18. Criticality matrix example

Severity is plotted on the x-axis and frequency on the y-axis. Components with a low failure mode will end up in the bottom right (the green area), while high failure mode components will be in the top left (the red area).

- ***Determine critical items and take appropriate action***

To lower the probability of failures occurring:

- Modify your designs to control for potential risks that come from parts/steps you cannot change.
- Make changes that reduce the likelihood of failure.
- Create redundancies that add an extra layer of security and make the systems more fault tolerant.
- Replace specific pieces to optimize performance.
- Build up your systems that detect failures early on.

2.4.4. Fault tree analysis

Fault Tree Analysis (FTA) is a top-down deductive fault analysis in which an undesirable state of a system is analyzed using Boolean logic to combine a series of lower-level events. This method of analysis is primarily used in safety engineering and reliability engineering to understand how systems can fail, to identify the best ways to reduce risk, and to determine event rates of a safety incident or a particular functional failure at the system level. FTA is used in aerospace, nuclear, chemical, petrochemical and other high-risk industries. But it is also used in fields as diverse as identifying risk factors related to failure of the social services system. FTA is also used in software engineering for debugging purposes and is closely related to the root elimination technique used to detect bugs.

In aerospace, the general term system failure condition is used for the undesired event at the top of the fault tree. These conditions are classified according to the severity of their effects. The most severe conditions require the most extensive fault tree analysis. These system failure conditions and their classification are often determined previously in the functional risk analysis.

- ***Usage***

Fault tree analysis can be used to:

- understand the logic leading to the top event, undesired state.
- show compliance with the input system safety and reliability requirements.
- prioritize the contributors leading to the top event, creating the critical equipment, parts, events lists for different importance measures
- monitor and control the safety performance of the complex system
- minimize and optimize resources
- assist in designing a system
- function as a diagnostic tool to identify and correct causes of the top event. It can help with the creation of diagnostic manuals and processes

- ***Methodology***

The FTA methodology is described in several government and industry standards, including MIL-HDBK-338 [15] for military systems.

Any sufficiently complex system is prone to failure due to the malfunction of one or more subsystems. The probability of failure, however, can often be reduced through improved system design. Fault tree analysis maps the relationship between faults, subsystems, and redundant safety design elements by creating a logical diagram of the entire system.

The unintended outcome is considered the root, main event, of a logic tree. When fault trees are labeled with real numbers for failure probabilities, computer programs can calculate failure probabilities from the fault trees. When a specific event is found to have more than one effect event, it is referred to as a common cause or common mode. Graphically speaking, this means that this event will appear in different locations in the tree. Common causes introduce dependency relationships between events. Probability calculations for a tree that contains some common cause are much more complicated than for regular trees where all events are assumed to be independent. The tree is usually written using conventional logic gate symbols. A cut set is a combination of events, usually component failures, that cause the main event. If no event can be removed from a cut set without failing to cause the main event, then it is called a minimal cut set.

Some industries use both fault trees and event trees. An event tree starts with an unwanted initiator and follows possible further system events to a series of final consequences. As each new event is considered, a new node is added to the tree with a split probability of taking either branch. You can then view the probabilities of a series of main events arising from the initial event.

- ***Graphic symbols***

The basic symbols used in FTA are grouped as events, gates, and transfer symbols. M

Event symbols

Event symbols are used for primary events and intermediate events. Primary events are not further developed on the fault tree. Intermediate events are found at the output of a gate. The event symbols are shown below:

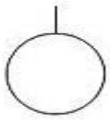
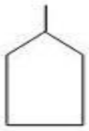
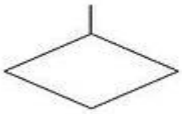
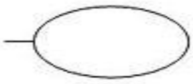
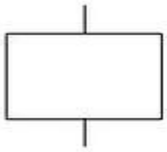
Basic event	**External event**	**Undeveloped event**	**Conditioning event**	**Intermediate event**
				

Table 14. Event Symbols

Primary event symbols are typically used as follows:

- Basic event: failure or error in a component or element of the system.
- External event: normally expected to occur.
- Undeveloped event: an event about which insufficient information is available or which has no consequences.
- Conditioning event: conditions that limit or affect logic gates.

Gate symbols

Gate symbols describe the relationship between input and output events. The symbols are derived from Boolean logic symbols:

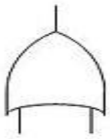
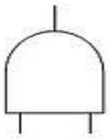
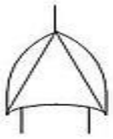
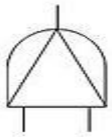
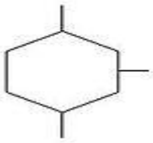
OR gate	AND gate	Exclusive OR gate	Priority AND gate	Inhibit gate
				

Table 15. Gate symbols

The gates work as follows:

- OR gate: the output occurs if any input occurs.
- AND gate: the output occurs only if all inputs occur. Inputs are independent from the source.
- Exclusive OR gate: the output occurs if exactly one input occurs.
- Priority AND gate: the output occurs if the inputs occur in a specific sequence specified by a conditioning event.
- Inhibit gate: the output occurs if the input occurs under an enabling condition specified by a conditioning event.

Transfer symbols

Transfer symbols are used to connect the inputs and outputs of related fault trees, such as the fault tree of a subsystem to its system.

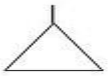
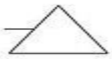
Transfer in	Transfer out
	

Table 16. Transfer symbols

➢ ***Mathematical models***

Events in a fault tree are associated with statistical probabilities or exponentially distributed Poisson constant rates. Component failures may typically occur at some constant failure rate λ. In this case, failure probability depends on the rate λ and the exposure time t, as in the equation (2.17) below:

$$P = 1 - \exp(-\lambda t) \qquad (2.16)$$

A fault tree is often normalized to a given time interval, such as a flight hour or an average mission time. Event probabilities depend on the relationship of the event hazard function to this interval.

Unlike conventional logic gate diagrams in which inputs and outputs hold the binary values of TRUE (1) or FALSE (0), the gates in a fault tree output probabilities related to the set operations of Boolean logic. The probability of a gate's output event depends on the input event probabilities.

An AND gate represents a combination of independent events. That is, the probability of any input event to an AND gate is unaffected by any other input event to the same gate. This is equivalent to the intersection of the input event sets, and the probability of the AND gate output is given by equation (2.18):

$$P\ (A \text{ and } B) = P\ (A \cap B) = P(A)*P(B) \qquad (2.17)$$

An OR gate, on the other hand, corresponds to set union and its output is given by equation (2.19):

$$P\ (A \text{ or } B) = P\ (A \cup B) = P(A) + P(B) - P\ (A \cap B) \qquad (2.18)$$

Since failure probabilities on fault trees tend to be small, P (A ∩ B) usually becomes a very small error term, and the output of an OR gate may be conservatively approximated by using an assumption that the inputs are mutually exclusive events:

$$P\ (A \text{ or } B) \approx P(A) + P(B);\ P\ (A \cap B) \approx 0$$

An exclusive OR gate with two inputs represents the probability that one or the other input, but not both, occurs, as in the following equation (2.20):

$$P\ (A \text{ xor } B) = P(A) + P(B) - 2P\ (A \cap B) \qquad (2.19)$$

Again, since P (A ∩ B) usually becomes a very small error term, the exclusive OR gate has limited value in a fault tree.

➢ ***Analysis***

Many different approaches can be used to model an FTA, but the most common and popular way can be summarized in just a few steps. A single fault tree is used to analyze one and only one undesired event, which can later be fed into another fault tree as a base event. While the nature of the undesired event can vary widely, a FTA follows the same procedure for any undesired event. FTA analysis involves five steps:

1) Define the undesired event to study - The definition of the undesired event can be very difficult to find out, although some of the events are very easy and obvious to observe. An engineer with extensive knowledge of system design is the best person to help define and number undesired events. The undesired events are then used to effect FTAs. Each FTA is limited to one undesired event.
2) Get an understanding of the system - Once the undesired event is selected, all causes with probabilities of influencing the undesired event equal to or greater than 0 are investigated and analyzed. Obtaining exact numbers for the probabilities leading to the event is usually impossible because it can be very costly and takes a long time. Computer software is used to study probabilities and can lead to a less costly system analysis. System analysts can help understand the overall system. System designers have full knowledge of the system and this knowledge is very important in order not to miss any cause that affects the undesired event. For the selected event, all the causes are then numbered and sequenced in the order of occurrence.
3) Construct the fault tree - After having selected the undesired event and having analyzed the system in order to know all its causal effects and their probabilities we can now construct the fault tree. The fault tree is based on AND and OR gates which define the main characteristics of the fault tree.
4) Evaluate the fault tree - After the fault tree is assembled for a specific undesired event, it is evaluated and analyzed for any possible improvement by risk management and find ways to improve the system. A wide range of qualitative and quantitative methods of analysis can be applied. This step is an introduction to the final step which will be to check the identified hazards. In short, in this phase we identify all the possible hazards that directly or indirectly affect the system.
5) Check identified hazards - This step is very specific and differs widely from one system to another, but the main point will always be that after identifying the hazards all possible methods are pursued to decrease the probability of occurrence.

➢ ***FTA Considerations***

FTA is a deductive, top-down method aimed at analyzing the effects of initiating faults and events on a complex system. This contrasts with failure mode and effects analysis (FMEA), which is a bottom-up inductive analysis method aimed at analyzing the effects of single component or function failures on equipment or subsystems. FTA is very good at showing how resistant a system is to single or multiple initial failures. It is not good at finding all possible initial flaws. FMEA is able to exhaustively catalog initial failures and identify their local effects. It is not useful for examining multiple failures or their system-wide effects. FTA considers external events, FMEA does not. In civil aerospace the usual practice is to perform both FTA and FMEA, with a failure mode effects summary (FMES) as the interface between FMEA and FTA. An alternative to FTA is the reliability block diagram (RBD).

3 Case Study

3.1. General overview

To show how the analysis RAMS works in reality, a case study about the SMART configuration for a helicopter will be analyzed. In particular, the analysis will be focused on the Monitor component, describing its reliability, safety and testability analysis. In the end, the fault tree analysis of the SMART system will be shown.

The SMART Configuration is an entire ecosystem for In Flight Entertainment and Cabin Management System (IFE/CMS) based on Synchronous Multimedia Avionic Ring Technology designed by Pariani. It is composed by these modules:

- 1x Media Server;
- 1x RIU Bus;
- 1x Audio Gateway for ICS;
- 2x Touchscreen 10.1”;
- 3x Monitor 21.5”;
- 1x HD-SDI Video Gateway;
- 1x HDMI Video Gateway;
- 4x Dual Headset.

The architecture is presented in the figure (19) below. In it, two categories are distinguished

- SMART Equipment: Part of the IFE& CMS (Yellow)
- External Interfaces: Not part of the SMART but the system will need to integrate its interfaces. (Green)

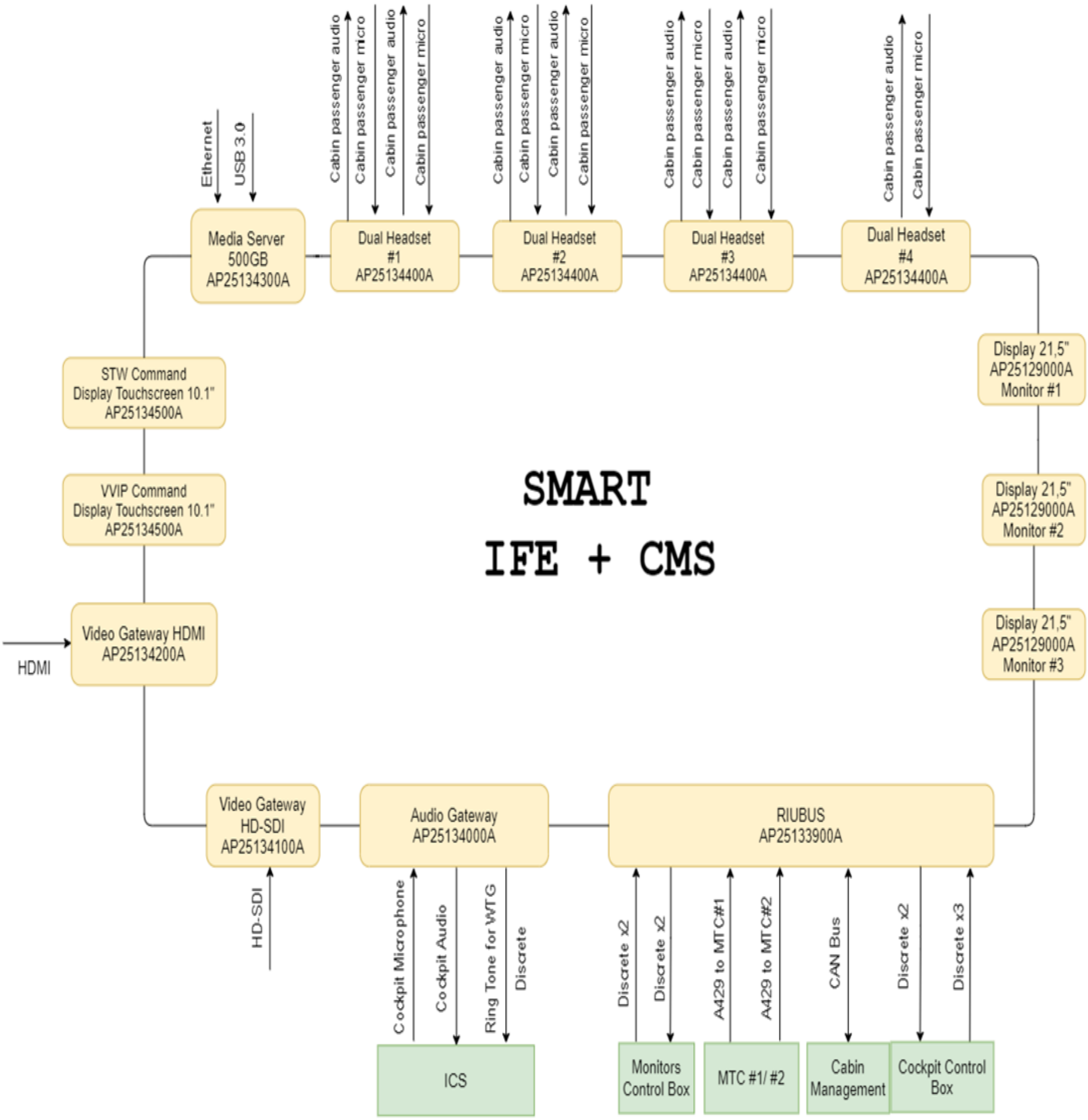


Figure 19. SMART IFE + CMS architecture

Equipment	*Functional Description*
Media Server	• Multimedia files storage • Jet Map • Diagnostic and system configuration • Communication rules • Ethernet • USB 3.0
RIU Bus	• Digital Inputs/Outputs • Lights system command through CAN BUS • ARINC 429 BUS
Touch Monitors 21.5"	• System controls • Communication • Wi-Fi • USB
Touchscreen 10,1"	• Stow Command • VVIP Command
Dual Headset	• Communication • Headset Interface
Audio Gateway	• Cockpit micro • Cockpit audio • Digital Inputs/Outputs • Bridge between SMART and ICS
HD-SDI Video Gateway	• HD-SDI for External Camera
HDMI Video Gateway	• HDMI

Table 17. Functional description of the component

- **Media Server**: SMART Media Server is the heart of the CMS and IFE. It’s based on a Linux embedded hardware with a max start-up time of 30s. Multimedia Files are stored in the SSD and can be easily uploaded and downloaded from USB mass storage devices or through TCP/IP connections. (USB3.0 to upload media files).

- **Riu Bus**: Equipped with digital I/O and serial buses, this gateway is able to interface third party systems such as avionic buses and discrete pushbuttons. Digital Inputs can be used to control keyboards, and more in general, all digital signals. Through Digital Outputs it is possible to switch-on lights, to control relays, and more in general, to control all devices that may need a digital command.

- **Touch Monitors**: SMART wired touch monitors are equipped with an embedded SoC and quad core CPU in order to maximize performance, reduce bandwidth and power supply, allowing full connectivity to system. SMART wired touch monitors are able to play media content from the bus. Equipped with a wide variety of connections including SMART bus, HDMI in, USB and RJ45. Through the HDMI it is possible to connect external devices and any other HDMI source. The sizes used in this configuration are the 10.1” and 21.5”.

- **Audio Gateway**: SMART Audio Gateway is able to interface the bus to external audio sources and devices like audio amplifier and pilot’s audio gateway. This unit acts as a gateway from any audio device and the bus. The digital Inputs and outputs are used to control buttons, to turn on lights, to switch relays related to the audio connection of this module.

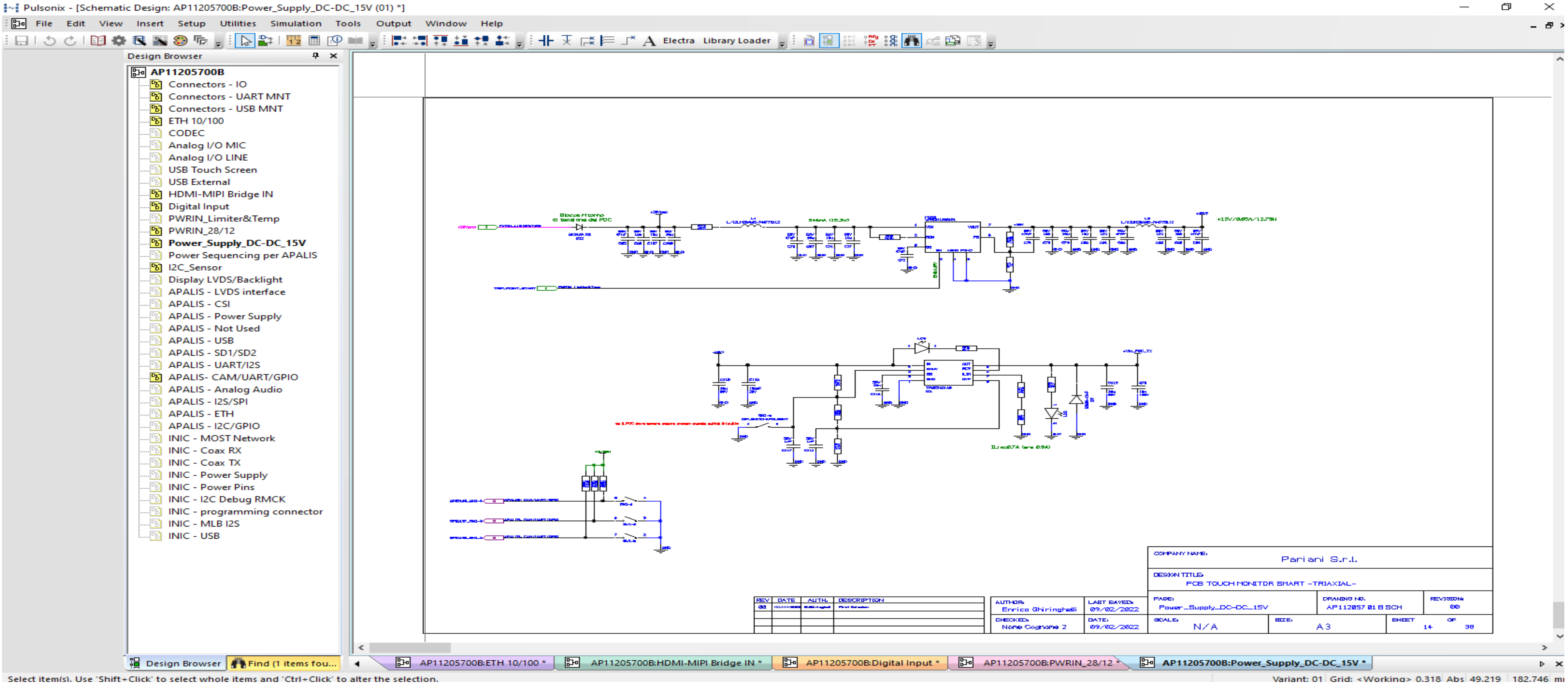
- **Dual Headset**: SMART Dual Headset is able to interface the SMART ring to passenger’s wired headset and is able to interact with the CMS/IFE. This unit acts as an audio gateway, from the headset and the bus.

- **Video Gateway**: Smart Video Gateway is able to interface an HD source, like HD video camera (for the HD-SDI Video Gateway) and other external sources with HDMI adapter (HDMI Video Gateway) and stream the video source on the network. The types of video gateways used in this configuration are:
  - 1x HD-SDI
  - 1x DVI (HDMI) with embedded Audio

3.2. Reliability, safety and testability analysis of the Display

➢ ***Display Reliability analysis***

By using the program Pulsonix, we can open the equipment scheme and take a look at its main parts, which are divided in pages that can be selected from the design browser located on the left side, as we can see in the figure (20).



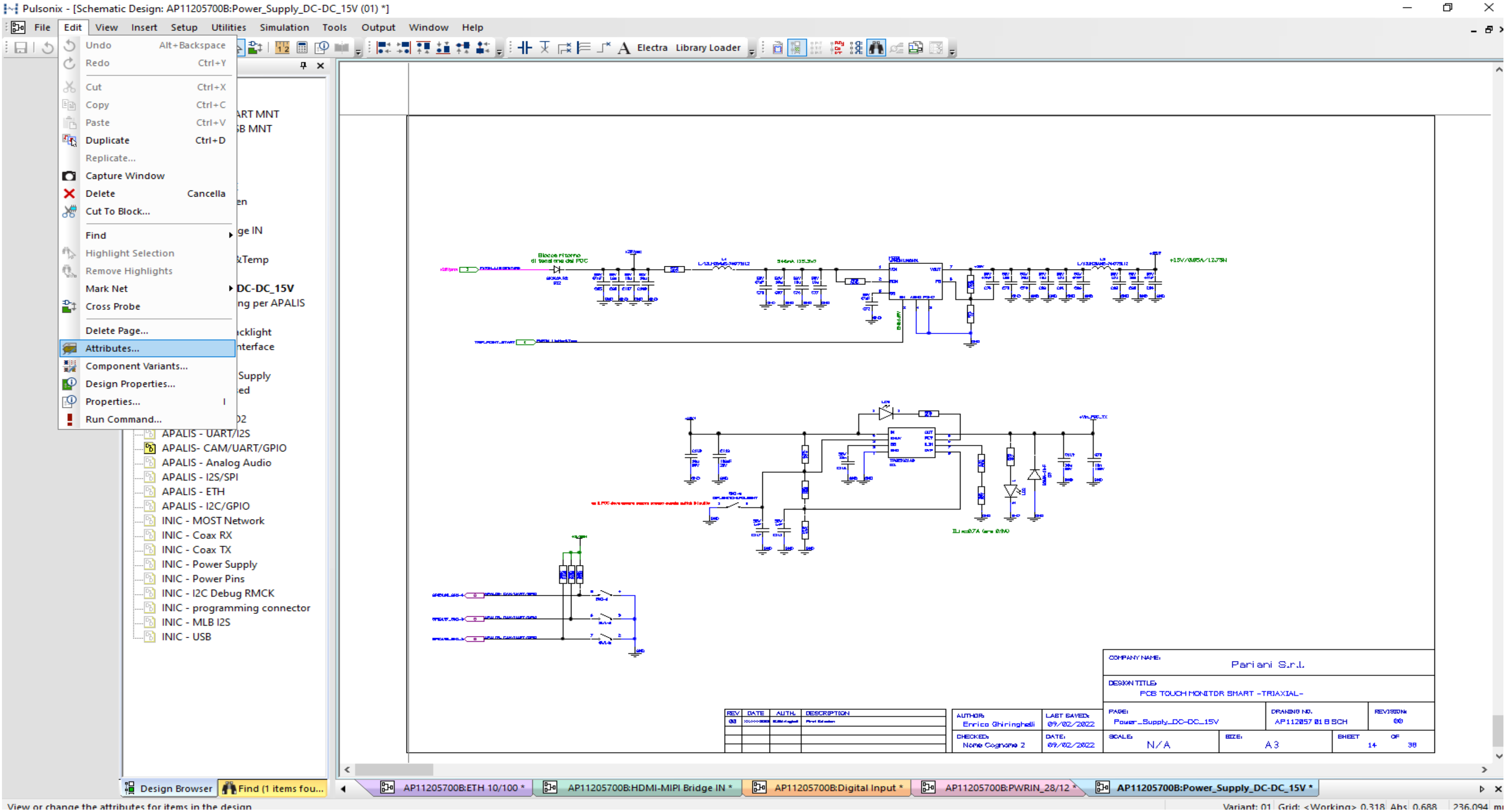
REV	DATE	AUTH.	DESCRIPTION
00	[illegible]	[illegible]	First Emission

COMPANY NAME: Pariani S.r.l.			
DESIGN TITLE: PCB TOUCH MONITOR SMART -TRIAXIAL-			
AUTHOR: Enrico Ghiringhelli	LAST SAVED: 09/02/2022	PAGE: Power_Supply_DC-DC_15V	DRAWING NO. AP112057 01 B SCH	REVISION: 00
CHECKED: Nome Cognome 2	DATE: 09/02/2022	SCALE: N/A	SIZE: A3	SHEET 14 OF 38

Select item(s). Use 'Shift+Click' to select whole items and 'Ctrl+Click' to alter the selection.

Figure 20. Pulsonix scheme

Next, to see the list of components, we use the edit attribute function as indicated in the figure (21) below.



COMPANY NAME: Pariani S.r.l.

