

IMdR

Working Group
Management, Methods,
Standard Tools (M2OS)



Method Sheets

Introduction

Since its origin at ISdF (Institut de Sûreté de Fonctionnement *1) then at IMdR (Institut de Maîtrise des Risques) the M2OS working group (Management, Methods, Standard Tools) along with around twenty members endeavored to publish books to be references for people caring about Dependability and Risk Management. People can be junior who look for help at starting in their occupation or senior who want to remember technical features whatsoever.

In line with documents elaborated by M2OS, the reader can find hereafter a compendium of method sheets. This compendium does not pretend to be definitive. It can evolve following its enrichment, the number of sheets, and addition of appendices (examples....).

To that end, you could participate, a model of editable blank sheet being available on