DESIGN TITLE: PCB TOUCH MONITOR SMART -TRIAXIAL-

REV	DATE	AUTH.	DESCRIPTION
00	[illegible]	[illegible]	[illegible]

AUTHOR: Enrico Ghiringhelli

LAST SAVED: 09/02/2022

PAGE: Power_Supply_DC-DC_15V

DRAWING NO. AP112057 01 B SCH

REVISION: 00

CHECKED: Nome Cognome 2

DATE: 09/02/2022

SCALE: N/A

SIZE: A3

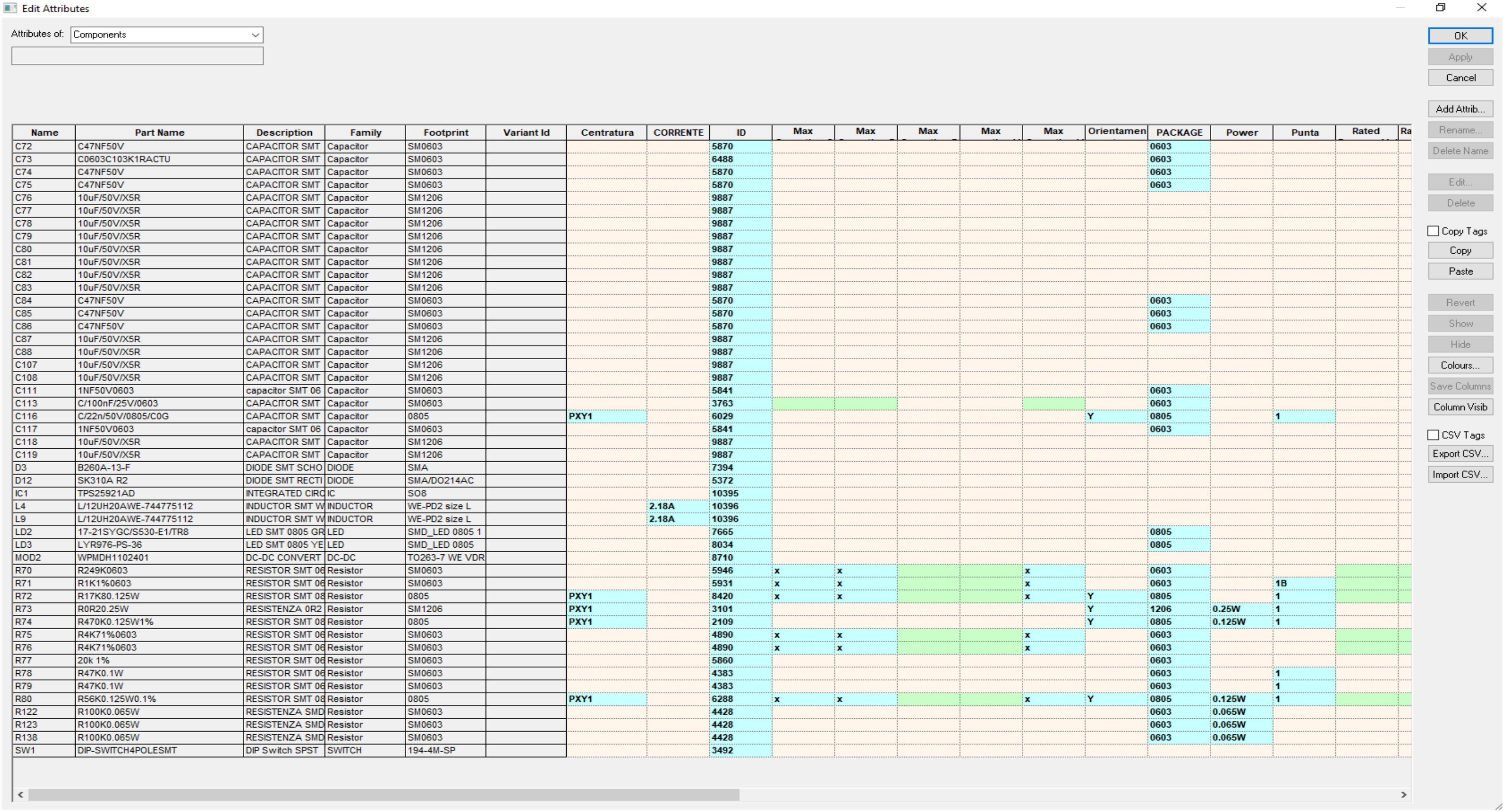
SHEET 14 OF 38

View or change the attributes for items in the design

Variant: 01 Grid: <Working> 0.318 Abs 0.688 236.094 m

Figure 21. Edit function

So, after using the edit function, we have now the list of components as we can see in the figure (22) below.

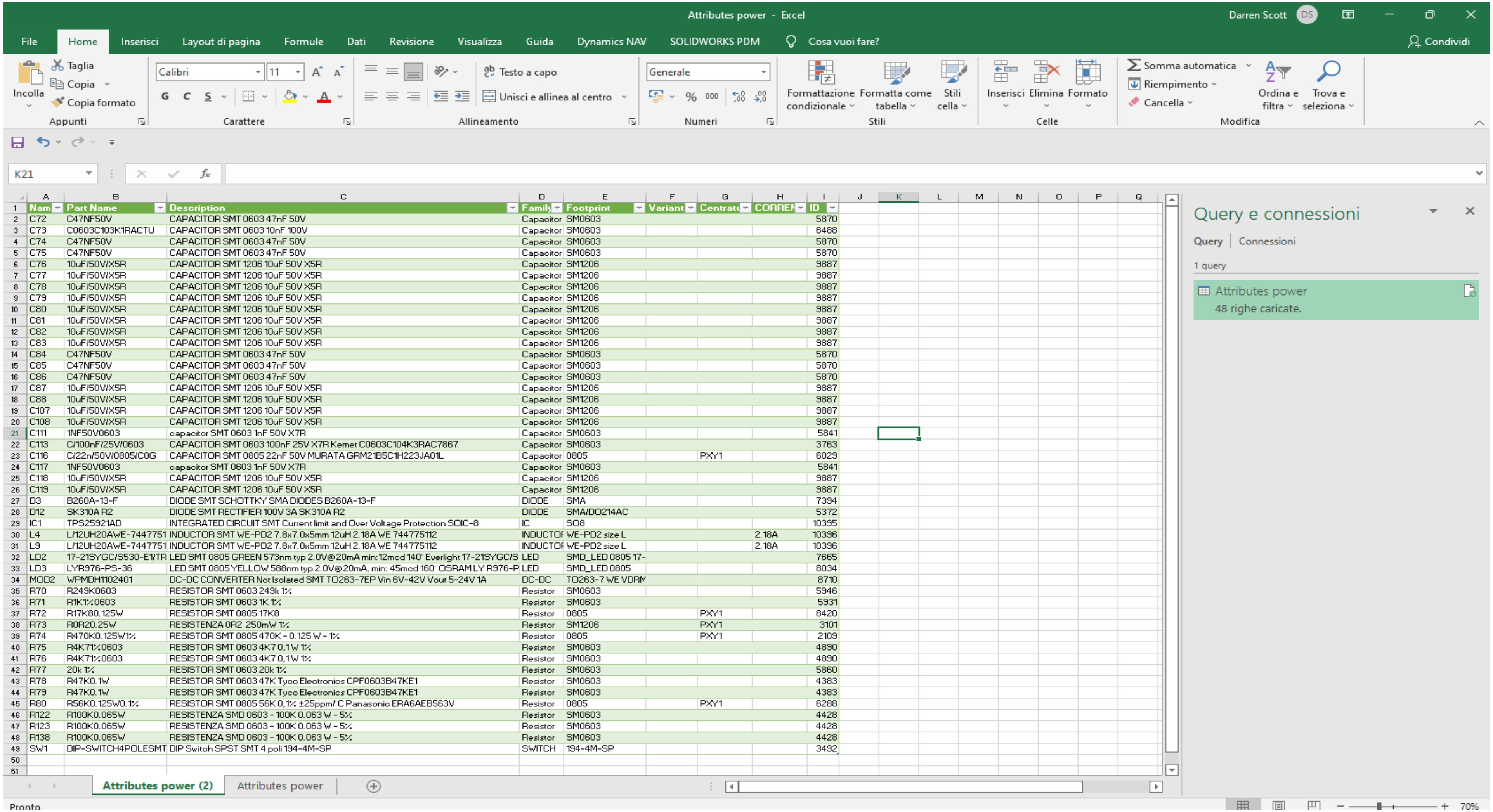


Attributes of: Components

Name	Part Name	Description	Family	Footprint	Variant Id	Centratura	CORRENTE	ID	Max	Max	Max	Max	Max	Orientamen	PACKAGE	Power	Punta	Rated	Ra
C72	C47NF50V	CAPACITOR SMT	Capacitor	SM0603				5870							0603				
C73	C0603C103K1RACTU	CAPACITOR SMT	Capacitor	SM0603				6488							0603				
C74	C47NF50V	CAPACITOR SMT	Capacitor	SM0603				5870							0603				
C75	C47NF50V	CAPACITOR SMT	Capacitor	SM0603				5870							0603				
C76	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C77	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C78	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C79	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C80	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C81	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C82	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C83	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C84	C47NF50V	CAPACITOR SMT	Capacitor	SM0603				5870							0603				
C85	C47NF50V	CAPACITOR SMT	Capacitor	SM0603				5870							0603				
C86	C47NF50V	CAPACITOR SMT	Capacitor	SM0603				5870							0603				
C87	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C88	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C107	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C108	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C111	1NF50V0603	capacitor SMT 06	Capacitor	SM0603				5841							0603				
C113	C/100nF/25V/0603	CAPACITOR SMT	Capacitor	SM0603				3763							0603				
C116	C/22n/50V/0805/C0G	CAPACITOR SMT	Capacitor	0805		PXY1		6029						Y	0805		1		
C117	1NF50V0603	capacitor SMT 06	Capacitor	SM0603				5841							0603				
C118	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
C119	10uF/50V/X5R	CAPACITOR SMT	Capacitor	SM1206				9887											
D3	B260A-13-F	DIODE SMT SCHO	DIODE	SMA				7394											
D12	SK310A R2	DIODE SMT RECTI	DIODE	SMA/DO214AC				5372											
IC1	TPS25921AD	INTEGRATED CIRC	IC	SO8				10395											
L4	L/12UH20AWE-744775112	INDUCTOR SMT W	INDUCTOR	WE-PD2 size L			2.18A	10396											
L9	L/12UH20AWE-744775112	INDUCTOR SMT W	INDUCTOR	WE-PD2 size L			2.18A	10396											
LD2	17-21SYGC/S530-E1/TR8	LED SMT 0805 GR	LED	SMD_LED 0805 1				7665							0805				
LD3	LYR976-PS-36	LED SMT 0805 YE	LED	SMD_LED 0805				8034							0805				
MOD2	WPMDH1102401	DC-DC CONVERT	DC-DC	TO263-7 WE VDR				8710											
R70	R249K0603	RESISTOR SMT 06	Resistor	SM0603				5946	x	x			x		0603				
R71	R1K1%0603	RESISTOR SMT 06	Resistor	SM0603				5931	x	x			x		0603		1B		
R72	R17K80.125W	RESISTOR SMT 08	Resistor	0805		PXY1		8420	x	x			x	Y	0805		1		
R73	R0R20.25W	RESISTENZA 0R2	Resistor	SM1206		PXY1		3101						Y	1206	0.25W	1		
R74	R470K0.125W1%	RESISTOR SMT 08	Resistor	0805		PXY1		2109						Y	0805	0.125W	1		
R75	R4K71%0603	RESISTOR SMT 06	Resistor	SM0603				4890	x	x			x		0603				
R76	R4K71%0603	RESISTOR SMT 06	Resistor	SM0603				4890	x	x			x		0603				
R77	20k 1%	RESISTOR SMT 06	Resistor	SM0603				5860							0603				
R78	R47K0.1W	RESISTOR SMT 06	Resistor	SM0603				4383							0603		1		
R79	R47K0.1W	RESISTOR SMT 06	Resistor	SM0603				4383							0603		1		
R80	R56K0.125W0.1%	RESISTOR SMT 08	Resistor	0805		PXY1		6288	x	x			x	Y	0805	0.125W	1		
R122	R100K0.065W	RESISTENZA SMD	Resistor	SM0603				4428							0603	0.065W			
R123	R100K0.065W	RESISTENZA SMD	Resistor	SM0603				4428							0603	0.065W			
R138	R100K0.065W	RESISTENZA SMD	Resistor	SM0603				4428							0603	0.065W			
SW1	DIP-SWITCH4POLESMT	DIP Switch SPST	SWITCH	194-4M-SP				3492											

Figure 22. List of components

Next, we export this list on Excel and then we can start the reliability analysis.



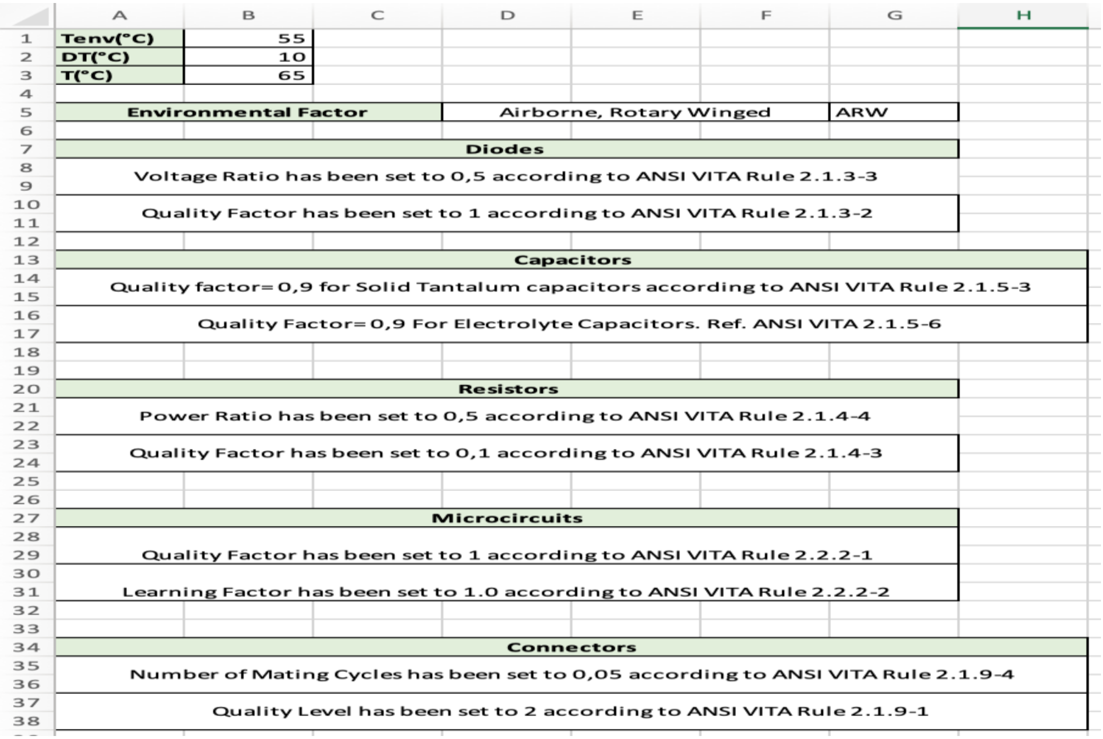
	A	B	C	D	E	F	G	H	I
1	Nam	Part Name	Description	Family	Footprint	Variant	Centratu	CORREN	ID
2	C72	C47NF50V	CAPACITOR SMT 0603 47nF 50V	Capacitor	SM0603				5870
3	C73	C0603C103K1RACTU	CAPACITOR SMT 0603 10nF 100V	Capacitor	SM0603				6488
4	C74	C47NF50V	CAPACITOR SMT 0603 47nF 50V	Capacitor	SM0603				5870
5	C75	C47NF50V	CAPACITOR SMT 0603 47nF 50V	Capacitor	SM0603				5870
6	C76	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
7	C77	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
8	C78	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
9	C79	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
10	C80	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
11	C81	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
12	C82	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
13	C83	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
14	C84	C47NF50V	CAPACITOR SMT 0603 47nF 50V	Capacitor	SM0603				5870
15	C85	C47NF50V	CAPACITOR SMT 0603 47nF 50V	Capacitor	SM0603				5870
16	C86	C47NF50V	CAPACITOR SMT 0603 47nF 50V	Capacitor	SM0603				5870
17	C87	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
18	C88	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
19	C107	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
20	C108	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
21	C111	1NF50V0603	capacitor SMT 0603 1nF 50V X7R	Capacitor	SM0603				5841
22	C113	C/100nF/25V/0603	CAPACITOR SMT 0603 100nF 25V X7R Kemet C0603C104K3RAC7867	Capacitor	SM0603				3763
23	C116	C/22n/50V/0805/C0G	CAPACITOR SMT 0805 22nF 50V MURATA GRM21B5C1H223JA01L	Capacitor	0805		PXY1		6029
24	C117	1NF50V0603	capacitor SMT 0603 1nF 50V X7R	Capacitor	SM0603				5841
25	C118	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
26	C119	10uF/50V/X5R	CAPACITOR SMT 1206 10uF 50V X5R	Capacitor	SM1206				9887
27	D3	B260A-13-F	DIODE SMT SCHOTTKY SMA DIODES B260A-13-F	DIODE	SMA				7394
28	D12	SK310A R2	DIODE SMT RECTIFIER 100V 3A SK310A R2	DIODE	SMA/DO214AC				5372
29	IC1	TPS25921AD	INTEGRATED CIRCUIT SMT Current limit and Over Voltage Protection SOIC-8	IC	SO8				10395
30	L4	L/12UH20AWE-7447751	INDUCTOR SMT WE-PD2 7.8x7.0x5mm 12uH 2.18A WE 744775112	INDUCTOR	WE-PD2 size L			2.18A	10396
31	L9	L/12UH20AWE-7447751	INDUCTOR SMT WE-PD2 7.8x7.0x5mm 12uH 2.18A WE 744775112	INDUCTOR	WE-PD2 size L			2.18A	10396
32	LD2	17-21SYGC/S530-E1/TR	LED SMT 0805 GREEN 573nm typ 2.0V@20mA min: 12mcd 140° Everlight 17-21SYGC/S	LED	SMD_LED 0805 17-				7665
33	LD3	LYR976-PS-36	LED SMT 0805 YELLOW 588nm typ 2.0V@20mA, min: 45mcd 160° OSRAM LY R976-P	LED	SMD_LED 0805				8034
34	MOD2	WPMDH1102401	DC-DC CONVERTER Not Isolated SMT TO263-7EP Vin 6V-42V Vout 5-24V 1A	DC-DC	TO263-7 WE VDRM				8710
35	R70	R249K0603	RESISTOR SMT 0603 249k 1%	Resistor	SM0603				5946
36	R71	R1K1%0603	RESISTOR SMT 0603 1K 1%	Resistor	SM0603				5931
37	R72	R17K80.125W	RESISTOR SMT 0805 17K8	Resistor	0805		PXY1		8420
38	R73	R0R20.25W	RESISTENZA 0R2 250mW 1%	Resistor	SM1206		PXY1		3101
39	R74	R470K0.125W1%	RESISTOR SMT 0805 470K - 0.125 W - 1%	Resistor	0805		PXY1		2109
40	R75	R4K71%0603	RESISTOR SMT 0603 4K7 0,1 W 1%	Resistor	SM0603				4890
41	R76	R4K71%0603	RESISTOR SMT 0603 4K7 0,1 W 1%	Resistor	SM0603				4890
42	R77	20k 1%	RESISTOR SMT 0603 20k 1%	Resistor	SM0603				5860
43	R78	R47K0.1W	RESISTOR SMT 0603 47K Tyco Electronics CPF0603B47KE1	Resistor	SM0603				4383
44	R79	R47K0.1W	RESISTOR SMT 0603 47K Tyco Electronics CPF0603B47KE1	Resistor	SM0603				4383
45	R80	R56K0.125W0.1%	RESISTOR SMT 0805 56K 0,1% ±25ppm/°C Panasonic ERA6AEB563V	Resistor	0805		PXY1		6288
46	R122	R100K0.065W	RESISTENZA SMD 0603 - 100K 0.063 W - 5%	Resistor	SM0603				4428
47	R123	R100K0.065W	RESISTENZA SMD 0603 - 100K 0.063 W - 5%	Resistor	SM0603				4428
48	R138	R100K0.065W	RESISTENZA SMD 0603 - 100K 0.063 W - 5%	Resistor	SM0603				4428
49	SW1	DIP-SWITCH4POLESMT	DIP Switch SPST SMT 4 poli 194-4M-SP	SWITCH	194-4M-SP				3492
50									
51									

Figure 23. Excel list

To perform the reliability analysis there are two ways:

- By using the standards and calculate each failure rate manually, but in this way the reliability analysis takes a long time
- By using a template related to the equipment, where we first set the temperature and the environment, and then, after filling the sheet with the list of components, we only need to indicate the operating voltage for the capacitors and the dissipated power for the resistors. Sometime for particular components, we have to calculate the failure rate manually, by using the standards. This method is obviously the fastest and the most used.

In the figure (24) below, we can see the notes about the temperature, the environment and the correction based on the ANSI VITA standard [7].



Tenv(°C)	55
DT(°C)	10
T(°C)	65

Environmental Factor	Airborne, Rotary Winged	ARW

Diodes

Voltage Ratio has been set to 0,5 according to ANSI VITA Rule 2.1.3-3

Quality Factor has been set to 1 according to ANSI VITA Rule 2.1.3-2

Capacitors

Quality factor= 0,9 for Solid Tantalum capacitors according to ANSI VITA Rule 2.1.5-3

Quality Factor= 0,9 For Electrolyte Capacitors. Ref. ANSI VITA 2.1.5-6

Resistors

Power Ratio has been set to 0,5 according to ANSI VITA Rule 2.1.4-4

Quality Factor has been set to 0,1 according to ANSI VITA Rule 2.1.4-3

Microcircuits

Quality Factor has been set to 1 according to ANSI VITA Rule 2.2.2-1

Learning Factor has been set to 1.0 according to ANSI VITA Rule 2.2.2-2

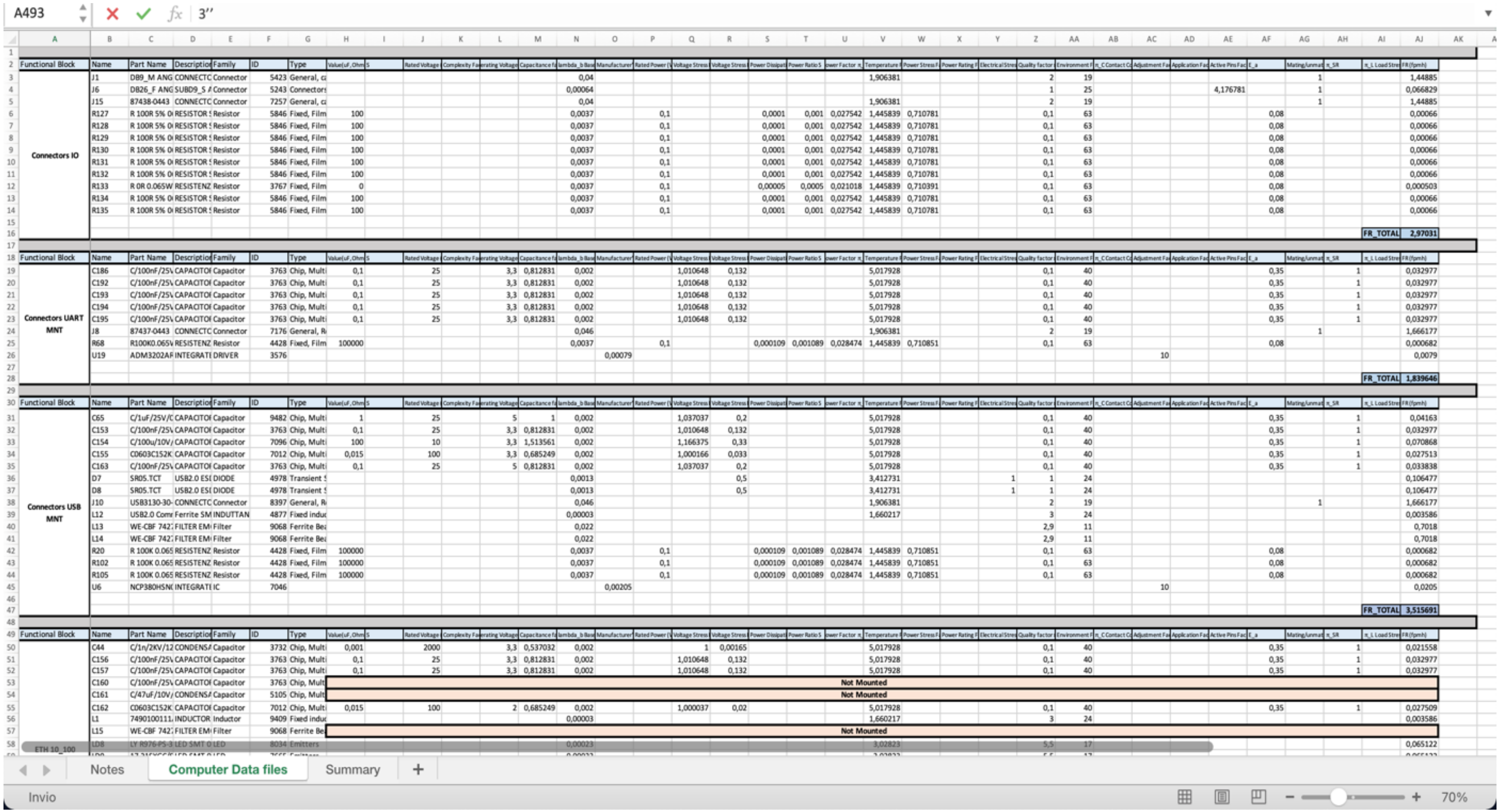
Connectors

Number of Mating Cycles has been set to 0,05 according to ANSI VITA Rule 2.1.9-4

Quality Level has been set to 2 according to ANSI VITA Rule 2.1.9-1

Figure 24. Temperature, Environment and ANSI VITA Notes

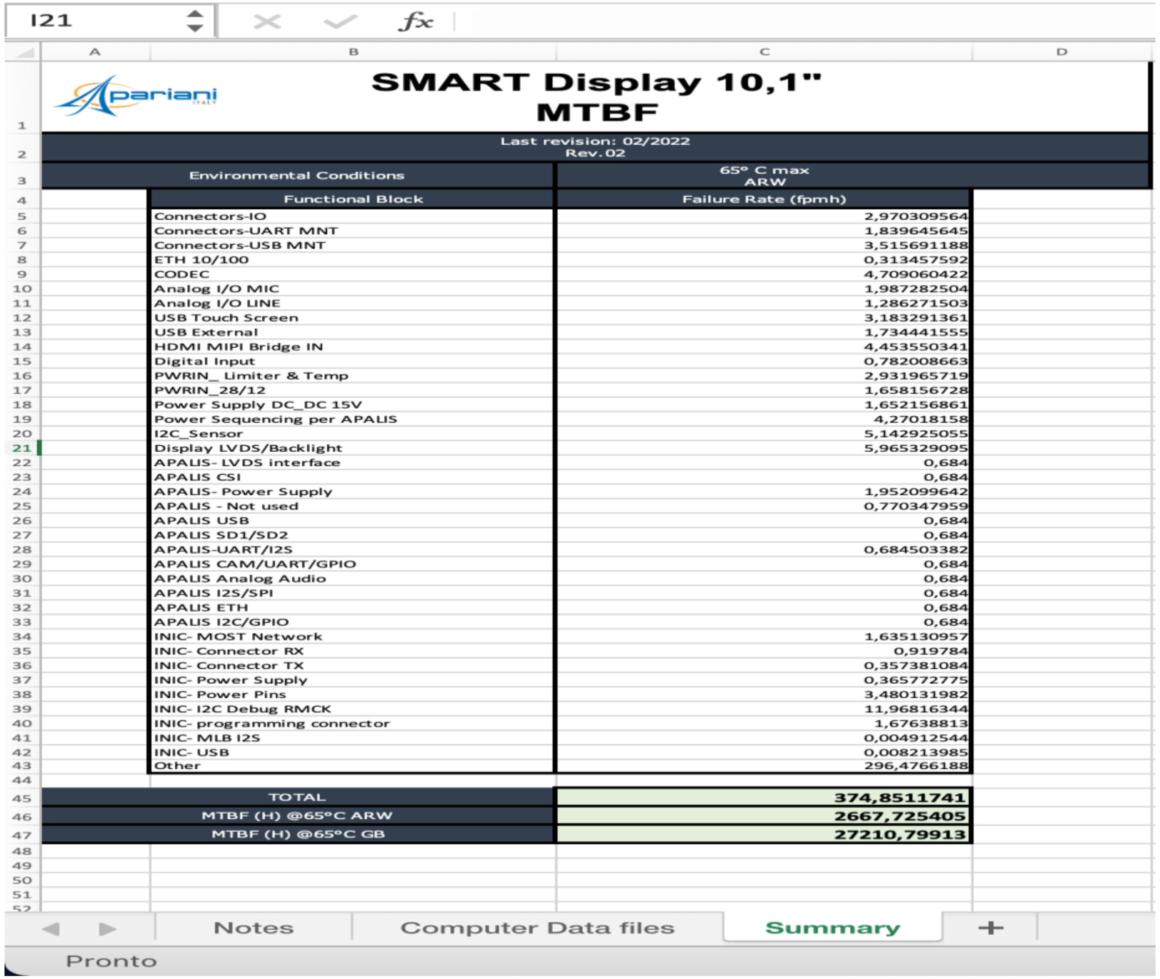
In the next figure (25), we can see the values of the coefficient, failure rates for each component and final failure rate of each part.



Functional Block	Name	Part Name	Descriptio	Family	ID	Type	Value(uF,Ohm	S	Rated Voltage	Complexity Fa	erating Voltage	Capacitance fa	lambda_b Base	Manufacturer	Rated Power (V	Voltage Stress	Voltage Stress	Power Dissipat	Power Ratio S	ower Factor π_	Temperature F	Power Stress F	Power Rating F	Electrical Stres	Quality factor	Environment F	π_C Contact C	Adjustment Fa	Application Fa	Active Pins Fac	E_a	Mating/unmat	π_SR	π_L Load Stre	FR (fpmh)
Connectors IO	J1	DB9_M ANG	CONNECTC	Connector	5423	General, ca							0,04								1,906381				2	19						1			1,44885
	J6	DB26_F ANG	SUBD9_S A	Connector	5243	Connectors							0,00064												1	25				4,176781		1			0,066829
	J15	87438-0443	CONNECTC	Connector	7257	General, ca							0,04								1,906381				2	19						1			1,44885
	R127	R 100R 5% 0	RESISTOR 5	Resistor	5846	Fixed, Film	100						0,0037		0,1			0,0001	0,001	0,027542	1,445839	0,710781			0,1	63					0,08				0,00066
	R128	R 100R 5% 0	RESISTOR 5	Resistor	5846	Fixed, Film	100						0,0037		0,1			0,0001	0,001	0,027542	1,445839	0,710781			0,1	63					0,08				0,00066
	R129	R 100R 5% 0	RESISTOR 5	Resistor	5846	Fixed, Film	100						0,0037		0,1			0,0001	0,001	0,027542	1,445839	0,710781			0,1	63					0,08				0,00066
	R130	R 100R 5% 0	RESISTOR 5	Resistor	5846	Fixed, Film	100						0,0037		0,1			0,0001	0,001	0,027542	1,445839	0,710781			0,1	63					0,08				0,00066
	R131	R 100R 5% 0	RESISTOR 5	Resistor	5846	Fixed, Film	100						0,0037		0,1			0,0001	0,001	0,027542	1,445839	0,710781			0,1	63					0,08				0,00066
	R132	R 100R 5% 0	RESISTOR 5	Resistor	5846	Fixed, Film	100						0,0037		0,1			0,0001	0,001	0,027542	1,445839	0,710781			0,1	63					0,08				0,00066
	R133	R 0R 0.065W	RESISTENZ	Resistor	3767	Fixed, Film	0						0,0037		0,1			0,00005	0,0005	0,021018	1,445839	0,710391			0,1	63					0,08				0,000503
	R134	R 100R 5% 0	RESISTOR 5	Resistor	5846	Fixed, Film	100						0,0037		0,1			0,0001	0,001	0,027542	1,445839	0,710781			0,1	63					0,08				0,00066
	R135	R 100R 5% 0	RESISTOR 5	Resistor	5846	Fixed, Film	100						0,0037		0,1			0,0001	0,001	0,027542	1,445839	0,710781			0,1	63					0,08				0,00066
																																		FR_TOTAL	2,97031
Functional Block	Name	Part Name	Descriptio	Family	ID	Type	Value(uF,Ohm	S	Rated Voltage	Complexity Fa	erating Voltage	Capacitance fa	lambda_b Base	Manufacturer	Rated Power (V	Voltage Stress	Voltage Stress	Power Dissipat	Power Ratio S	ower Factor π_	Temperature F	Power Stress F	Power Rating F	Electrical Stres	Quality factor	Environment F	π_C Contact C	Adjustment Fa	Application Fa	Active Pins Fac	E_a	Mating/unmat	π_SR	π_L Load Stre	FR (fpmh)
Connectors UART MNT	C186	C/100nF/25V	CAPACITOR	Capacitor	3763	Chip, Multi	0,1		25		3,3	0,812831	0,002			1,010648	0,132				5,017928				0,1	40					0,35		1		0,032977
	C192	C/100nF/25V	CAPACITOR	Capacitor	3763	Chip, Multi	0,1		25		3,3	0,812831	0,002			1,010648	0,132				5,017928				0,1	40					0,35		1		0,032977
	C193	C/100nF/25V	CAPACITOR	Capacitor	3763	Chip, Multi	0,1		25		3,3	0,812831	0,002			1,010648	0,132				5,017928				0,1	40					0,35		1		0,032977
	C194	C/100nF/25V	CAPACITOR	Capacitor	3763	Chip, Multi	0,1		25		3,3	0,812831	0,002			1,010648	0,132				5,017928				0,1	40					0,35		1		0,032977
	C195	C/100nF/25V	CAPACITOR	Capacitor	3763	Chip, Multi	0,1		25		3,3	0,812831	0,002			1,010648	0,132				5,017928				0,1	40					0,35		1		0,032977
	J8	87437-0443	CONNECTC	Connector	7176	General, R							0,046								1,906381				2	19						1			1,666177
	R68	R100K0.065V	RESISTENZ	Resistor	4428	Fixed, Film	100000						0,0037		0,1			0,000109	0,001089	0,028474	1,445839	0,710851			0,1	63					0,08				0,000682
	U19	ADM3202AF	INTEGRATI	DRIVER	3576									0,00079														10							0,0079
																																		FR_TOTAL	1,839646
Functional Block	Name	Part Name	Descriptio	Family	ID	Type	Value(uF,Ohm	S	Rated Voltage	Complexity Fa	erating Voltage	Capacitance fa	lambda_b Base	Manufacturer	Rated Power (V	Voltage Stress	Voltage Stress	Power Dissipat	Power Ratio S	ower Factor π_	Temperature F	Power Stress F	Power Rating F	Electrical Stres	Quality factor	Environment F	π_C Contact C	Adjustment Fa	Application Fa	Active Pins Fac	E_a	Mating/unmat	π_SR	π_L Load Stre	FR (fpmh)
Connectors USB MNT	C65	C/1uF/25V/C	CAPACITOR	Capacitor	9482	Chip, Multi	1		25		5	1	0,002			1,037037	0,2				5,017928				0,1	40					0,35		1		0,04163
	C153	C/100nF/25V	CAPACITOR	Capacitor	3763	Chip, Multi	0,1		25		3,3	0,812831	0,002			1,010648	0,132				5,017928				0,1	40					0,35		1		0,032977
	C154	C/100u/10V/	CAPACITOR	Capacitor	7096	Chip, Multi	100		10		3,3	1,513561	0,002			1,166375	0,33				5,017928				0,1	40					0,35		1		0,070868
	C155	C0603C152K	CAPACITOR	Capacitor	7012	Chip, Multi	0,015		100		3,3	0,685249	0,002			1,000166	0,033				5,017928				0,1	40					0,35		1		0,027513
	C163	C/100nF/25V	CAPACITOR	Capacitor	3763	Chip, Multi	0,1		25		5	0,812831	0,002			1,037037	0,2				5,017928				0,1	40					0,35		1		0,033838
	D7	SR05.TCT	USB2.0 ESI	DIODE	4978	Transient S							0,0013				0,5				3,412731			1	1	24									0,106477
	D8	SR05.TCT	USB2.0 ESI	DIODE	4978	Transient S							0,0013				0,5				3,412731			1	1	24									0,106477
	J10	USB3130-30-	CONNECTC	Connector	8397	General, R							0,046								1,906381				2	19						1			1,666177
	L12	USB2.0 Comr	Ferrite SM	INDUTTAN	4877	Fixed induc							0,00003								1,660217				3	24									0,003586
	L13	WE-CBF 742	FILTER EMI	Filter	9068	Ferrite Bea							0,022												2,9	11									0,7018
	L14	WE-CBF 742	FILTER EMI	Filter	9068	Ferrite Bea							0,022												2,9	11									0,7018
	R20	R 100K 0.065	RESISTENZ	Resistor	4428	Fixed, Film	100000						0,0037		0,1			0,000109	0,001089	0,028474	1,445839	0,710851			0,1	63					0,08				0,000682
	R102	R 100K 0.065	RESISTENZ	Resistor	4428	Fixed, Film	100000						0,0037		0,1			0,000109	0,001089	0,028474	1,445839	0,710851			0,1	63					0,08				0,000682
	R105	R 100K 0.065	RESISTENZ	Resistor	4428	Fixed, Film	100000						0,0037		0,1			0,000109	0,001089	0,028474	1,445839	0,710851			0,1	63					0,08				0,000682
	U6	NCP380HSNC	INTEGRATI	IC	7046									0,00205														10							0,0205
																																		FR_TOTAL	3,515691
Functional Block	Name	Part Name	Descriptio	Family	ID	Type	Value(uF,Ohm	S	Rated Voltage	Complexity Fa	erating Voltage	Capacitance fa	lambda_b Base	Manufacturer	Rated Power (V	Voltage Stress	Voltage Stress	Power Dissipat	Power Ratio S	ower Factor π_	Temperature F	Power Stress F	Power Rating F	Electrical Stres	Quality factor	Environment F	π_C Contact C	Adjustment Fa	Application Fa	Active Pins Fac	E_a	Mating/unmat	π_SR	π_L Load Stre	FR (fpmh)
	C44	C/1n/2KV/12	CONDENSA	Capacitor	3732	Chip, Multi	0,001		2000		3,3	0,537032	0,002			1	0,00165				5,017928				0,1	40					0,35		1		0,021558
	C156	C/100nF/25V	CAPACITOR	Capacitor	3763	Chip, Multi	0,1		25		3,3	0,812831	0,002			1,010648	0,132				5,017928				0,1	40					0,35		1		0,032977
	C157	C/100nF/25V	CAPACITOR	Capacitor	3763	Chip, Multi	0,1		25		3,3	0,812831	0,002			1,010648	0,132				5,017928				0,1	40					0,35		1		0,032977
	C160	C/100nF/25V	CAPACITOR	Capacitor	3763	Chip, Mult	Not Mounted																												
	C161	C/47uF/10V/	CONDENSA	Capacitor	5105	Chip, Mult	Not Mounted																												
	C162	C0603C152K	CAPACITOR	Capacitor	7012	Chip, Multi	0,015		100		2	0,685249	0,002			1,000037	0,02				5,017928				0,1	40					0,35		1		0,027509
	L1	7490100111.	INDUCTOR	Inductor	9409	Fixed induc							0,00003								1,660217				3	24									0,003586
	L15	WE-CBF 742	FILTER EMI	Filter	9068	Ferrite Be	Not Mounted																												
ETH 10_100	LD8	LY R976-PS-3	LED SMT 0	LED	8034	Emitters							0,00023								3,02823				5,5	17									0,065122

Figure 25. Failure rates calculations

In the figure (26) below, we can see the summary and the final failure rate which in the end is converted in MTBF in helicopter environment and by multiplying with an adjustment factor we obtain the MTBF for the ground environment. In the end, the results of the reliability analysis are reported in the reliability document which is sent to the costumer that requested the analysis.



SMART Display 10,1"
MTBF

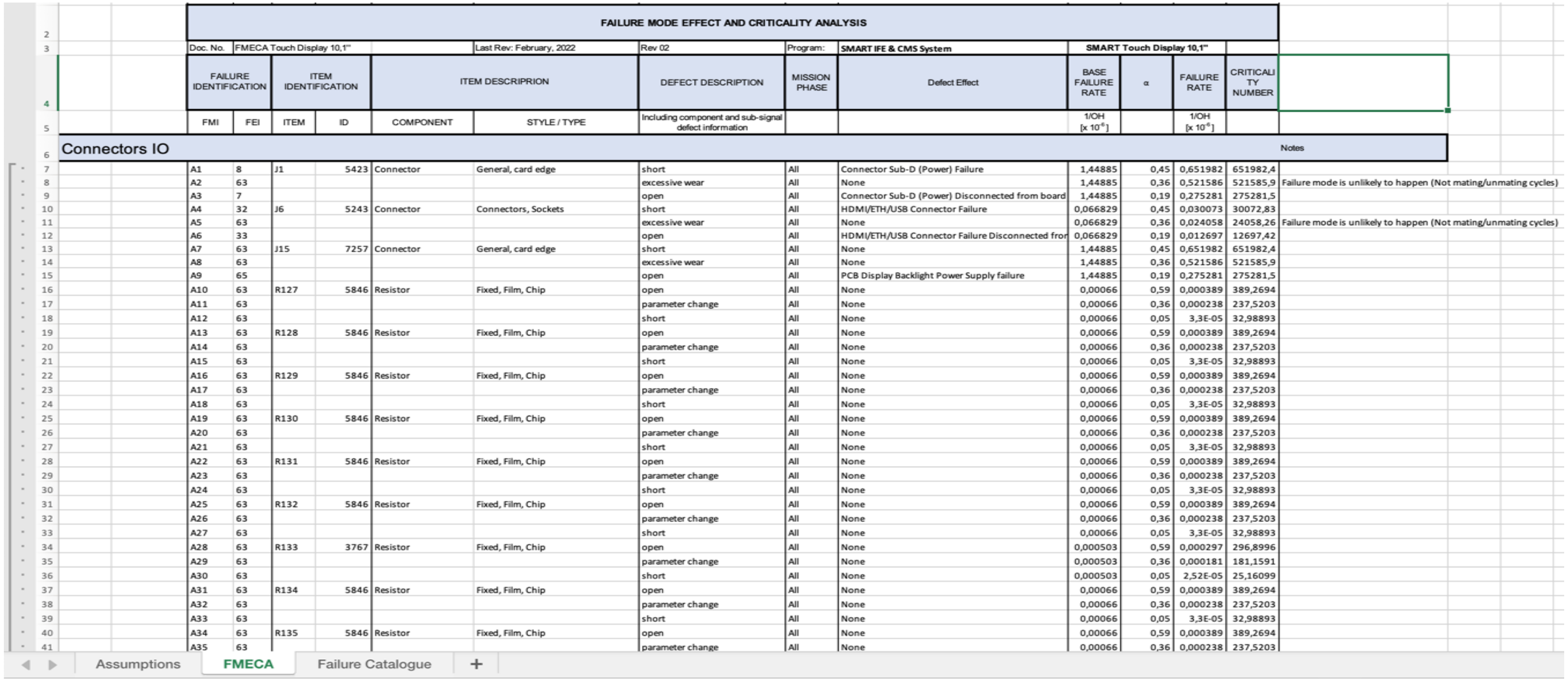
Last revision: 02/2022
Rev.02

Environmental Conditions	65° C max ARW
Functional Block	Failure Rate (fpmh)
Connectors-IO	2,970309564
Connectors-UART MNT	1,839645645
Connectors-USB MNT	3,515691188
ETH 10/100	0,313457592
CODEC	4,709060422
Analog I/O MIC	1,987282504
Analog I/O LINE	1,286271503
USB Touch Screen	3,183291361
USB External	1,734441555
HDMI MIPI Bridge IN	4,453550341
Digital Input	0,782008663
PWRIN_ Limiter & Temp	2,931965719
PWRIN_28/12	1,658156728
Power Supply DC_DC 15V	1,652156861
Power Sequencing per APALIS	4,27018158
I2C_Sensor	5,142925055
Display LVDS/Backlight	5,965329095
APALIS- LVDS interface	0,684
APALIS CSI	0,684
APALIS- Power Supply	1,952099642
APALIS - Not used	0,770347959
APALIS USB	0,684
APALIS SD1/SD2	0,684
APALIS-UART/I2S	0,684503382
APALIS CAM/UART/GPIO	0,684
APALIS Analog Audio	0,684
APALIS I2S/SPI	0,684
APALIS ETH	0,684
APALIS I2C/GPIO	0,684
INIC- MOST Network	1,635130957
INIC- Connector RX	0,919784
INIC- Connector TX	0,357381084
INIC- Power Supply	0,365772775
INIC- Power Pins	3,480131982
INIC- I2C Debug RMCK	11,96816344
INIC- programming connector	1,67638813
INIC- MLB I2S	0,004912544
INIC- USB	0,008213985
Other	296,4766188
TOTAL	**374,8511741**
MTBF (H) @65°C ARW	**2667,725405**
MTBF (H) @65°C GB	**27210,79913**

Figure 26. Summary and final ground MTBF

➢ ***Display Safety analysis***

To perform the safety analysis, we start from the reliability that we did previously. We first select each component with its relative coefficient and failure rate, then we use the Octave program to transform the reliability list in the list which is needed to fill the FMECA analysis, which is composed by the item number, its ID and description, and the defect description which in most cases can be divided in three possible types of defects: short, open or excessive wear. The job of the RAMS engineer is to describe the possible defect effect for each component and type of failure. Based on the type of defect we have different alfa coefficients, that multiplied with the failure rate coming from the reliability analysis, gives the final safety failure rate.

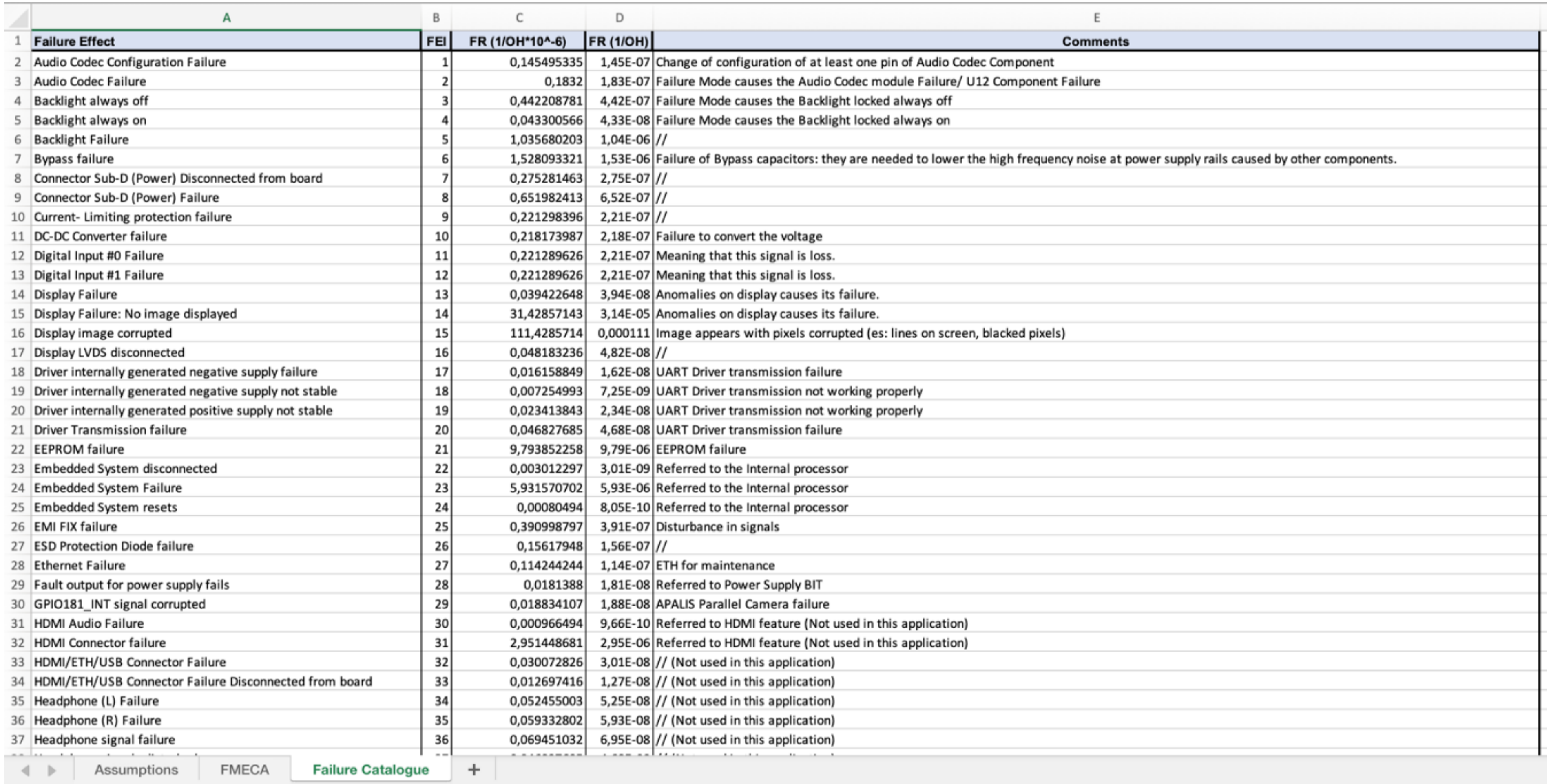


FAILURE MODE EFFECT AND CRITICALITY ANALYSIS

Doc. No.	FMECA Touch Display 10,1"				Last Rev: February, 2022	Rev 02	Program:	SMART IFE & CMS System	SMART Touch Display 10,1"				
FAILURE IDENTIFICATION		ITEM IDENTIFICATION		ITEM DESCRIPRION		DEFECT DESCRIPTION	MISSION PHASE	Defect Effect	BASE FAILURE RATE	α	FAILURE RATE	CRITICALITY NUMBER	
FMI	FEI	ITEM	ID	COMPONENT	STYLE / TYPE	Including component and sub-signal defect information			1/OH [x 10^{-6}]		1/OH [x 10^{-6}]		
Connectors IO													Notes
A1	8	J1	5423	Connector	General, card edge	short	All	Connector Sub-D (Power) Failure	1,44885	0,45	0,651982	651982,4	
A2	63					excessive wear	All	None	1,44885	0,36	0,521586	521585,9	Failure mode is unlikely to happen (Not mating/unmating cycles)
A3	7					open	All	Connector Sub-D (Power) Disconnected from board	1,44885	0,19	0,275281	275281,5	
A4	32	J6	5243	Connector	Connectors, Sockets	short	All	HDMI/ETH/USB Connector Failure	0,066829	0,45	0,030073	30072,83	
A5	63					excessive wear	All	None	0,066829	0,36	0,024058	24058,26	Failure mode is unlikely to happen (Not mating/unmating cycles)
A6	33					open	All	HDMI/ETH/USB Connector Failure Disconnected fror	0,066829	0,19	0,012697	12697,42	
A7	63	J15	7257	Connector	General, card edge	short	All	None	1,44885	0,45	0,651982	651982,4	
A8	63					excessive wear	All	None	1,44885	0,36	0,521586	521585,9	
A9	65					open	All	PCB Display Backlight Power Supply failure	1,44885	0,19	0,275281	275281,5	
A10	63	R127	5846	Resistor	Fixed, Film, Chip	open	All	None	0,00066	0,59	0,000389	389,2694	
A11	63					parameter change	All	None	0,00066	0,36	0,000238	237,5203	
A12	63					short	All	None	0,00066	0,05	3,3E-05	32,98893	
A13	63	R128	5846	Resistor	Fixed, Film, Chip	open	All	None	0,00066	0,59	0,000389	389,2694	
A14	63					parameter change	All	None	0,00066	0,36	0,000238	237,5203	
A15	63					short	All	None	0,00066	0,05	3,3E-05	32,98893	
A16	63	R129	5846	Resistor	Fixed, Film, Chip	open	All	None	0,00066	0,59	0,000389	389,2694	
A17	63					parameter change	All	None	0,00066	0,36	0,000238	237,5203	
A18	63					short	All	None	0,00066	0,05	3,3E-05	32,98893	
A19	63	R130	5846	Resistor	Fixed, Film, Chip	open	All	None	0,00066	0,59	0,000389	389,2694	
A20	63					parameter change	All	None	0,00066	0,36	0,000238	237,5203	
A21	63					short	All	None	0,00066	0,05	3,3E-05	32,98893	
A22	63	R131	5846	Resistor	Fixed, Film, Chip	open	All	None	0,00066	0,59	0,000389	389,2694	
A23	63					parameter change	All	None	0,00066	0,36	0,000238	237,5203	
A24	63					short	All	None	0,00066	0,05	3,3E-05	32,98893	
A25	63	R132	5846	Resistor	Fixed, Film, Chip	open	All	None	0,00066	0,59	0,000389	389,2694	
A26	63					parameter change	All	None	0,00066	0,36	0,000238	237,5203	
A27	63					short	All	None	0,00066	0,05	3,3E-05	32,98893	
A28	63	R133	3767	Resistor	Fixed, Film, Chip	open	All	None	0,000503	0,59	0,000297	296,8996	
A29	63					parameter change	All	None	0,000503	0,36	0,000181	181,1591	
A30	63					short	All	None	0,000503	0,05	2,52E-05	25,16099	
A31	63	R134	5846	Resistor	Fixed, Film, Chip	open	All	None	0,00066	0,59	0,000389	389,2694	
A32	63					parameter change	All	None	0,00066	0,36	0,000238	237,5203	
A33	63					short	All	None	0,00066	0,05	3,3E-05	32,98893	
A34	63	R135	5846	Resistor	Fixed, Film, Chip	open	All	None	0,00066	0,59	0,000389	389,2694	
A35	63					parameter change	All	None	0,00066	0,36	0,000238	237,5203	

Figure 27. FMECA analysis

Next, we order alphabetically the failure effects with its relative failure rate and so we obtain the failure catalogue with its additional comments. In the end, the failure catalogue is reported in the safety document which is sent to the customer that requested the safety analysis.



	A	B	C	D	E
1	**Failure Effect**	**FEI**	**FR (1/OH*10^-6)**	**FR (1/OH)**	**Comments**
2	Audio Codec Configuration Failure	1	0,145495335	1,45E-07	Change of configuration of at least one pin of Audio Codec Component
3	Audio Codec Failure	2	0,1832	1,83E-07	Failure Mode causes the Audio Codec module Failure/ U12 Component Failure
4	Backlight always off	3	0,442208781	4,42E-07	Failure Mode causes the Backlight locked always off
5	Backlight always on	4	0,043300566	4,33E-08	Failure Mode causes the Backlight locked always on
6	Backlight Failure	5	1,035680203	1,04E-06	//
7	Bypass failure	6	1,528093321	1,53E-06	Failure of Bypass capacitors: they are needed to lower the high frequency noise at power supply rails caused by other components.
8	Connector Sub-D (Power) Disconnected from board	7	0,275281463	2,75E-07	//
9	Connector Sub-D (Power) Failure	8	0,651982413	6,52E-07	//
10	Current- Limiting protection failure	9	0,221298396	2,21E-07	//
11	DC-DC Converter failure	10	0,218173987	2,18E-07	Failure to convert the voltage
12	Digital Input #0 Failure	11	0,221289626	2,21E-07	Meaning that this signal is loss.
13	Digital Input #1 Failure	12	0,221289626	2,21E-07	Meaning that this signal is loss.
14	Display Failure	13	0,039422648	3,94E-08	Anomalies on display causes its failure.
15	Display Failure: No image displayed	14	31,42857143	3,14E-05	Anomalies on display causes its failure.
16	Display image corrupted	15	111,4285714	0,000111	Image appears with pixels corrupted (es: lines on screen, blacked pixels)
17	Display LVDS disconnected	16	0,048183236	4,82E-08	//
18	Driver internally generated negative supply failure	17	0,016158849	1,62E-08	UART Driver transmission failure
19	Driver internally generated negative supply not stable	18	0,007254993	7,25E-09	UART Driver transmission not working properly
20	Driver internally generated positive supply not stable	19	0,023413843	2,34E-08	UART Driver transmission not working properly
21	Driver Transmission failure	20	0,046827685	4,68E-08	UART Driver transmission failure
22	EEPROM failure	21	9,793852258	9,79E-06	EEPROM failure
23	Embedded System disconnected	22	0,003012297	3,01E-09	Referred to the Internal processor
24	Embedded System Failure	23	5,931570702	5,93E-06	Referred to the Internal processor
25	Embedded System resets	24	0,00080494	8,05E-10	Referred to the Internal processor
26	EMI FIX failure	25	0,390998797	3,91E-07	Disturbance in signals
27	ESD Protection Diode failure	26	0,15617948	1,56E-07	//
28	Ethernet Failure	27	0,114244244	1,14E-07	ETH for maintenance
29	Fault output for power supply fails	28	0,0181388	1,81E-08	Referred to Power Supply BIT
30	GPIO181_INT signal corrupted	29	0,018834107	1,88E-08	APALIS Parallel Camera failure
31	HDMI Audio Failure	30	0,000966494	9,66E-10	Referred to HDMI feature (Not used in this application)
32	HDMI Connector failure	31	2,951448681	2,95E-06	Referred to HDMI feature (Not used in this application)
33	HDMI/ETH/USB Connector Failure	32	0,030072826	3,01E-08	// (Not used in this application)
34	HDMI/ETH/USB Connector Failure Disconnected from board	33	0,012697416	1,27E-08	// (Not used in this application)
35	Headphone (L) Failure	34	0,052455003	5,25E-08	// (Not used in this application)
36	Headphone (R) Failure	35	0,059332802	5,93E-08	// (Not used in this application)
37	Headphone signal failure	36	0,069451032	6,95E-08	// (Not used in this application)

Figure 28. Failure catalogue

Display Testability

Starting from the FMECA analysis, we take the failure catalogue with the list of failure effect and relative failure rate and we begin to write down the testability analysis.

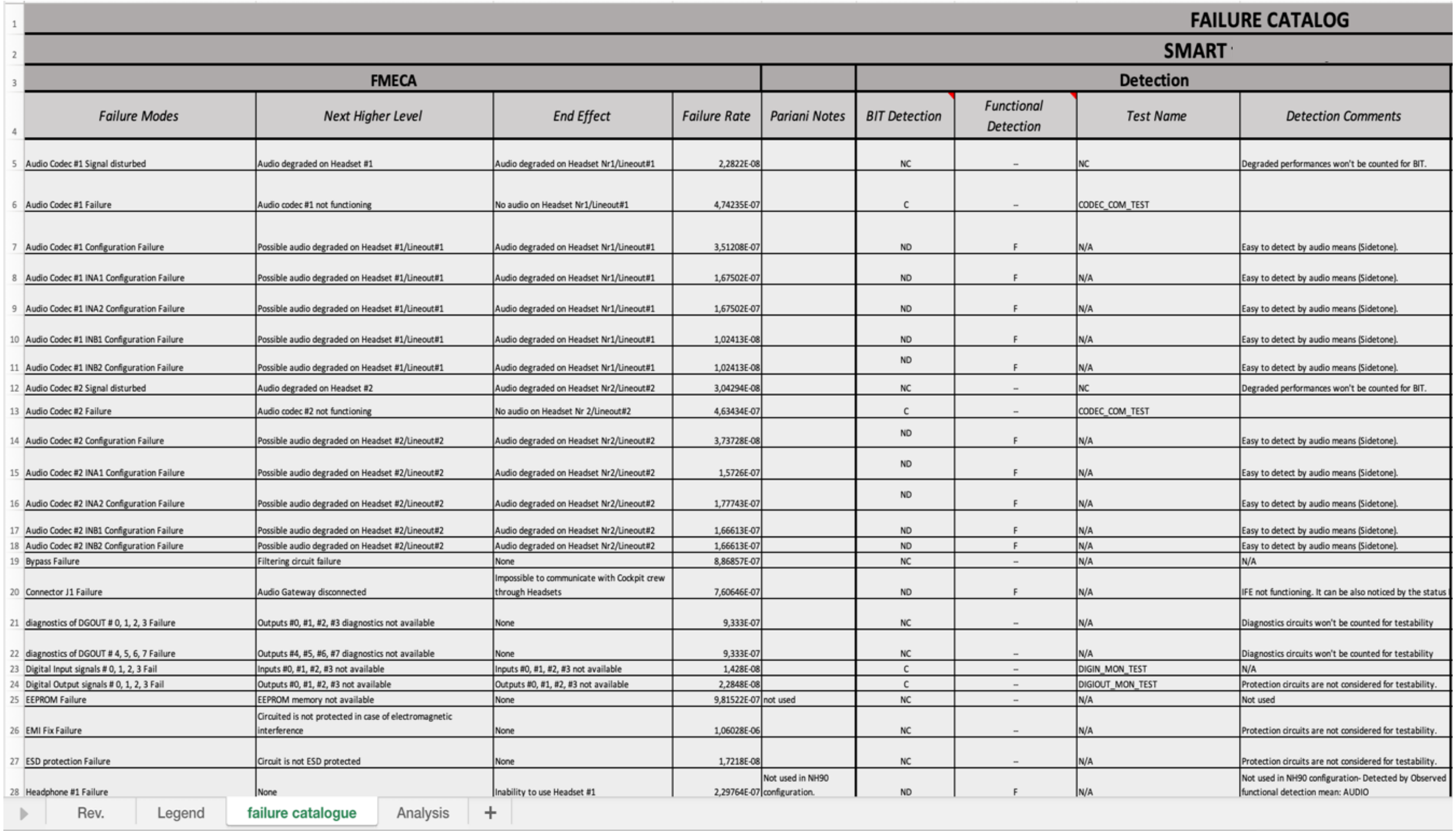
The FMECA failure effects are elevated in two level effects: the side effect and the end effect. The side effect is the nearest higher-level effect and the end effect is final level.

The end effect can be detected by continuous built-in test (CBIT), initiated built-in test (IBIT), power built-in test (PBIT), not candidate for detection (C) or candidate for detection but not detected (ND).

As we can see in figure (29), in the functional test section, it is indicated how the failure is detected. Failure can be detected in many ways, as follows:

- Failure is detected by Preflight check or postflight check (without external vision aids) – (**PF**)
- Failure is detected by a “Manual Functional” test, requiring a manual action of the operator for failure detection. The name of the functional test and the periodicity shall be given in “Detection Comments” column **–** (**H**)
- Failure is detected by a maintenance operation, requiring a manual action of the operator for failure detection. The name of the operation and the periodicity shall be given in “Detection Comments” column **–** (**M**)
- Failure is detected from “external Functional” detection means, existing or possibly developed inside external equipment/ system – (**S**)
- Failure is detectable by Observed Functional detection mean: visual, audio, sensitive means. Mean shall be given in “Detection Comments” column – (**F**)

For each detection there can be addition comments.



FAILURE CATALOG

SMART

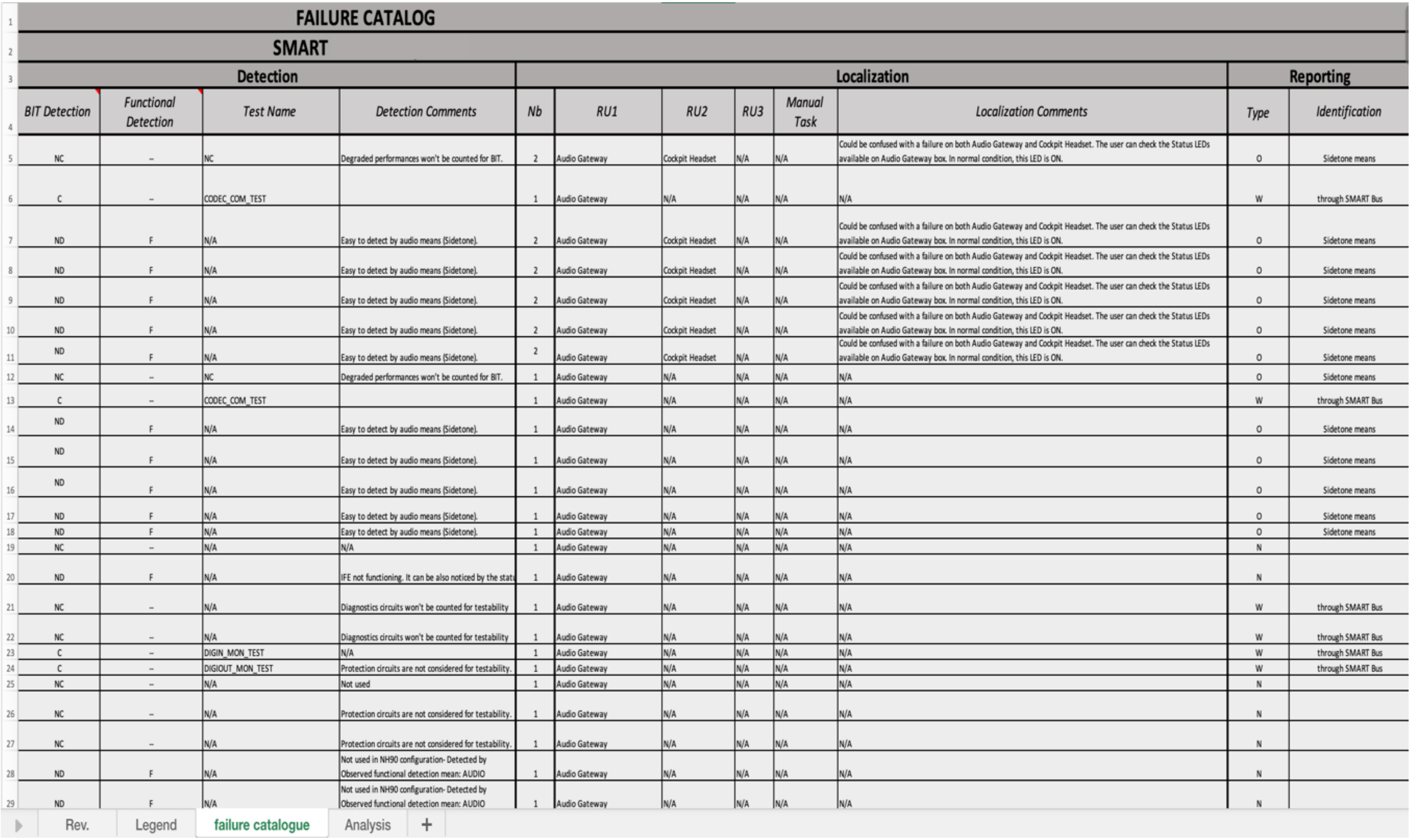
FMECA					Detection			
Failure Modes	*Next Higher Level*	*End Effect*	*Failure Rate*	*Pariani Notes*	*BIT Detection*	*Functional Detection*	*Test Name*	*Detection Comments*
Audio Codec #1 Signal disturbed	Audio degraded on Headset #1	Audio degraded on Headset Nr1/Lineout#1	2,2822E-08		NC	–	NC	Degraded performances won't be counted for BIT.
Audio Codec #1 Failure	Audio codec #1 not functioning	No audio on Headset Nr1/Lineout#1	4,74235E-07		C	–	CODEC_COM_TEST	
Audio Codec #1 Configuration Failure	Possible audio degraded on Headset #1/Lineout#1	Audio degraded on Headset Nr1/Lineout#1	3,51208E-07		ND	F	N/A	Easy to detect by audio means (Sidetone).
Audio Codec #1 INA1 Configuration Failure	Possible audio degraded on Headset #1/Lineout#1	Audio degraded on Headset Nr1/Lineout#1	1,67502E-07		ND	F	N/A	Easy to detect by audio means (Sidetone).
Audio Codec #1 INA2 Configuration Failure	Possible audio degraded on Headset #1/Lineout#1	Audio degraded on Headset Nr1/Lineout#1	1,67502E-07		ND	F	N/A	Easy to detect by audio means (Sidetone).
Audio Codec #1 INB1 Configuration Failure	Possible audio degraded on Headset #1/Lineout#1	Audio degraded on Headset Nr1/Lineout#1	1,02413E-08		ND	F	N/A	Easy to detect by audio means (Sidetone).
Audio Codec #1 INB2 Configuration Failure	Possible audio degraded on Headset #1/Lineout#1	Audio degraded on Headset Nr1/Lineout#1	1,02413E-08		ND	F	N/A	Easy to detect by audio means (Sidetone).
Audio Codec #2 Signal disturbed	Audio degraded on Headset #2	Audio degraded on Headset Nr2/Lineout#2	3,04294E-08		NC	–	NC	Degraded performances won't be counted for BIT.
Audio Codec #2 Failure	Audio codec #2 not functioning	No audio on Headset Nr 2/Lineout#2	4,63434E-07		C	–	CODEC_COM_TEST	
Audio Codec #2 Configuration Failure	Possible audio degraded on Headset #2/Lineout#2	Audio degraded on Headset Nr2/Lineout#2	3,73728E-08		ND	F	N/A	Easy to detect by audio means (Sidetone).
Audio Codec #2 INA1 Configuration Failure	Possible audio degraded on Headset #2/Lineout#2	Audio degraded on Headset Nr2/Lineout#2	1,5726E-07		ND	F	N/A	Easy to detect by audio means (Sidetone).
Audio Codec #2 INA2 Configuration Failure	Possible audio degraded on Headset #2/Lineout#2	Audio degraded on Headset Nr2/Lineout#2	1,77743E-07		ND	F	N/A	Easy to detect by audio means (Sidetone).
Audio Codec #2 INB1 Configuration Failure	Possible audio degraded on Headset #2/Lineout#2	Audio degraded on Headset Nr2/Lineout#2	1,66613E-07		ND	F	N/A	Easy to detect by audio means (Sidetone).
Audio Codec #2 INB2 Configuration Failure	Possible audio degraded on Headset #2/Lineout#2	Audio degraded on Headset Nr2/Lineout#2	1,66613E-07		ND	F	N/A	Easy to detect by audio means (Sidetone).
Bypass Failure	Filtering circuit failure	None	8,86857E-07		NC	–	N/A	N/A
Connector J1 Failure	Audio Gateway disconnected	Impossible to communicate with Cockpit crew through Headsets	7,60646E-07		ND	F	N/A	IFE not functioning. It can be also noticed by the status
diagnostics of DGOUT # 0, 1, 2, 3 Failure	Outputs #0, #1, #2, #3 diagnostics not available	None	9,333E-07		NC	–	N/A	Diagnostics circuits won't be counted for testability
diagnostics of DGOUT # 4, 5, 6, 7 Failure	Outputs #4, #5, #6, #7 diagnostics not available	None	9,333E-07		NC	–	N/A	Diagnostics circuits won't be counted for testability
Digital Input signals # 0, 1, 2, 3 Fail	Inputs #0, #1, #2, #3 not available	Inputs #0, #1, #2, #3 not available	1,428E-08		C	–	DIGIN_MON_TEST	N/A
Digital Output signals # 0, 1, 2, 3 Fail	Outputs #0, #1, #2, #3 not available	Outputs #0, #1, #2, #3 not available	2,2848E-08		C	–	DIGIOUT_MON_TEST	Protection circuits are not considered for testability.
EEPROM Failure	EEPROM memory not available	None	9,81522E-07	not used	NC	–	N/A	Not used
EMI Fix Failure	Circuited is not protected in case of electromagnetic interference	None	1,06028E-06		NC	–	N/A	Protection circuits are not considered for testability.
ESD protection Failure	Circuit is not ESD protected	None	1,7218E-08		NC	–	N/A	Protection circuits are not considered for testability.
Headphone #1 Failure	None	Inability to use Headset #1	2,29764E-07	Not used in NH90 configuration.	ND	F	N/A	Not used in NH90 configuration- Detected by Observed functional detection mean: AUDIO

Figure 29. Testability part 1

In the next section (Figure 30) we find the probable failed replaceable units involved in the localization ambiguity, divided in three level based on the failed probability.

In the end, we have the localization comments and the reporting type of the failure that can be:

- Failure is reported by discrete signal (s) – (**D**)
- Failure is reported by maintenance word(s)- SMART Bus - (**W**)
- Failure is not reported - (**N**)
- Failure is reported by discrete signal(s) and maintenance word(s) - (**DW**)
- Failure is reported by other mean (for example Sidetones) - (**O**)



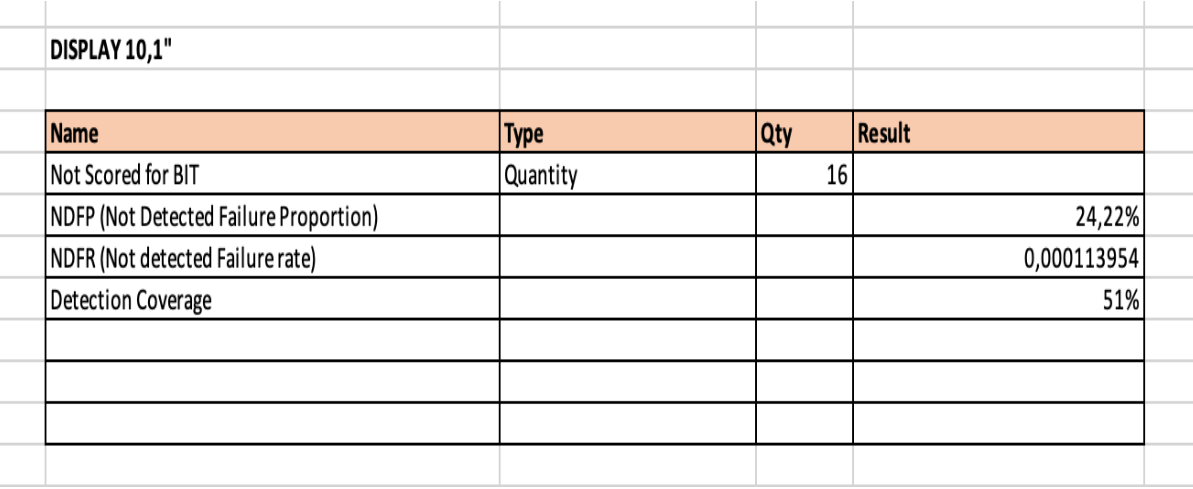
FAILURE CATALOG

SMART

	Detection				Localization						Reporting	
4	BIT Detection	Functional Detection	Test Name	Detection Comments	Nb	RU1	RU2	RU3	Manual Task	Localization Comments	Type	Identification
5	NC	–	NC	Degraded performances won't be counted for BIT.	2	Audio Gateway	Cockpit Headset	N/A	N/A	Could be confused with a failure on both Audio Gateway and Cockpit Headset. The user can check the Status LEDs available on Audio Gateway box. In normal condition, this LED is ON.	O	Sidetone means
6	C	–	CODEC_COM_TEST		1	Audio Gateway	N/A	N/A	N/A	N/A	W	through SMART Bus
7	ND	F	N/A	Easy to detect by audio means (Sidetone).	2	Audio Gateway	Cockpit Headset	N/A	N/A	Could be confused with a failure on both Audio Gateway and Cockpit Headset. The user can check the Status LEDs available on Audio Gateway box. In normal condition, this LED is ON.	O	Sidetone means
8	ND	F	N/A	Easy to detect by audio means (Sidetone).	2	Audio Gateway	Cockpit Headset	N/A	N/A	Could be confused with a failure on both Audio Gateway and Cockpit Headset. The user can check the Status LEDs available on Audio Gateway box. In normal condition, this LED is ON.	O	Sidetone means
9	ND	F	N/A	Easy to detect by audio means (Sidetone).	2	Audio Gateway	Cockpit Headset	N/A	N/A	Could be confused with a failure on both Audio Gateway and Cockpit Headset. The user can check the Status LEDs available on Audio Gateway box. In normal condition, this LED is ON.	O	Sidetone means
10	ND	F	N/A	Easy to detect by audio means (Sidetone).	2	Audio Gateway	Cockpit Headset	N/A	N/A	Could be confused with a failure on both Audio Gateway and Cockpit Headset. The user can check the Status LEDs available on Audio Gateway box. In normal condition, this LED is ON.	O	Sidetone means
11	ND	F	N/A	Easy to detect by audio means (Sidetone).	2	Audio Gateway	Cockpit Headset	N/A	N/A	Could be confused with a failure on both Audio Gateway and Cockpit Headset. The user can check the Status LEDs available on Audio Gateway box. In normal condition, this LED is ON.	O	Sidetone means
12	NC	–	NC	Degraded performances won't be counted for BIT.	1	Audio Gateway	N/A	N/A	N/A	N/A	O	Sidetone means
13	C	–	CODEC_COM_TEST		1	Audio Gateway	N/A	N/A	N/A	N/A	W	through SMART Bus
14	ND	F	N/A	Easy to detect by audio means (Sidetone).	1	Audio Gateway	N/A	N/A	N/A	N/A	O	Sidetone means
15	ND	F	N/A	Easy to detect by audio means (Sidetone).	1	Audio Gateway	N/A	N/A	N/A	N/A	O	Sidetone means
16	ND	F	N/A	Easy to detect by audio means (Sidetone).	1	Audio Gateway	N/A	N/A	N/A	N/A	O	Sidetone means
17	ND	F	N/A	Easy to detect by audio means (Sidetone).	1	Audio Gateway	N/A	N/A	N/A	N/A	O	Sidetone means
18	ND	F	N/A	Easy to detect by audio means (Sidetone).	1	Audio Gateway	N/A	N/A	N/A	N/A	O	Sidetone means
19	NC	–	N/A	N/A	1	Audio Gateway	N/A	N/A	N/A	N/A	N	
20	ND	F	N/A	IFE not functioning. It can be also noticed by the statu	1	Audio Gateway	N/A	N/A	N/A	N/A	N	
21	NC	–	N/A	Diagnostics circuits won't be counted for testability	1	Audio Gateway	N/A	N/A	N/A	N/A	W	through SMART Bus
22	NC	–	N/A	Diagnostics circuits won't be counted for testability	1	Audio Gateway	N/A	N/A	N/A	N/A	W	through SMART Bus
23	C	–	DIGIN_MON_TEST	N/A	1	Audio Gateway	N/A	N/A	N/A	N/A	W	through SMART Bus
24	C	–	DIGIOUT_MON_TEST	Protection circuits are not considered for testability.	1	Audio Gateway	N/A	N/A	N/A	N/A	W	through SMART Bus
25	NC	–	N/A	Not used	1	Audio Gateway	N/A	N/A	N/A	N/A	N	
26	NC	–	N/A	Protection circuits are not considered for testability.	1	Audio Gateway	N/A	N/A	N/A	N/A	N	
27	NC	–	N/A	Protection circuits are not considered for testability.	1	Audio Gateway	N/A	N/A	N/A	N/A	N	
28	ND	F	N/A	Not used in NH90 configuration- Detected by Observed functional detection mean: AUDIO	1	Audio Gateway	N/A	N/A	N/A	N/A	N	
29	ND	F	N/A	Not used in NH90 configuration- Detected by Observed functional detection mean: AUDIO	1	Audio Gateway	N/A	N/A	N/A	N/A	N	

Figure 30. Testability part 2

In the end the results of the testability analysis (Figure 31) are reported in the testability document which is sent to the costumer.



DISPLAY 10,1"

Name	Type	Qty	Result
Not Scored for BIT	Quantity	16	
NDFP (Not Detected Failure Proportion)			24,22%
NDFR (Not detected Failure rate)			0,000113954
Detection Coverage			51%

Figure 31. Testability results

3.3. SMART system Fault Tree Analysis (FTA)

3.3.1. Fault Tree Analysis

The purpose of FTA is to study how failure modes at one level produce critical failure modes at higher level.

FTA has been developed by building a functional block diagram based on the equipment's schematic design to break the system into its main modules with the aim of simplifying the analysis. The causes of failure can then be further investigated separately one from each other, allowing for a more detailed analysis.

The undesired event (Top Event) is analyzed using Boolean logic to combine a series of lower-level events; up to the Basic Event, which is internal to the system under analysis and requires no further development (i.e. has the capability of causing a fault to occur).

All fault trees are composed of two kinds of symbols, logic and event.

Logic symbols are used to tie together in the fault tree, their inputs and outputs should always be events; here are reported some of the most common logic symbols:

- OR gate: the output occurs if any input occurs
- AND gate: the output occurs only if all inputs occur (inputs are independent)
- Exclusive OR gate: the output occurs if exactly one input occurs.
- Priority AND gate: the output occurs if the inputs occur in a specific sequence specified by a conditioning event.
- Inhibit gate: the output occurs if the input occurs under an enabling condition specified by a conditioning event.

The event symbols can be:

- Triangle: Transfer symbols (IN, OUT). Indicates transfer of information of related fault trees, such as the FT of a subsystem to its system.
- Rectangle: contains the description of a logic symbol output or an event.
- Oval: represents a conditional event which defines a necessary condition for a failure mode to occur.
- Circle: Represent a Basic Event - Primary event no further developed
- House: Event which is external to the system under analysis, it will or will not happen. It will be represented with a trapezoid figure.
- Diamond: Event which is not developed further because it has little impact on the top-level event or because the details necessary for further event development are not readily available.

3.3.2. Evaluation for Compliance with Safety Objectives

Events in a fault tree are associated with statistical probabilities, as follows:

- An AND represents a combination of independent events. That is, the probability of any input event to an AND gate is unaffected by any other input event to the same gate,
- The probability of obtaining an outcome A is denoted by P(A), outcome B by P(B) and so on for other outcomes;
- The probability that A AND B occur is denoted by P(AB);
- The probability that A OR B occur is denoted by P(A+B);
- If A and B are two independent events with the probabilities P(A) and P(B), then the probability that both events will occur is the product given by equation (3.1) below:

$$P(AB) = P(A) * P(B) \qquad (3.1)$$

- If A, B and C are three independent events with the probabilities P(A), P(B) and P(C), then the probability that all three events will occur is the product given by equation (3.2) below:

$$P(ABC) = P(A) * P(B) * P(C) \qquad (3.2)$$

- If the two independent events can occur simultaneously, the probability that either A OR B or both A AND B will occur is given by equation (3.3) below:

$$P(A + B) = P(A) + P(B) - (P(A) * P(B)) \qquad (3.3)$$

- If the three independent events can occur simultaneously, the probability that A OR B OR C, or any combination of these three will occur is given by equation (3.4) below:

$$P(A + B + C) = P(A) + P(B) + P(C) - (P(A) * P(B)) - (P(A) * P(C)) - (P(B) * P(C)) + (P(A) * P(B) * P(C)) \qquad (3.4)$$

- If the two events are mutually exclusive so that when one occurs the other cannot occur, the equation for a two input OR-gate simplifies to:

$$P(A + B) = P(A) + P(B); \quad P(AB) = 0$$

The probability of failure can be estimated as the following equation (3.5):

$$P_f = 1 - e^{-\lambda t} \qquad (3.5)$$

Where λ is the Failure Rate and t is the Period of time (OH).

Note that fault tree method can be applied beginning in the early design phase, and progressively refined and updated to track the probability of undesirable event as the design evolves. Initial fault tree diagrams might represent functional blocks (units, equipment, etc.), becoming more definitive at lower levels as the design materializes in the form of specific parts.

3.3.3. Undesired Events

Function	Ref. of UE	Undesired event	Severity (safety)	Mission impact (Reliability)	Occurrence rate (/FH)	Comments
To provide passengers with cabin environment management	UE01	Loss or degradation of lighting management	Minor	no	10E-3	Cabin lighting management by IFE is superseded by command in Cockpit**
To provide passengers with cabin environment management	UE02	Loss of windows shading command capabilities	Minor	no	10E-3	Windows shading management by IFE is superseded by command in cockpit**.
To provide passengers with cabin environment management	UE03	Spurious command of change of shading level of windows	Minor	no	10E-3	Windows shading management by IFE is superseded by command in cockpit**.
To provide passengers with cabin environment management	UE04	Loss or degradation of air conditioning in cabin management	Minor	no	10E-3	Temperature in cabin increases.
To provide passengers Passenger Address	UE05	Loss of intercommunication between cockpit and cabin	Minor	no	10E-3	This situation can lead to slight increase of crew workload to recover a normal communication between cockpit and cabin.

Table 18. Undesired events

➢ ***Undesired event 01 (UE01)***

Function	Ref. of UE	Undesired event	Severity (safety)	Mission impact (Reliability)	TARGET Occurrence rate (/FH)	Actual Occurrence rate (/OH)
To provide passengers with cabin environment management	UE01	Loss or degradation of lighting management	MIN*	no	10E-3	6,51E-04

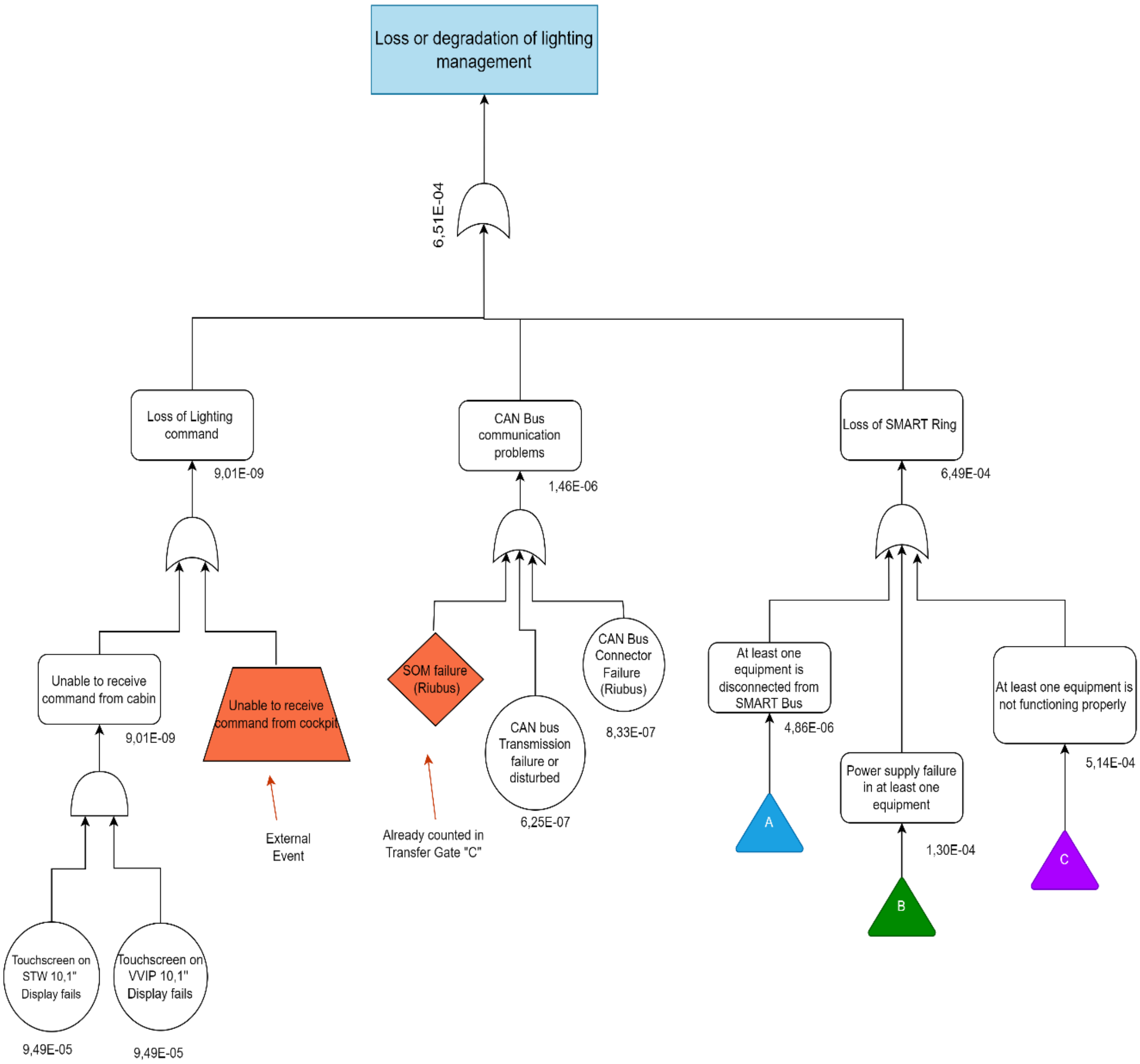

Loss or degradation of lighting management
6,51E-04
Loss of Lighting command
9,01E-09
CAN Bus communication problems
1,46E-06
Loss of SMART Ring
6,49E-04
Unable to receive command from cabin
9,01E-09
Unable to receive command from cockpit
External Event
SOM failure (Riubus)
Already counted in Transfer Gate "C"
CAN bus Transmission failure or disturbed
6,25E-07
CAN Bus Connector Failure (Riubus)
8,33E-07
At least one equipment is disconnected from SMART Bus
4,86E-06
A
Power supply failure in at least one equipment
1,30E-04
B
At least one equipment is not functioning properly
5,14E-04
C
Touchscreen on STW 10,1" Display fails
9,49E-05
Touchscreen on VVIP 10,1" Display fails
9,49E-05

Figure 32. FTA of UE01: "Loss or degradation of lighting management"

The Top Event UE01 can be caused by tree main events:

- Loss of lighting Command;
- CAN Bus communication problems;
- Loss of SMART Ring.

The “Loss of lighting command” defect effect can be caused by the failure of the window command. This command is present in both Cabin and Cockpit:

- “***Unable to receive command from cockpit***”: this event is external to the IFE system, and depends on H/C field (for example, from MTC.).
  Or:
- “***Unable to receive command from cabin***”: This event is related to the command displays available for the STW and VVIP, where they can manage many lights types. For this reason, this defect effect can take place if both of the following are true:
  - Touchscreen on STW 10,1” Display fails,
  - Touchscreen on VVIP 10.1” Display fails.

If both touchscreens are not functioning properly, the user cannot manage the lighting.

The Cabin lighting management by SMART IFE CMS is superseded by command in cockpit, and this action is seen by the “Riubus” box, which acquires this action through CAN Bus. The Can Bus failure is analyzed in another branch of the tree, as follows:

The “***CAN Bus communications problems***” may happen if at least one of the following events takes place:

- “SOM failure (Riubus)”: This is referred to the internal processor on the Riubus box, which is used to execute the services that communicate with ARINC429, CAN Bus, etc. Given the importance of this component, it was preferred to include this failure event under “Riubus Failure”, which is another branch of this tree. Ref. to Transfer Gate C.
- “CAN Bus transmission failure or disturbed”: This is referred to CAN Bus signal interrupted or disturbed due to a failure of a component in series or the CAN Bus transceiver failure.
- “CAN Bus connector failure” this is related to the failure of the connector J4 of Riubus. (J4 used for ARINC429, CAN Bus in this application).

The “***Loss of SMART Ring***” is considered to be the most critical defect effect, because it causes the failure of the entire IFE and CMS.

- ***Transfer Gate A***

EVENT: “At least one equipment is disconnected from SMART Bus”: As explained above, this is related to the Connectors of SMART Ring, including its mating connector. Based events inside circles are related to the Failures of FMECA Catalogue, and are not further analyzed. In case of multiple equipment performing similar functions, for example, four Dual Headsets, the Probability of occurrence of the combination of basic events is multiplied by four.

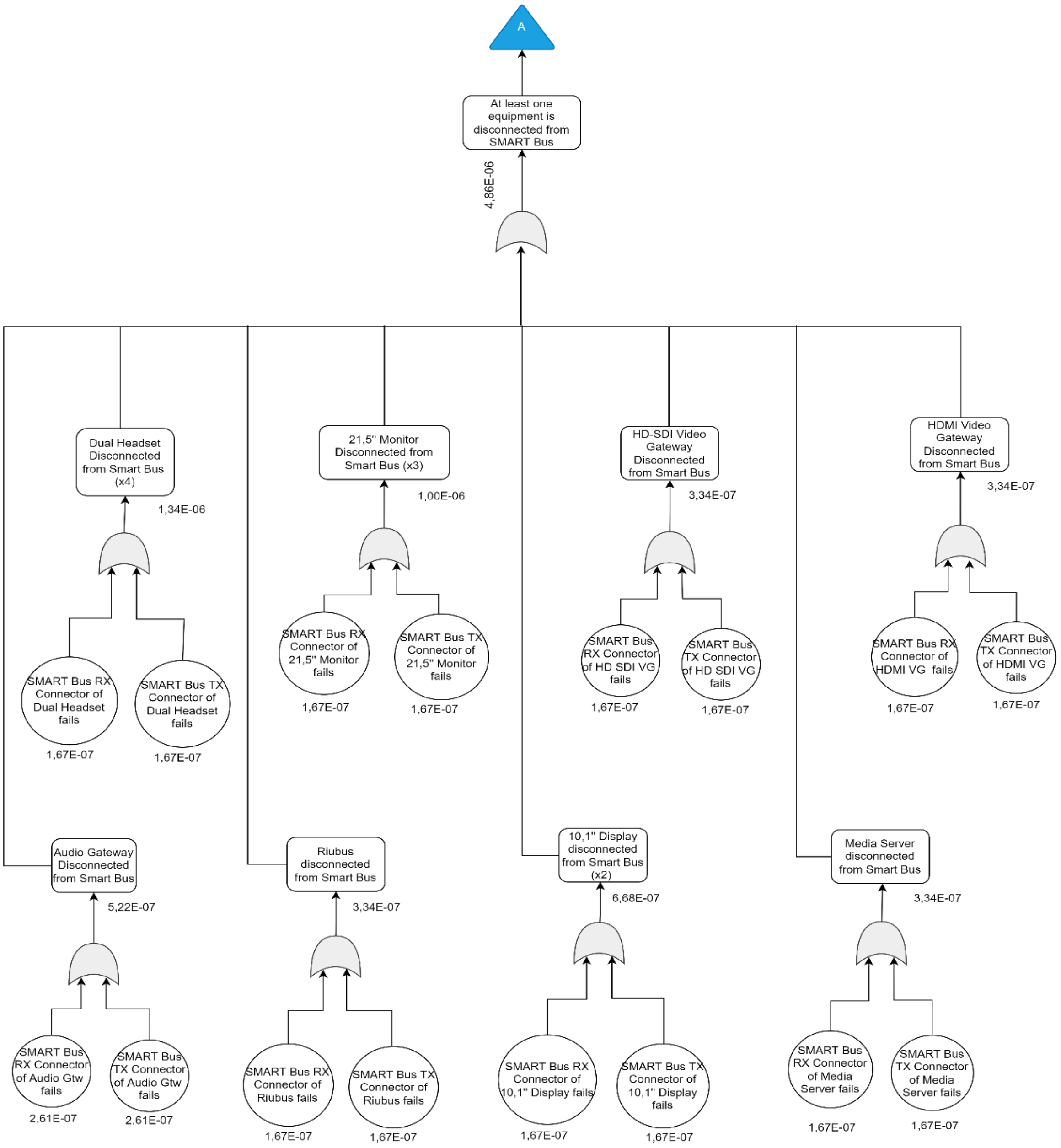

A
At least one equipment is disconnected from SMART Bus
4,86E-06
Dual Headset Disconnected from Smart Bus (x4)
1,34E-06
SMART Bus RX Connector of Dual Headset fails
1,67E-07
SMART Bus TX Connector of Dual Headset fails
1,67E-07
21,5" Monitor Disconnected from Smart Bus (x3)
1,00E-06
SMART Bus RX Connector of 21,5" Monitor fails
1,67E-07
SMART Bus TX Connector of 21,5" Monitor fails
1,67E-07
HD-SDI Video Gateway Disconnected from Smart Bus
3,34E-07
SMART Bus RX Connector of HD SDI VG fails
1,67E-07
SMART Bus TX Connector of HD SDI VG fails
1,67E-07
HDMI Video Gateway Disconnected from Smart Bus
3,34E-07
SMART Bus RX Connector of HDMI VG fails
1,67E-07
SMART Bus TX Connector of HDMI VG fails
1,67E-07
Audio Gateway Disconnected from Smart Bus
5,22E-07
SMART Bus RX Connector of Audio Gtw fails
2,61E-07
SMART Bus TX Connector of Audio Gtw fails
2,61E-07
Riubus disconnected from Smart Bus
3,34E-07
SMART Bus RX Connector of Riubus fails
1,67E-07
SMART Bus TX Connector of Riubus fails
1,67E-07
10,1" Display disconnected from Smart Bus (x2)
6,68E-07
SMART Bus RX Connector of 10,1" Display fails
1,67E-07
SMART Bus TX Connector of 10,1" Display fails
1,67E-07
Media Server disconnected from Smart Bus
3,34E-07
SMART Bus RX Connector of Media Server fails
1,67E-07
SMART Bus TX Connector of Media Server fails
1,67E-07

Figure 33. Sub-tree for Transfer Gate A

- ***Transfer Gate B***

Event: “Power Supply Failure in at least one equipment”.

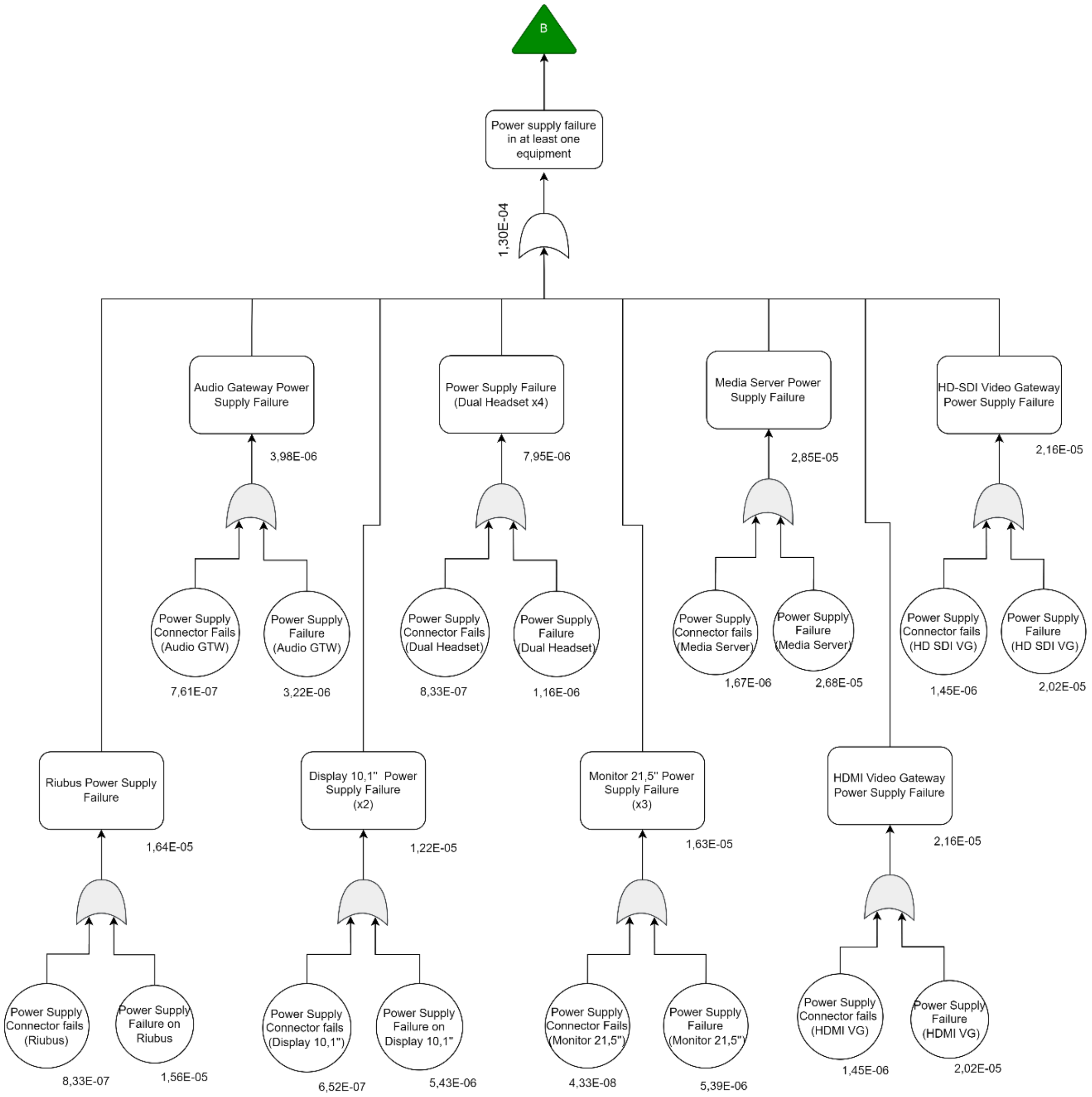

B
Power supply failure in at least one equipment
1,30E-04
Audio Gateway Power Supply Failure
3,98E-06
Power Supply Connector Fails (Audio GTW)
7,61E-07
Power Supply Failure (Audio GTW)
3,22E-06
Power Supply Failure (Dual Headset x4)
7,95E-06
Power Supply Connector Fails (Dual Headset)
8,33E-07
Power Supply Failure (Dual Headset)
1,16E-06
Media Server Power Supply Failure
2,85E-05
Power Supply Connector fails (Media Server)
1,67E-06
Power Supply Failure (Media Server)
2,68E-05
HD-SDI Video Gateway Power Supply Failure
2,16E-05
Power Supply Connector fails (HD SDI VG)
1,45E-06
Power Supply Failure (HD SDI VG)
2,02E-05
Riubus Power Supply Failure
1,64E-05
Power Supply Connector fails (Riubus)
8,33E-07
Power Supply Failure on Riubus
1,56E-05
Display 10,1" Power Supply Failure (x2)
1,22E-05
Power Supply Connector fails (Display 10,1")
6,52E-07
Power Supply Failure on Display 10,1"
5,43E-06
Monitor 21,5" Power Supply Failure (x3)
1,63E-05
Power Supply Connector Fails (Monitor 21,5")
4,33E-08
Power Supply Failure (Monitor 21,5")
5,39E-06
HDMI Video Gateway Power Supply Failure
2,16E-05
Power Supply Connector fails (HDMI VG)
1,45E-06
Power Supply Failure (HDMI VG)
2,02E-05

Figure 34. Sub-tree for Transfer Gate B

- ***Transfer Gate C***

Event: “At least one equipment is not functioning properly”.

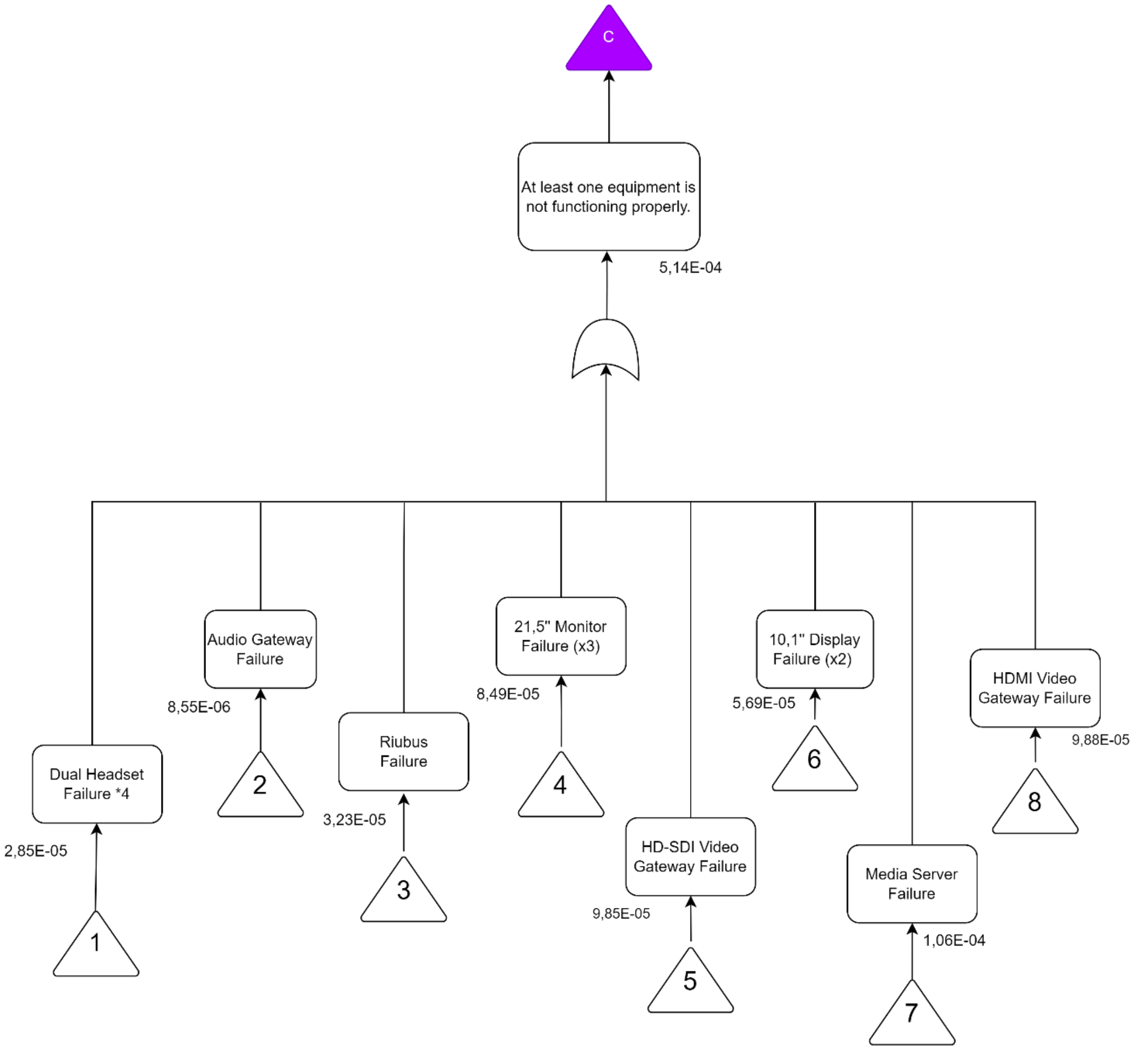


Figure 35. Sub-tree for Transfer Gate C

Each equipment is composed by different components, even if the architecture is the same.

For simplicity, the number of basic events in the failure catalogue of FMECA for each equipment have been grouped in no-more than three Root Causes.

➢ ***Undesired event 02 (UE02)***

Function	Ref. of UE	Undesired event	Severity (safety)	Mission impact (Reliability)	TARGET Occurrence rate (/FH)	Actual Occurrence rate (/OH)
To provide passengers with cabin environment management	UE02	Loss of windows shading command capabilities	MIN*	no	10E-3	6,51E-04

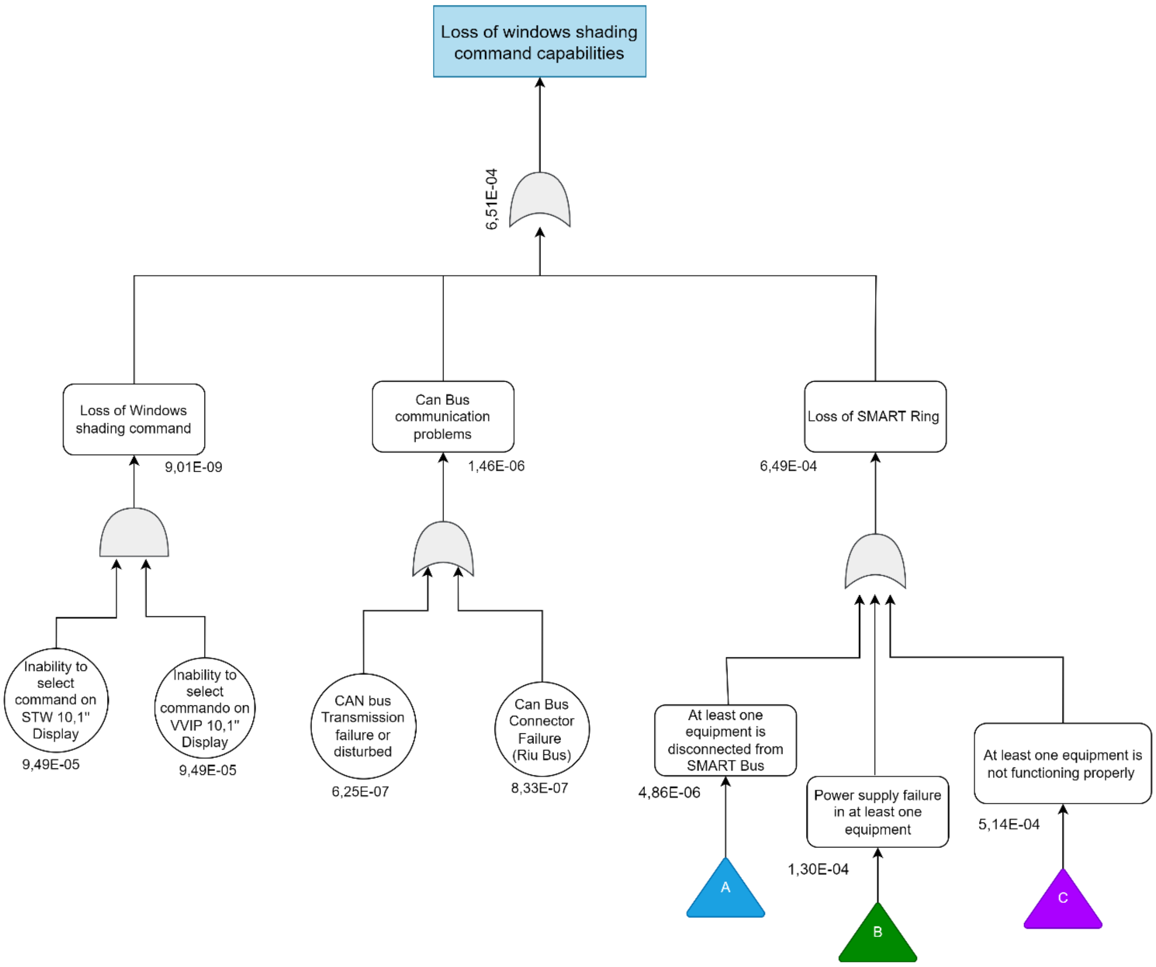

Loss of windows shading command capabilities
6,51E-04
Loss of Windows shading command
9,01E-09
Can Bus communication problems
1,46E-06
Loss of SMART Ring
6,49E-04
Inability to select command on STW 10,1" Display
9,49E-05
Inability to select commando on VVIP 10,1" Display
9,49E-05
CAN bus Transmission failure or disturbed
6,25E-07
Can Bus Connector Failure (Riu Bus)
8,33E-07
At least one equipment is disconnected from SMART Bus
4,86E-06
Power supply failure in at least one equipment
1,30E-04
At least one equipment is not functioning properly
5,14E-04
A
B
C

Figure 36. FTA of UE02: "Loss of windows shading command capabilities"

For UE02, the failure tree is very similar to UE01: same equipment that controls the same functionalities for cabin management.

- ***Undesired event 03 (UE03)***

Function	Ref. of UE	Undesired event	Severity (safety)	Mission impact (Reliability)	TARGET Occurrence rate (/FH)	Actual Occurrence rate (/OH)
To provide passengers with cabin environment management	UE03	Spurious command of change of shading level of windows.	MIN*	no	10E-3	3,96E-04

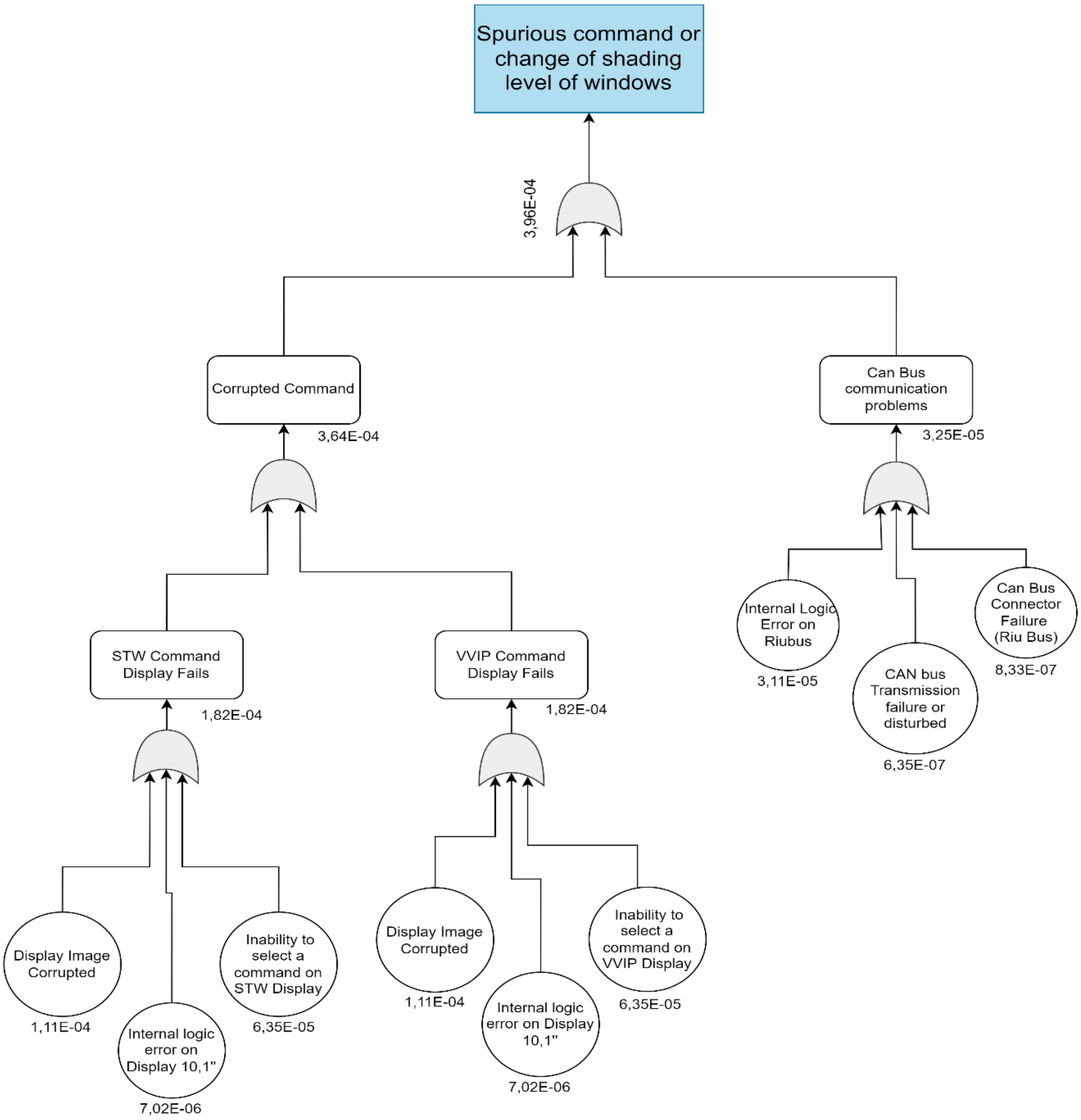

Spurious command or change of shading level of windows
3,96E-04
Corrupted Command
3,64E-04
Can Bus communication problems
3,25E-05
STW Command Display Fails
1,82E-04
VVIP Command Display Fails
1,82E-04
Internal Logic Error on Riubus
3,11E-05
CAN bus Transmission failure or disturbed
6,35E-07
Can Bus Connector Failure (Riu Bus)
8,33E-07
Display Image Corrupted
1,11E-04
Internal logic error on Display 10,1"
7,02E-06
Inability to select a command on STW Display
6,35E-05
Display Image Corrupted
1,11E-04
Internal logic error on Display 10,1"
7,02E-06
Inability to select a command on VVIP Display
6,35E-05

Figure 37. FTA of UE03: “Spurious command of change of shading level of windows”

The Top Event “Spurious command or change of shading level of windows” can be caused by at least one of the following:

- “Corrupted Command”, referring to the commands in the windows page available on 10,1 Displays;
- “Can Bus communication problems”, referring to the CAN Bus interface in Riubus box.

“Corrupted Command” defect effect can be caused by any defect in the 10,1 display, available for the STW or VVIP:

- Display image corrupted,
- Internal logic error on display 10.1’’;
- Inability to select a command on STW command. (or VVIP Command).

“CAN Bus Communication problems can be caused by:

- “Internal logic error on Riubus”, which is the box that allows to interface with the CAN Bus and manages the low-level communication.
- “CAN Bus transmission failure or disturbed”,
- “CAN Bus Connector Failure”, which is located on Riubus box.

- ***Undesired event 04 (UE04)***

Function	Ref. of UE	Undesired event	Severity (safety)	Mission impact (Reliability)	TARGET Occurrence rate (/FH)	Actual Occurrence rate (/OH)
To provide passengers with cabin environment management	UE04	Loss or degradation of air conditioning in cabin management	MIN*	no	10E-3	6,51E-04

This top event can be caused by:

- “Loss of air conditioning command”: Related to the commands from cabin and from cockpit, which is an external event, no further analyzed.
- “CAN Bus communication problems”, explained in previous fault trees
- “Loss of SMART Ring”

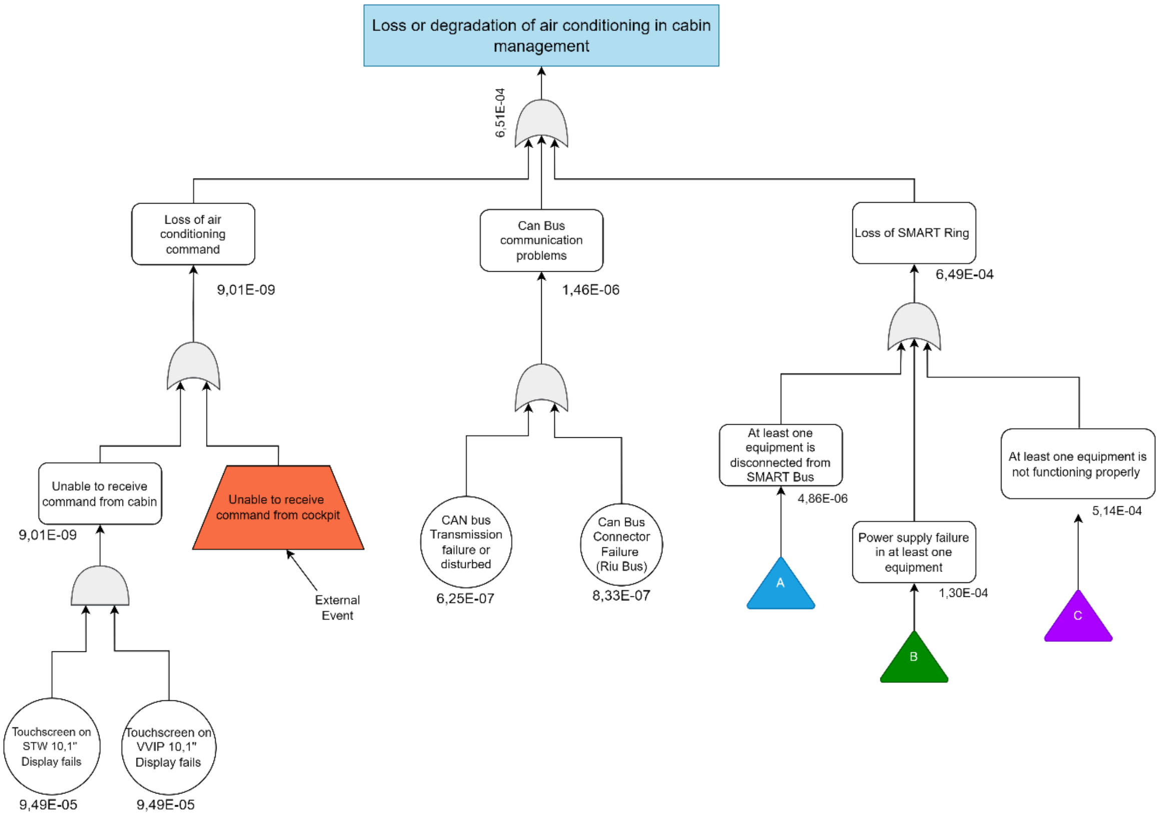

Loss or degradation of air conditioning in cabin management
6,51E-04
Loss of air conditioning command
9,01E-09
Can Bus communication problems
1,46E-06
Loss of SMART Ring
6,49E-04
Unable to receive command from cabin
9,01E-09
Unable to receive command from cockpit
External Event
CAN bus Transmission failure or disturbed
6,25E-07
Can Bus Connector Failure (Riu Bus)
8,33E-07
At least one equipment is disconnected from SMART Bus
4,86E-06
A
Power supply failure in at least one equipment
1,30E-04
B
At least one equipment is not functioning properly
5,14E-04
C
Touchscreen on STW 10,1" Display fails
9,49E-05
Touchscreen on VVIP 10,1" Display fails
9,49E-05

Figure 38. FTA of UE05: “Loss or degradation of air conditioning in cabin management”

➢ ***Undesired event 05 (UE05)***

Function	Ref. of UE	Undesired event	Severity (Safety)	TARGET Occurrence rate (/FH)	Actual Occurrence rate (/OH)
To provide passengers Passenger Address	UE05	**Loss of intercommunication between cockpit and cabin**	MIN	10E-3	6,67E-04

Top Event UE08 can be caused by:

- ➢ Loss of Smart Ring, discussed in previous fault trees:
- ➢ Audio Codec Failure, which can be caused by;
  - Audio Connection on Dual Headsets fail: It has been considered the “OR” Gate, meaning “at least one” of the dual headsets, to make the analysis more conservative: losing one Dual Headset audio connection, means that two of the passengers are not able to hear communication from cockpit.
  - Audio Connection on Audio Gateway fails: Audio Gateway is the box that allows to interface the system with ICS.

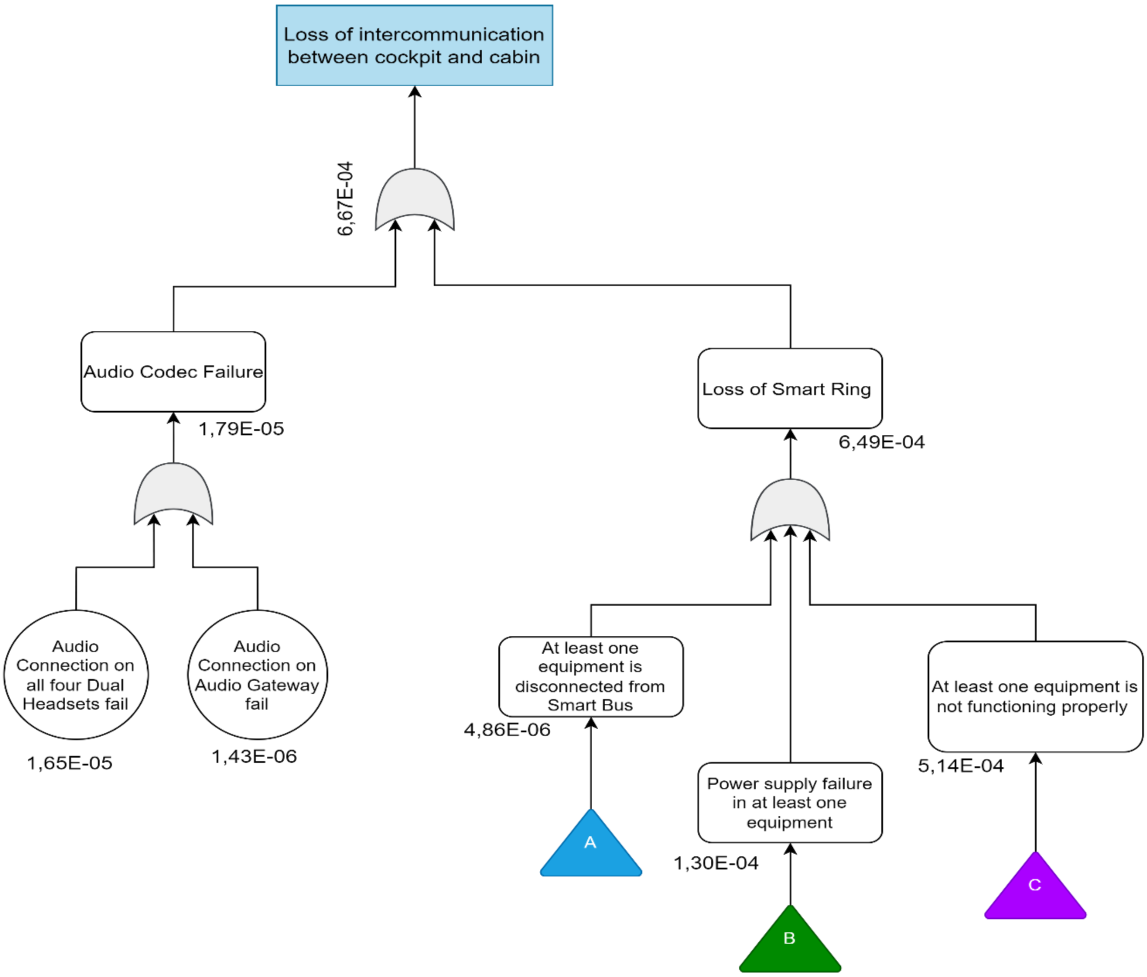

Loss of intercommunication between cockpit and cabin
6,67E-04
Audio Codec Failure
1,79E-05
Loss of Smart Ring
6,49E-04
Audio Connection on all four Dual Headsets fail
1,65E-05
Audio Connection on Audio Gateway fail
1,43E-06
At least one equipment is disconnected from Smart Bus
4,86E-06
Power supply failure in at least one equipment
1,30E-04
At least one equipment is not functioning properly
5,14E-04
A
B
C

Figure 39. FTA of UE05: “Loss of intercommunication between cockpit and cabin”

3.3.4. Considerations

The actual occurrence rates of the undesired events respect the target occurrence rates, so the analysis results in compliance.

The most critical module is the main SMART Bus ring, as its failure causes the failure of the entire system (CCF). In this event, it has been taken into account three main failures that may happen to each equipment:

- “INIC” System Failure: It is the heart of each box;
- “Power Supply Failure”: It is linked to the supply of each equipment but also to the internal electronics of each box, which is important for ensuring correct operation. For the Dual Headset Gateway, as it receives the Power from the SMART Bus signal, it corresponds to the Power Supply module which is used to adapt the power supply from the SMART Bus signal to be available to provide supply to the INIC Card. When available, this event includes the power supply connector.
- SMART Bus Connectors: includes the mating connector.

4 Conclusion and future developments

The objective of this thesis is to discuss new updated RAMS estimation models and possible future developments using new technologies.

Globally the available models have the following shortcomings:

- Limited because affected by uncertainties;
- No new technologies considered;
- Based on obsolete statistical data.

Aerospace and defense systems are becoming progressively more complex. It is increasingly difficult to understand how they will perform and when or why they might fail. Meeting these safety and reliability needs requires better analysis fidelity to support the design process. This means moving away from spreadsheets and manual analysis methods. It means digitizing the RAMS process.

Where operational availability and cost of ownership are critical determinants of success, organizations developing and managing complex, safety, or mission-critical systems understand the importance of the RAMS function.

Companies need to recognize the impact of a digital transformation on RAMS and what it potentially means for their current way of doing business. It is essential to validate how a model-based approach that digitizes the RAMS function can generate significant and demonstrable product and process benefits.

RAMS Digitalization system (RAMS-D) will shorten the time needed to perform RAMS analyses and product qualification testing. This method will ensure robust and reliable products with fast Time to Market. From analyzing the time spent on doing RAMS analyses, it was found that more than 50% of the time is spent on collecting product data and preparing it for the RAMS analyses. This digitalization system reduces the time spent for creating and standardizing the data. The digital model includes templates that are plugged into the designer CAD system, IEC standards that standardize the data such as ICD Interface Control Document and new processes on how to create the data. This method will help designers from different organizations to generate data in the same format for RAMS analyses. This new method was implemented during one year in an aerospace company successfully.

Moreover, here are five reasons to apply a model-based approach to RAMS analysis:

1. ***System complexity***

- With the inexorably increasing complexity of modern engineering systems, traditional manual methods are no longer practical or realistic. They may not identify and analyze potential technical risk in a design configuration and then build it into a tool. However, if you do not efficiently identify and mitigate potential technical risks during the design process, you cannot efficiently design, certify, manufacture or support the system.

2. ***Distributed organization structures***

- The pandemic, industry acceptance of segmented design responsibility and the cost benefits of smart working have accelerated the trend towards work environments where an engineer may not be physically together with colleagues. Successful organizations require technology to ensure that data, analytical methods and processes are consistent, reliable and efficient when used in a distributed work environment.

3. ***Digital domain knowledge***

- In a distributed environment, it is essential to acquire and then leverage efficiently team's knowledge and experience, which is a high-value intangible asset. The ability to integrate domain knowledge into a model-driven RAMS solution is critical in industries where there is an experience gap in the age profile of the team, as well as for long-running programs to communicate design intent and decision-making inputs.

4. ***Digital transformation***

- All aspects of a process must be digital to fully benefit from digital transformation. In case a model-based approach to RAMS is not introduce, it will reduce the overall potential benefits of a digital transformation project and these potential negative impacts increase proportionally with system complexity.

5. ***Cost benefits and ROI (Return on Investment)***

- Demonstrable cost, schedule and technical benefits can be achieved if organizations apply a model-based approach to RAMS. The specific return on investment and the expected payback period will vary based on the specific circumstances of an organization. The cost-benefit analysis should reflect the potential cost advantages in the design process through automation, reducing resource or scheduling costs for reliability analyses, and during operations through increased system reliability leading to lower maintenance requirements and lower cost of ownership.

Additional benefits of digitalizing RAMS process

- In the drive towards Industry 4.0, stages of the engineering design process are digitized to move beyond increased productivity towards greater agility, real-time opportunity, development of innovative capability and true innovation.
  However, to take full advantage of this trend, organizations must consider the entire product lifecycle management (PLM) process and ensure that every stage is digitized, including the RAMS function. The PLM process is a critical component in designing increasingly complex systems and leveraging critical data on asset operation and field performance.

For more information about the digitalization model, consult bibliography reference [16].

In addition to the digitalizing model, four different innovative methods to improve RAMS analysis, will be discussed:

- Improvement of reliability prediction models
- Predictive maintenance systems under industry 4.0
- DevOps for Airborne Software
- Integrated Deterministic and Probabilistic Safety Assessment

4.1. Improvement of reliability prediction models

For more information about this section, consult bibliography reference [17].

- ***Uncertainty in Traditional Approach Estimates***

Reliability predictions have been used successfully as a reliability-engineering tool for five decades, but represent only one element of a well-structured reliability program and, to be effective, they must be complemented by other elements. The premise of traditional methods such as MIL-HDBK-217F [6] is that the failure rate is primarily determined by the technology and application stress of the components comprising the system. This was a good premise when components exhibited higher failure rates and systems were not as complex as they are today. Increased system complexity and component quality have resulted in a shift of system failure causes away from components to more system-level factors, including system requirements, and interface and software problems. A significant number of failures also stem from non-component causes such as defects in design and manufacturing. Historically, these factors have not been explicitly addressed in prediction methods.

Therefore, there is a need for a reliability assessment technique that can be used to estimate the reliability of systems in the field. A viable assessment methodology needs:

- Updated component reliability prediction models, since MIL-HDBK- 217 [6] has not been updated
- A methodology for quantifying the impact that non-component effects have on system reliability
- To be useable by typical reliability engineers with data that is readily available during the system development process

- ***217Plus model***

In response to this need, the Reliability Information Analysis Center (RIAC) developed the PRISM software tool, initially released in 1999, for estimating the failure rate of electronic systems. This methodology included new component reliability prediction models and a methodology for assessing the reliability of systems due to non-component variables. The system assessment methodology was developed as part of an Air Force study performed by the RIAC and Performance Technology in which the intent was to overcome some of the perceived limitations of MIL-HDBK-217 [6]. 217Plus [17] is the next generation model of the PRISM tool, a reliability prediction methodology developed by the RIAC that includes a much more comprehensive set of component models than its PRISM predecessor.

The approach used to develop the 217Plus [17] methodology was to:

1. quantify the uncertainty in predictions using "component-based" traditional approaches.
2. explicitly model the factors contributing to that uncertainty.

Data was collected on systems for which both predicted and observed MTBF data was available. This was done for the purpose of quantifying the uncertainty in traditional component-based predictions.

The purpose of 217Plus [17] methodology is to provide an engineering tool to assess the reliability of electronic systems. Also, the methodology allows the user to estimate the failure rate of parts, assemblies and systems.

The 217Plus [17] methodology is structured to allow the user the ability to estimate the reliability of a system in the initial design stages when little is known about the system. For example, early in the development phase of a system, a reliability estimate can be made based on a generic parts list, using default values for operational profiles and stresses.

An initial estimate of a system failure rate is based on a combination of the 217Plus [17] component failure rate models developed by RIAC, the empirical field failure rate data contained in the RIAC databases, or user-defined failure rates entered directly by the user. This initial failure rate is then used as a seed value that represents a typical failure rate for the system. It is then adjusted in accordance with the process grading factors, infant mortality characteristics, reliability growth characteristics, and environmental stresses.

As additional information becomes available, the model allows the incremental addition of empirical test and field data to supplement the initial prediction.

The methodology allows modification of a base reliability estimate using process grading factors for the following failure causes:

- Parts - Failures resulting from a part (i.e., microcircuit, transistor, resistor, connector, etc.) failing to perform its intended function.
- Design - Failures resulting from an inadequate design. Examples are tolerance stack-up, unanticipated logic conditions, a non-robust design for given environmental stresses, etc.
- Manufacturing - Failures resulting from anomalies in the manufacturing process, i.e., faulty solder joints, inadequate wire routing resulting in chafing, bent connector pins, etc.
- System Management - Failures traceable to faulty interpretation of system requirements, or failure to provide the resources required to design and build a reliable system.
- Wear out - Failures resulting from wear out related failure mechanisms. Examples of components exhibiting wear out related failure mechanisms are electrolytic capacitors, solder joints, tubes, switch and relay contacts.
- No defect - Perceived failures that cannot be reproduced upon further testing. These may or may not be an actual failure; however, they are removals and, therefore, count toward the logistic failure rate.

- Induced - Failures resulting from an externally applied stress. Examples are electrical overstress and maintenance-induced failures (i.e., dropping, bending pins, etc.).
- Software - Failures of a system to perform its intended function due to the manifestation of a software fault.

These process grades correspond to the degree to which an organization has been taken actions necessary to mitigate the occurrence of system failure due to these failure categories.

Features of process grading methodology are that it:

- Explicitly recognizes and accounts for special, assignable cause problems.
- Models reliability from the user or total system level perspective.
- Promotes cross-organizational commitment to Reliability, Availability and Maintainability (RAM).
- Quantitatively grades developers' efforts to affect improved reliability.
- Maintains continuing organizational focus on RAM throughout the development cycle.

Once the base estimate is modified with the process grades, the reliability estimate is further modified by empirical data taken throughout system development and testing. This modification is accomplished using Bayesian techniques that apply the appropriate weights for the different data elements.

Advantages of the 217Plus [17] methodology over its predecessors are that it uses all available information to form the best estimate of field reliability, it is tailorable, it has quantifiable confidence bounds, and it has sensitivity to the predominant system reliability drivers.

The 217Plus [17] approach represents a broader scope to predicting reliability by accounting for all primary factors that influence the inability of a system to perform its intended function. It factors in all available reliability data as it becomes available during each phase of the system life cycle. It thus integrates test and analysis data, which provides a better prediction foundation and a means of estimating variances from different reliability measures.

4.2. Predictive maintenance systems under industry 4.0

For more information about this section, consult bibliography reference [18].

Technologies such as the Internet of Things, Artificial Intelligence, Cloud Computing, Robotic Automation and Big Data Analytics have led to a whole new paradigm of doing business. This change is referred to as the fourth industrial revolution or "Industry 4.0" for short. In order to maximize the benefits of Industry 4.0, business operations must move to the new paradigm in its entirety, which means that maintenance of plant machinery and systems must also follow the same pace and modes. There are multiple challenges in implementing Industry 4.0. Today's factories need access to a variety of information, but there are often issues related to large volumes of data, multiple system integration, and security. As a result, there is an increased need to share expertise across facilities to optimize safety, production and recovery. Subject matter experts are becoming increasingly difficult to locate, and companies must find ways to use them more efficiently. Remote management allows authorized specialists to monitor automation systems, help diagnose problems, adjust loops, optimize processes and generally improve production. Industrial process plants can be monitored remotely using system architectures equipped with General Packet Radio Service (GPRS) and wireless Internet connection in combination with Distributed Control System (DCS), Supervisory Control And Data Acquisition (SCADA) with consequent improvements of the reliability and response times under adverse environmental conditions of process plants to maximize plant operating conditions.

Technologies such as Industrial Internet of Things (IIOT), Artificial Intelligence (AI), Cloud Computing (CC), Autonomous Robotics, Information and Communication Technologies (ICT) and big data analytics have revolutionized the way industries can operate. Industries are leveraging these technologies for their business operations to be more competitive and profitable.

In this increasingly competitive environment, asset maintenance strategies must also be aligned so that equipment and systems are maintained to meet overall business expectations for availability and readiness. Engineering activities and operations under Industry 4.0 will have the following main components:

- Cyber Physical Systems (CPS)
- Internet of Things (IoT)
- Internet of Services (IoS)

Industries are increasingly configuring their machinery and systems as Cyber Physical Systems (CPS) using the above technologies. CPS involves the control and surveillance of physical systems through the computational and supervisory capacity of computers, including web-based software resources. Such web-based resources are available as Cloud Computing applications. Internet of Things (IoT) also refers to the smallest of components or subsystems capable of sending and receiving signals from the Internet. Internet of Services (IoS) refers to services that can be provided over the Internet and which can be used by industries aligned with the Industry 4.0 concept. Factories that are in line with the above configuration can be called Smart Factories. The Internet of Services and the Internet of

Things are two fundamental concepts that should be implemented in factories as a precondition for the smart factory of the future.

These changing industries operating scenarios are, in fact, more relevant to remote plants as the benefits thus derived can offset many of the constraints of remote location. Industry 4.0 generally spreads from developed to developing countries through a rather slow process of diffusion and adoption of constituent technologies. Therefore, different behavior patterns are usually observed and perceptions regarding the usefulness of different technologies differ widely from one region or sector to another. Studies therefore show that there is significant dispersion across countries in the readiness of their industries in terms of their ability to adopt Industry 4.0. Reasons for differences between countries in their ability to adapt to Industry 4.0 are for example the structure of the industrial sector, its role within each country's economy, and differences in business models or management styles. The level of application can vary from single machines, single processes or complete factory in increasing order of automation or complexity. Furthermore, the level of intelligence embedded in the machines, process and in the whole factory can vary in increasing order from simple automated control, integration of automated controls of different functions or integration of higher-level intelligence into the whole factory for autonomous and intelligent functions. This aspect has been well presented as nine applications of intelligence ranging from low intelligence and simple automation to high intelligence and complicated automation so that the production system becomes more and more automated, flexible and intelligent.

Experts believe that predictive maintenance cannot prevent more than 20-35% of failures, depending on whether only the condition monitoring inputs or other additional failure detection mechanisms are employed. Under this condition, in order to make predictive maintenance within Industry 4.0 an applicable and significantly effective strategy for total maintenance, it is necessary to combine technological progress with basic maintenance. Working cross-functionally to handle large amounts of data, leveraging technology development along with basic maintenance practices will be the key to better maintenance under Industry 4.0. Augmented Reality (AR) is an important Industry 4.0 technology and its application for maintenance has been known for some time. However, practical limitations such as lack of adequate knowledge of its application have made it difficult to realize its benefits. Now that some of the technological limitations have been overcome and AR looks ready to become a tool for industry, it is believed that the scientific community can focus on trying to solve real industrial problems. Technologies like AR and Additive Manufacturing (AM) can provide a better way to perform maintenance operations than a traditional approach, as shown in the case of aircraft maintenance. AR can support operators with easy-to-use manuals where virtual models and instructions mix with the real world, while AM can help avoid large warehouses and cut through the supply chain.

Industry 4.0 assumes a limited participation of machine operators in the monitoring and diagnosis of production and technological processes. This applies not only to checking machines and systems, but also to monitoring their condition. The industrial condition monitoring platform consists of three main modules: Monitoring and Feature Extraction (MFE), Real-Time Anomaly Detection (RTAD), and Fault Diagnosis (FD). These three modules are also valid for conventional systems. However, the scope and reach of these modules within Industry 4.0 is very extensive. The MFE module can consist of IIOT-based sensing equipment, collection of a large number of detected and calculated data from which feature extraction becomes more accurate and provides better coverage to the maintained system. MFE information is transmitted to RTAD which can leverage Artificial Intelligence (AI) and Machine Learning (ML) tools, among others, to detect anomalies. Similarly, the FD module uses AI, ML at plant locations, as well as remote expertise and analytical tools via internet communication and cloud resources.

The local operations and maintenance (O&M) platform has machinery and systems to monitor. Data on monitored conditions is processed in the local platform as much as possible for the detection and prognosis of impending fault conditions. Remote competence centers are configured in the system as extensions of local platform capabilities. The communication management module ensures that the overall e-management effort is performed successfully. The implementation of real-time data collection, data analysis and decision-making systems has benefited electronic maintenance and helped reduce downtime and uncertainty about the current state of equipment and possible failures in the future. The correct use of available technologies will lead to intelligent systems that will reduce uncertainty in the decision-making process. The e-maintenance framework is extended using IOT based sensing, cloud technologies and also with the effective use of AI and ML

Sensor and other data acquired in real time, historical, environmental and asset design data are used by the system for the presentation of the processed information in the following forms:

- Indication of asset performance: Key performance indicators (KPIs) are defined as a set of quantifiable and strategic metrics in a performance monitoring system (PMS) that reflect a company's critical success factors. Performance data collected through a variety of IOT-based sensors and classic wired or wireless sensors is processed against data from other sources to provide information indicating asset performance on the appropriate HMI or recorder. Both the number of equipment and the number of sensors are limited to a minimum in systems with manual monitoring mode. However, with IOT-based and wireless communication of performance parameters, the number of parameters and equipment under cover can be significantly increased, thus improving the effectiveness of health monitoring, trends, analysis and predictive maintenance.

- Indication of resource deterioration curves: this feature provides static and dynamic factors that can help explain the failure of resources and processes and their relative importance. The risk of failure of an asset at any given moment is also analyzed and presented. Feature engineering can be done to capture degradation over time using techniques such as regression, binary and multiclass classification, survival analysis, and anomaly detection. In doing so, the solution provider will discover features, which exhibit a degradation pattern with significant predictive power. Industry 4.0 technologies such as Artificial Intelligence (AI) and Big Data analytics can help to use all the data collected, interpret the suggested trends and continuously improve the prognosis of failure.

- Asset life or survival simulation results: effects of various asset maintenance scenarios, probability of an asset surviving beyond a given time, prediction of failure probability over time are some of the useful simulations that can be undertaken and presented to the maintenance team.

- Recommendations for predictive maintenance interventions: the predictive maintenance recommendations are based on the collection of a large amount of data involving multiple KPIs from multiple equipment and their processing using Industry 4.0 technologies. Unlike conventional systems where maintenance decisions were based on very few KPIs and standalone monitored equipment, in Industry 4.0 systems, decisions are more dynamic, sane and robust through extensive data analysis, simulation , modeling and applying AI/ML. AI/ML tools, when properly understood and applied by the maintenance decision maker, can unravel the mechanisms or trends behind many of the unexpected failures. Additionally, there is a need for careful determination of the type of data that needs to be captured and processed in order to be able to maximize the desired results from the predictive maintenance system.

Some studies have been conducted on the issues related to the adoption of Industry 4.0 on legacy systems. In one of these studies, respondents said that the main adoption challenges are the analysis of the data generated, the integration of new technologies with the available equipment and workforce and computational limitations, as well as changes in the business model of the company through the integration of internal resources with complementary activities of their partners and other companies in the cluster. One of the characteristics of remote industries is the complexity of systems in terms of configuration, diversity, size, criticality and inability to provide long interruptions in production. Machine tools are often isolated, not well equipped with modern communication technologies and with a lack of open APIs (Application Programming Interfaces). It is therefore difficult to monitor and control the entire production process using these systems. Systems are difficult to monitor easily, which can introduce inefficiencies and generate higher costs for sensor integration. As a solution, industries can reconfigure their systems into smart machines. However, there are challenges in identifying the standard IoT architecture and clearly establishing the benefits of the transition. Industries are also concerned about the protection of their data when exposed to a cloud or internet-based architecture. For large plants, especially those located in remote areas, progressive conversion is a good option, even switching to fully Industry 4.0 machines and systems during replacement and modernization projects.

As mentioned earlier, large, remotely located engineering, process, or manufacturing facilities have unique custom designs, sets of equipment, systems, and operating philosophies. The set of goals and constraints including logistics for such industries is also unique. Therefore, there is a need to customize the PdM 4.0 solution for these sectors as well. Out of the box solutions are bound to be suboptimal due to inadequate coverage and integration challenges.

To achieve customization, the ideal option would be to integrate PdM 4.0 when designing a plant. The machinery and systems of the plant must be compatible, supportable and integrable with PdM systems. However, this is rarely practical as the obsolescence rates of plant machine systems and PdM systems are very different. Therefore, customization efforts are required to consider a mix of current and new equipment for PdM 4.0 design.

The main goals of PdM 4.0 for a remote process plant would be maximizing plant availability, equipment and process reliability, safety and minimizing costs. However, depending on the nature of the plant, there will also be several minor targets. All goals matter to certain stakeholders at certain times. Many of the objectives would compete with each other resulting in trade-offs and no single optimal solution. Likewise, there are major and minor constraints in achieving goals. Of course, designing a PdM 4.0 platform for such plants will be a multi-objective, multi-constraint decision optimization problem.

A multi-objective optimization problem (MOOP) is solved with input from field data and detectability and prognostic skills. The last two, briefly explained below, are derived based on data or by experts with the help of logic frameworks. The solution to the MOOP consists of a set of optimal points, each one different from the other with compromises. The decision maker selects that solution which would be the most optimal under the prevailing conditions. This solution corresponds to the set of parameters that would define the system that would be selected. In the optimization process, it is essential to identify or create certain parametric metrics for the desirable characteristics of the PdM 4.0 system and quantitatively ascertain how they might influence the achievement of the PdM 4.0 objectives. For example, the ability of a PdM system to be able to detect the onset of a defect or imminent failure and also its ability to prognose and diagnose defects are important requirements for any user.

Monitoring the health of plant systems is essential for predictive maintenance. Some of the health monitoring objectives under Industry 4.0 are as follows:

- Reduce the downtime.
- Prediction of potential failure.
- Dashboard for maintenance and operation staff for monitoring of asset health accessible from mobile as well as in PC.
- Continuously display real-time operational status, running hours, predictions such as Remaining useful life, Time to failure and predictive alerts as they occur and when the as the running states of the equipment changes.
- Automated alert actions triggered by maintenance diagnoses from machine learning predictive analytical platform and equipment prediction of failures and performance variations.
- Unit wise segregation of sensors and equipment.
- Alerts and events.
- The predictive system should have self-learning features for providing real time signature-based diagnosis and prognosis.

The Integrated Business Performance System provides a flow of data, virtually unlimited capabilities for analysis and a valuable flow of information to support business operations. With such information integration, dashboards are also easily obtained for management groups to monitor and control. The Integrated Business Performance System, as the name suggests, includes all operations of the business enterprise, including business systems and plant systems. Control, condition monitoring and predictive maintenance will be part of this overall architecture, taking care of plant systems.

The outputs that are expected from the asset predictive maintenance framework will be briefly discussed here.

1) Asset Performance Indicators Requirement: there are several equipment and multiple KPIs related to each of them.

Industry 4.0 technologies not only make it feasible to measure and transmit KPIs in large numbers, but also facilitate the processing of such a large amount of data using Artificial Intelligence (AI), Machine Learning (ML), Data Analytics and generate extremely useful information for predictive maintenance. The role of these technologies will also be exploited to guarantee the integrity of the data and the reliability of the information thus generated. In connection with measurement requirement and information visualization, the following features are also included with the help of technologies such as AI and ML:

- Equipment and System Diagnosis.
- Dashboard for maintenance engineers.

The following are some of the features that will also be included in the dashboard:

- Remaining Useful Life.
- Expected Life with Age and installation date.
- Time to Failure Prediction within a given time window.
- Survival models for the prediction of failure probability over time.
- MTBF, MTTR, OEE (Overall Equipment Effectiveness), open work orders.
- Short and detailed report about equipment health to be made accessible from web and mobile devices with maintenance recommendations.
- Spare parts material code and no should be linked with sap current stock availability.
- Pattern recognition or other machine learning techniques for detecting anomalies/predicting failures.
- Performance correlated to a slowly degrading metric.
- All key personnel to be alerted on their mobile device and email about overall Asset health score or developing problems in critical assets when threshold is breached.

2) Asset deterioration curves: degradation pattern in speed, efficiency, pressure, load, heat, noise etc. to be tracked and monitored.

3) Asset survival simulation: following are some of the simulations that are undertaken as decision support by maintenance team:

- Effects of various asset maintenance scenarios.
- Probability of an asset that survive beyond a given time.
- Prediction of failure probability in a certain given interval of time.

4) Predictive maintenance interventions/recommendations: The feature provides predictions about the assets at greatest risk of impending failure, so shifting the maintenance regime from fail-and-fix to predict-and-prevent by issuing work order and schedule maintenance rules.

Some of the major technical requirements of such a predictive maintenance decision platform are as follows:

- Fixing and monitoring of KPIs of production, profitability, cost, target versus actual scenario, historical performance, equipment overall efficiency, health indices, probability of failure calculations, reliability modelling, failure reasons, reliability parameters MTBF/MTTR calculation, trends, spares consumptions, and performance curves of equipment integrated with notifications.
- Real time performance-based surveillance based on stability modelling for any process and equipment parameter and performance curve.
- Root Cause Analysis with integration of relevant data.
- Automation of plant-wide repository for all corrective and preventive action taken.
- Provision of tools to track the effectiveness of maintenance.
- Provisioning for predictive, prescriptive of cognitive analytics.

The nature and quantity of data required for predictive maintenance analysis would differ from one application to another. Some major categories of data that would be necessary are as follows:

- Static data: equipment make, model, configuration, best practices and OEM recommendations.
- Frequently updated data and usage history: age of asset in days, failure history and the preventive maintenance schedules of assets, KPIs for asset performance tracking.
- Maintenance data: maintenance, breakdown details, service history.
- Time series data: KPIs that are needed as function of time.
- Feature engineering: collection of data which are collated in the form of averages, linked data, such as ambient temperature and vibration, in order to draw better inferences about the health of machinery.

In addition to the above basic structure of predictive maintenance framework, following are some of the major features that are included in a predictive maintenance decision framework for better technology and resource utilization and enterprise level outcomes:

- Asset Data Mapping and Modeling: mapping of operational, environmental, historical, and age data is performed to generate information that more accurately indicates the health of the equipment system. This data mapping can support regression models, classification models to predict failure within a given time window, models to report anomalous behavior, survival models to predict failure probability over time.
- Machine learning-based asset health score in the dashboard: by using AI and ML tools, the decision support system can generate certain scores that represent the health of an equipment or system. This information, when available in the platform for access by the maintenance team or on the dashboard for senior management, can serve as a valuable decision-making tool.
- Operational and business reporting automation and dashboards: one of the important requirements of a predictive maintenance decision support system is a very versatile and rich reporting system. Reports range from direct real-time

logged data, data from direct calculations, alarms, trends, diagnostics, maintenance reports and dashboard summaries. For the benefits of such a decision support system to be fully realized, adequate attention must be paid to the development and configuration of dashboards, HMIs and other reporting mechanisms.

- Cyber security requirements: The platform is normally developed based on industry standard and secure software development practices. The implementation of cyber security best practices in accordance with international standards is respected for better interoperability and to ensure data integrity and security. The necessary plant and user department specific safeguards are also integrated. However, care must be taken to ensure that system usefulness and ease of operation are not obstructed while security measures are instituted.
- Safety requirements: complex, critical and expensive systems such as the Integrated Business Performance System should have all the protections against hazardous materials, electrical hazards, fire, vibration and shock or mechanical impact.

➢ ***Final considerations***

In modern industry where reliability, availability, productivity and specially safety are the main point of concern, the traditional operator driven approach has its drawbacks to fully meet all these criteria. So the modern approach of IIOT-based Industry 4.0 techniques will definitely help to improve plant safety and reliability along with other production-related parameters. To achieve the same result, it is necessary to employ Industry 4.0 technologies in a complete, optimal and plant-wide way. While high-intelligence and complicated automation in maintenance would be desirable, constraints such as initial and recurring costs, and human resources factors need to be taken into account when finalizing the scope for PdM 4.0 systems.

Industry 4.0 know-how based on IIOT is itself a challenge. Management and operator training is a first step in the implementation process. To take advantage of the system, the detailed engineering part can be outsourced to agencies with experience in data acquisition and processing technologies. The software solution providers in the market can provide the complete solution and customized packages as per the requirements of the plant management. The various stages are described below:

- Identification of requirements: identification of critical assets that you want to monitor remotely.
- Choice of technology: as mentioned above, there are service provider companies that can provide various sensor technologies, data acquisition, processing and presentation techniques for IIOT-based Industry 4.0.
- The plant management will choose the right technology and train its employees on it.
- After implementation, system maintenance and data validation will need to be institutionalized according to the current situation.

Industry 4.0 is being adopted by manufacturing and process industries in line with global industrial and research trends. Maintenance, as an indispensable element of industrial operations, will also need to align its practices, hardware and facilities in line with this global trend for industries to gather the full benefits of Industry 4.0. There is a large dispersion across countries, regions and sectors regarding the extent to which Industry 4.0 is implemented. These leaks will reduce with increased acceptability and readiness for constituent technologies by industries around the world. However, it is clear that a comprehensive implementation of Industry 4.0 leveraging all relevant technologies will deliver immense growth which can truly be termed the fourth industrial revolution. Furthermore, the application of Industry 4.0 in maintenance is not only desirable but also imperative for industries to remain competitive. The transition to predictive maintenance within Industry 4.0, especially with regards to current systems, is a universal challenge and must be managed appropriately. The benefits of using Industry 4.0 technologies such as IIOT, AI, cloud resources, and automation include improved RAMS analysis and therefore increased productivity and competitiveness.

4.3. DevOps for Airborne software

For more information about this section, consult bibliography reference [19].

To take advantage of upcoming new technologies such as virtualization, software as a service (SaaS), and big data revolutions, new development strategies have emerged.

These strategies, collectively referred to as DevOps, enable software teams to deliver functionality to users faster and more reliably and offer new opportunities for transforming software practices in traditional software domains such as defense and aerospace.

DevOps emphasizes integrated development and operations, continuous delivery, and heavy use of automation and virtualization to improve consistency and reliability.

In a traditional software lifecycle, feature development and operational activities such as implementation, support, and maintenance are loosely coupled.

Defense and aerospace software has modeled this process through the use of block releases corresponding to major system upgrades, often in connection with releases of updated electronic and mechanical systems. This software delivery model gives users many new features all at once, at the expense of long release cycles and buggy releases that require many successive patches.

In a DevOps software process, some of the traditional relationships between technology and process are reversed. First, in DevOps, development and operations are closely linked. Often, the same small engineering team is responsible for the entire lifecycle of a feature or component, from design and development to testing, deployment, support, and uptime. This strategy removes the bottlenecks in implementing new features created by handovers between various product teams with different needs and goals. Instead, the features themselves are often loosely coupled and treated as application programming interfaces (APIs) or isolated services. This allows them to be independently maintained and updated without significant integration testing.

This decoupling allows for continued development of features. DevOps releases can happen multiple times a day if needed. Every DevOps update, whether it's a bug fix or a new feature, is treated like a live patch to an existing system. Using virtual architectures ensures that resources are always available to support the new release.

DevOps is as much about making teams work well as it is about new releases or sustaining strategies. As DevOps teams will design, develop, deploy and maintain their software components, it is imperative that the right attitude and skills are in place. Developers need to pay more attention to quality and especially how imperceptible changes might affect the embedded system as most DevOps teams will not include independent quality assurance. Everyone needs expertise in virtual machines as virtualization will play a big role in engineering for quality, reliability and scalability. Finally, teams will need to have some degree of permanence, as DevOps engineers are responsible for maintaining their code long-term. Organizations accustomed to maximizing developer productivity through frequent reassignments will need to adjust.

DevOps can offer significant improvements in time-to-market, consistency, reliability, and cost of defense and aerospace technologies, but will require some adaptation to meet industry needs and practices.

As prevailing industry technologies and standards change, aerospace and defense technology companies will need to adopt DevOps to remain competitive and successful.

DevOps in the context of avionics simply has to do with the speed of implementation due to FAA certifications, aircraft rectification, and how the airline industry releases their modifications. Development on LRU can easily be done using the DevOps mindset. These many small changes can be memorized and periodically released to be subjected to final tests and certifications. Furthermore, implementing DevOps does not involve systematic problems arising from regulations, policies and industry standards. Avionics companies that are able to innovate and deliver better value, higher reliability and lower costs will easily be able to innovate their competitors and gain traction and market share.

- ***DevSecOps***

DevOps originates from the combination of software development and system operations to ensure that software development occurs in conjunction with the teams that manage these systems in the real world.

The next step in this improvement of software development methods is DevSecOps, where security is included as a fundamental part of the development process. A security failure is equal to, or worse than, a quality error. Defective products affect the company's profits and reputation. It's even worse if a review determines these flaws could have easily been avoided. So DevSecOps is the team-level integration of the teams that build the software, manage the software, and secure the software.

Furthermore, a key reason for integrating security into your processes is to build on the experience and knowledge that you accumulate over the course of the project. It is unreasonable to expect software teams to have a complete overview at the outset of the project. Integrating security into day-to-day operations gains experience. DevSecOps is often illustrated as follows in the DevOps flowchart, security every part of the cycle:

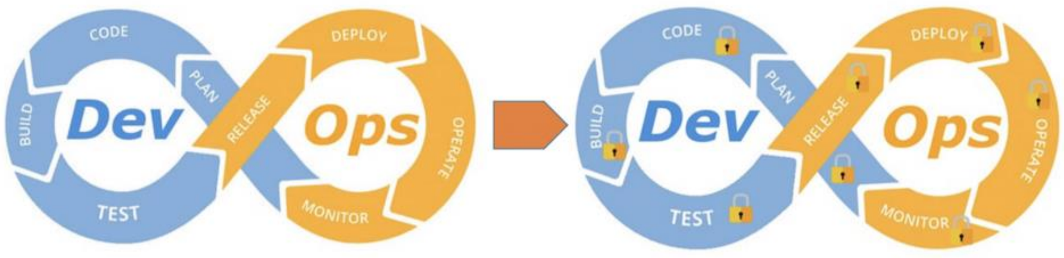


Figure 40. The DevSecOps cycle

- ***DevSecOps in Safety Critical Software***

A key aspect of adopting DevSecOps is automating tedious and potentially error-prone manual steps in the development process. Part of that is the move to continuous integration (CI) and deployment (CD). The goal of each is to accelerate time to quality and safety by identifying and resolving integration and deployment issues early in the lifecycle. A continuous process provides feedback on defects and vulnerabilities that improve subsequent iterations.

The biggest challenge to adopting DevSecOps in safety critical software is the need to meet audit, validation, and certification requirements. DevOps processes and techniques are not defined in detail, allowing teams to adopt the details of interest to them. However, safety and security standards require a rigorous and well-defined process. This is compatible but requires software teams to define and document their DevOps tools, processes and techniques. An important example is traceability. The demonstration requirements are met with proven validation tests which are important to demonstrate the functionality and airworthiness of the system. Any DevSecOps process should handle traceability with precision.

- ***Security as Code***

An interesting approach that has emerged from the DevSecOps practice is the concept of treating security requirements in the same way as safety and functional requirements. Guided by the outcome of detailed threat analysis and implementation of security controls, then to validation through testing and documentation. This is the way to integrate security into DevOps and a good way to integrate security into the development culture and get software teams to communicate using a familiar language.

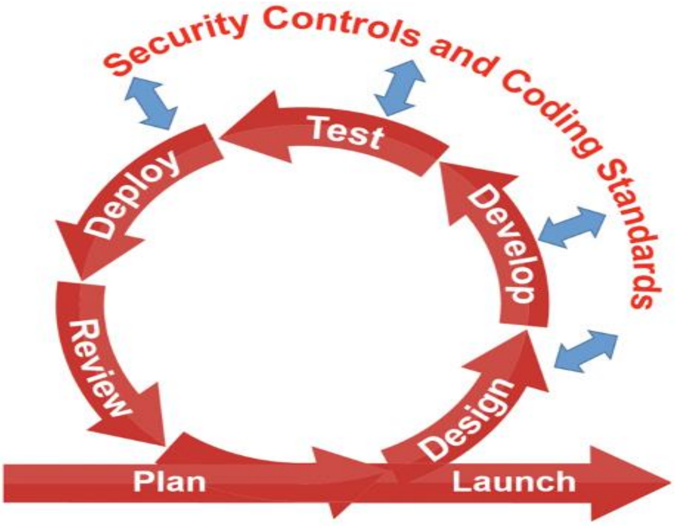


Figure 41. DevSecOps requires security requirements, controls and coding standards

➢ ***Role of Static Analysis***

Static analysis tools are designed to integrate well with any software automation tool chain and development methodology and process. This is mainly because they can be used locally by developers on their desktop for instant feedback and used to analyze a complete build. Furthermore, these tools are completely autonomous as they require no interaction with testers or developers. They are applicable whenever it makes sense to check the code for bugs and security vulnerabilities:

- **Develop:** This is the critical time to detect any new security vulnerabilities as soon as developers write new code, even before it's submitted to a build or software control system. Turnaround time is important here, feedback needs to be fast. Violations of the coding standard and potentially dangerous coding practices are flagged for developers to investigate.

- **Test:** This is where all the changes from all developers are brought together for more comprehensive testing, static analysis plays an important part in that process.

- **Deploy:** Static analysis tools analyze deployable binaries and libraries. This is a good practice to detect bugs introduced during building and deployment of deliverables.

- **Review:** Static analysis reporting and analysis that software teams can use to evaluate individual warnings but also higher-level assessments of application quality and security.

These integrations into the DevSecOps cycle are illustrated below.

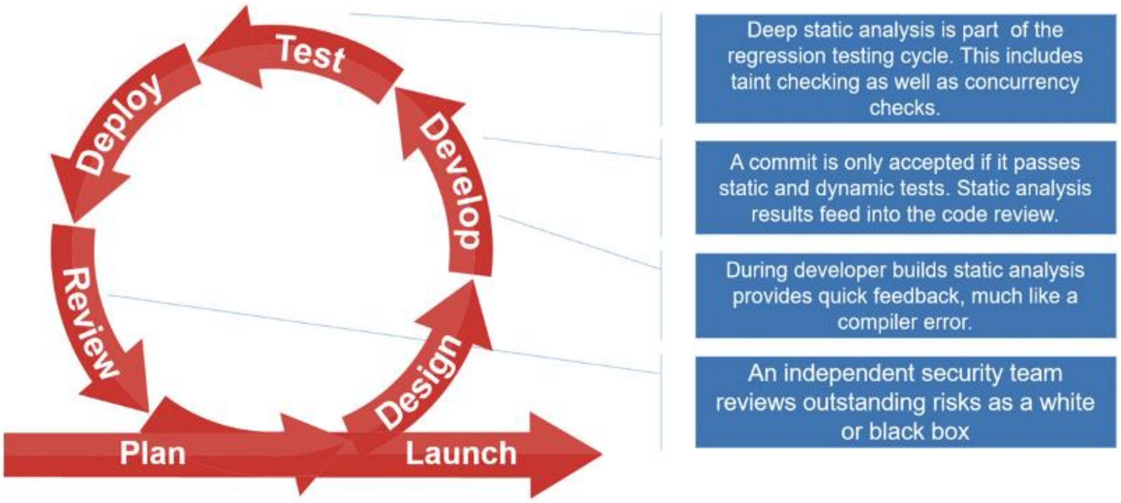

Test
Deploy
Develop
Review
Design
Plan
Launch
Deep static analysis is part of the regression testing cycle. This includes taint checking as well as concurrency checks.
A commit is only accepted if it passes static and dynamic tests. Static analysis results feed into the code review.
During developer builds static analysis provides quick feedback, much like a compiler error.
An independent security team reviews outstanding risks as a white or black box

Figure 42. The role of Static Analysis

- ***<u>Third-Party Software</u>***

Use of third-party code such as commercial off-the-shelf software (COTS) and open-source software is largely used in embedded software development and is increasingly part of avionics software. Static analysis tools can analyze third party source and binaries to discover defects and security vulnerabilities in software that could be impossible to test otherwise without including it and running it, which is an expensive option.

- ***<u>Tool qualification</u>***

Although software development tools used in Avionics aren’t certified, they do require qualification to certification bodies such as the FAA. As such, it’s important that any tools used meet qualification requirements.

- ***<u>Final considerations</u>***

Modern safety critical avionics software requires rigorous security engineering connected with the established safety practices in place. New cyber security standards are requiring security design from the very beginning of product lifecycle. To address these requirements, there are advantages to modern software development practices found in DevSecOps. Just as it is impossible to build-in safety into software, the same holds true for security. Security must be part of the product concept and built-in.

4.4. Integrated Deterministic and Probabilistic Safety Assessment

For more information about this section, consult bibliography reference [18].

Deterministic safety analyzes and probabilistic safety assessments are widely used in the risk management of complex engineering systems. Challenges to these approaches include modeling the dynamic interactions between physical process, safety systems, and operator actions, as well as the propagation of these model uncertainties. Dynamic Event Tree (DET) analysis enables integrated deterministic and probabilistic safety assessment (IDPSA) by coupling process system models with safety system and operator response models. This section introduces the concept of IDPSA, highlights the advantages of the approach as well as its limitations.

➢ ***Introduction to Integrated Deterministic and Probabilistic Safety Assessment***

In the safety analysis of complex engineering systems, we develop accident sequence models to quantify the risk. In this process, it is a challenge to consider dynamic interactions and capture their impact on accident models. Such dynamic, time-dependent interactions can arise due to human interactions, digital control systems, and passive system behavior. The main goal is to increase the realism in modeling the dynamics during risk quantification. An integrated deterministic and probabilistic safety analysis (IDPSA) approach is introduced including its basic elements and their relationships.

➢ ***Probabilistic and Deterministic Safety***

In the Risk Analysis of complex engineering systems, we mainly address these questions:

- What is the hazard?
- How likely is it?
- What are the consequences?
- How to improve the level of safety?

We use a systematic and comprehensive Probabilistic Safety Assessment (PSA) methodology to evaluate the risk associated with complex engineering systems. Here are the high-level tasks of PSA:

- Identify accident initiators
- Development of accident models including sequence delineation and definitions of success criteria. Success criteria focus on identifying the requirements for the success of safety systems. These requirements concern how many systems or equipment must operate, the maximum time within which operators must intervene, for how long the equipment must operate.
- Quantifying the risk therefore corresponds to estimating the probability that the requirements are not met and an accident follows.

➢ ***Issues in Current Approach***

Risk and safety assessments are performed extensively to evaluate the risks associated with complex engineering systems such as aircraft systems. The classical combination of event trees is used to build risk models. Quantification of risk models requires inputs such as data and simulations. Typical results include risk, sequence contribution and risk baseline events.

Deterministic safety analysis is based on offline process analysis with predefined boundary conditions, which is performed for sequence outcome determination and success criteria definition. Probability safety models, which consists in a classical combination of event tree and fault tree models, address the probability that these criteria are not met. The accident scenario is simulated with an autonomous tool. Typically, a few sequences with predefined boundary conditions are simulated to test whether the sequences lead to a safe state or an unintended consequence.

How a complex engineered system works under normal conditions is well known, but things change in an accident scenario, characterized by the dynamics of the accident. The behavior of the process evolves with time and the process parameters change with respect to time influencing the response of the safety systems. The operator's response can affect the physical process. A typical accident scenario involves complex interactions between process, safety devices and operator actions.

The main question is whether we adequately consider complex interactions in the current practice of system simulations with pre-set system states and operator times.

For example, total operator time is dynamic, it's hard to predict offline. Also, when stochastic variables are considered in such responses, defining success criteria will be complex. Boundary assumptions are needed when winding sequences and defining success requirements in PSA. Not only is bounding difficult, but it also produces modeling artifacts in some cases. One of the main problems in the current PSA practice is the uncertainty in the physical process models. The parameters of the PSA model, such as failure rates or probability of failure, are already accounted for, but uncertainties in the parameters of the physical model also need to be addressed when creating the risk models. These can influence sequence results, success requirements, subsequently risk estimates and contributors.

➢ ***Dynamic Event Trees***

Dynamic Event Tree (DET) analysis provides a framework for integrated incident simulation of physical processes, equipment, and operator actions. In other words, DET provides the means to simulate the evolutions of physical systems, the evolution of system states due to stochastic events, and the dynamic interactions between these evolutions. DET simulates the dynamic interactions between physical process, safety system responses and operator responses. DET models include deterministic physical models and stochastic models.

The accident scenario is simulated considering the dynamic interactions and stochastic variables to generate the sequences. The results of the sequences are labeled according to the values of the physical parameters. The risk is estimated considering all unwanted sequences. In the dynamic event tree, the transient is simulated in a deterministic dynamic model and the values of the process parameters are obtained from the dynamic model of the plant with respect to time.

The scheduler has the integrated model of the plant which describes the behavior of the various elements as a set of rules. When the process parameter reaches a level, it triggers one of these rules. As a result, sequences of events are generated based on the rules. When the process parameter requires safety system or human action, one of the rules in the scheduler is triggered and branching occurs in the DET.

- ***IDPSA Methodologies***

This section describes two IDPSA methodologies available in the literature, namely, DET informed PSA and quantified DET.

- ***DET Informed PSA***

The high-level tasks of the DET Informed PSA approach include DET Modeling, DET accident simulator, and success criteria analysis to develop event tree models and their evaluation. DET models mainly consist of physical models of system behavior, stochastic models of the equipment, and operator response models.

Focusing on the detailed tasks involved in this approach, the scope of the overall analysis is first defined, including the boundary conditions of the initiating event, the safety functions to consider, variables to address and the final sequence criteria. Simulation models are developed for the physical process, the response of safety functions and operator responses. The accident scenarios are simulated with simulators considering the random variables. The results of the simulations are analyzed to understand the dynamics of the accident and identify the evolutions that lead to undesirable consequences. Success criteria are identified by examining the sequences generated by the DETs, initially for individual safety functions and initial events. The initiators and sequences with similar success criteria for each safety function are then grouped, as a basis for defining one or more event trees to represent the overall variability of the initiating event. Finally, the success criteria for these trees are defined. For the operator actions, additional DET simulations are used to estimate the time windows in order to calculate the human error probabilities (HEP) in consideration of the boundary conditions of the sequence. The overall risk and also important contributors are identified and quantified.

Quantification of event trees requires various activities such as fault tree modeling, common cause failure modeling, human reliability analysis, and failure data. Fault trees for safety functions are developed and linked to event trees. Modeling common cause failures takes into account any implied dependencies between similar safety equipment. DET simulations provide useful information for estimating time windows for operator actions, which are used to estimate probabilities of human error. PSA parameters are also needed, including probabilities and frequencies of initial events, hardware, and operator actions. Finally, PSA tools are used for the quantification of accident sequence patterns to obtain risk outcomes, including point estimation of risk and important contributions to baseline risk events and sequences.

- ***Quantified DET Based IDPSA***

The high-level tasks of the DET quantification approach are DET modeling, simulation, and evaluation. The DET modeling and simulation task is quite similar to the DET Informed approach. DET evaluation replaces success criteria and bounded compact event tree modeling in this approach. In the DET evaluation, all individual generated sequences are explicitly quantified. The DET sequences whose outcomes lead to undesirable consequences are identified, and the frequencies for each of these failure sequences are estimated, as well as the total risk from the scenario.

Both the Informed DET approach and DET quantification use the same integrated DET simulation tool. While the tool and DET models are the same, the simulations in DET Informed are with bounding while the latter approach runs simulations without bounding. The DET Informed PSA provides an integrated framework for accounting for complex dynamic interactions and stochastic variability between physical processes, safety equipment and operator actions. DET Informed PSA helps to obtain success criteria definitions and build compact event tree which is quite practical in large-scale PSA of complex engineering systems. On the other hand, in the DET-informed PSA, delimitation assumptions are inevitable to wrap the sequences and define the success requirements. Some detrimental effects of the limit may arise due to the dynamics of the accidents, which could be overlooked. The quantified DET approach does not need bounding assumptions, thus circumventing the problems associated with bounding effects. However, further calculations are needed. The DET Informed approach produces classical event trees compatible with current PSA practice. Typically, classic event trees contain binary branches. On the other hand, the quantified DET approach can generate several branches for safety systems that represent various combinations of conditions across safety functions. With regards to risk quantification, both approaches differ in the way they handle safety systems whose response involves a continuous random variable. For example, power recovery time or operator action response time. In classic event trees, the probability of human error or probability of recovery is estimated offline, then used as input for quantifying the binary branches.

In contrast, Quantified DET does not require time windows to estimate these probabilities. The quantified DET approach faces the following practical problems: it must evaluate all generated sequences, deal with support system dependencies between safety functions, as well as account for safety systems whose response is continuous.

- ***Final considerations***

In conclusion, bounding in PSA and DET informed quantification leads to a conservative estimate of overall risk, but may be sensitive to bounding assumptions and their ability to capture accident dynamics. Additionally, both quantifications underestimated the percent risk contribution and event importance due to bounding success criteria. Bounding becomes complicated when we consider the uncertainties of the physical parameters and the uncertainties of the failure and repair parameters. The IDPSA approach, quantified DET, improves accident dynamics modeling, eliminates boundary effects, and provides a framework for the physical model, safety system mode, and operator response models. However, quantified DET requires additional calculations and discretization of continuous stochastic responses.

Bibliography

[1] Saraswat, S. and Yadava, G.S. (2008), "An overview on reliability, availability, maintainability and supportability (RAMS) engineering", International Journal of Quality & Reliability Management, Vol. 25 No. 3, pp. 330-344

[2] M. S. Saglimbene, "Reliability analysis techniques: How they relate to aircraft certification," (2009) Annual Reliability and Maintainability Symposium, pp. 218-222

[3] CEI EN 50126, Railway applications (2000) - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

[4] Birolini, A. (2013). Reliability engineering: theory and practice. Springer Science & Business Media.

[5] EventHelix,https://www.eventhelix.com/fault-handling/reliability-availability-basics/, consulted 12/09/2022

[6] MIL-HDBK-217F, military handbook (1991), reliability prediction of electronic equipment

[7] Standard ANSI / VITA 51.1, Reliability Prediction MIL-HDBK-217 Subsidiary Specification (2013)

[8] Stapelberg, R. F. (2009). Availability and maintainability in engineering design (pp. 295-527). Springer London.

[9] Ebeling, C. E. (2019). An introduction to reliability and maintainability engineering. Waveland Press.

[10] MIL-HDBK-472, military standardization handbook: maintainability prediction (1966)

[11] Bahr, N. J. (2014). System safety engineering and risk assessment: a practical approach. CRC press.

[12] FMD-91, reliability analysis center: failure mode/mechanism distributions (1991)

[13] MIL-STD-882E, department of defense standard practice: system safety (2012)

[14] MIL-STD-1629A, military standard: procedures for performing a failure mode, effects, and criticality analysis (1980)

[15] MIL-HDBK-338B, military handbook: electronic reliability design handbook (1998)

[16] Y. Bot, "Is Your Organization Ready For RAMS Digitalization Lessons Learned From Implementation in an Aerospace Company," 2020 Annual Reliability and Maintainability Symposium (RAMS), 2020, pp. 1-4,

[17] MIL-HDBK-217 Plus, Quanterion, Reliability Prediction Models (2006)

[18] Durga Rao Karanki, Gopika Vinod and Srividya Ajit (2020), “Advances in RAMS Engineering”

[19] Garcia, J., Shannon, R., Jacobson, A., Mosca, W., Burger, M., & Maldonado, R. (2021). Powerful authentication regime applicable to naval OFP integrated development (PARANOID): a vision for non-circumventable code signing and traceability for embedded avionics software. Journal of Defense Analytics and Logistics.

List of Figures

List of Tables

Acknowledgments

Essendo questa tesi la tappa finale di un importante capitolo della mia vita e la conclusione della mia carriera da studente, è doveroso in chiusura ringraziare tutte le persone che mi sono state vicine e hanno reso stupendo questo viaggio insieme.

Un grazie di cuore va a tutte le persone con le quali è stato condiviso un, seppur breve, momento di questa avventura, le quali hanno saputo essere anche per una sola chiacchierata validi compagni.

Al professor Magnani che ha saputo essermi vicino per tutto il percorso di questa tesi con validi consigli, al team della Pariani, in particolar modo Suelì, Stefano, Fabrizio ed Enrico, i quali mi hanno fatto fin da subito sentire parte di un gruppo, accogliendomi sotto la loro ala protettiva e dai quali ho imparato molto sul mondo del lavoro.

Ringraziamenti speciali sono poi per gli amici di una vita della mia città con i quali si è cresciuti insieme senza perdersi mai di vista.

Alla mia famiglia, esempio e riferimento in questa vita, alla mia mamma, il mio papà, mia sorella Loren e mia nonna Liri, le persone che mi hanno reso ciò che sono adesso.

Un ringraziamento finale di cuore alle persone che più di tutte mi hanno accompagnato in questi anni di Università, amici veri che hanno reso preziosa e indimenticabile ogni avventura vissuta insieme e rigorosamente a modo nostro, Lore, Gio, Dani e Luca.

Un grazie a tutti loro che hanno saputo, sanno e sapranno essere parte della mia vita e senza i quali tutto perderebbe di gusto!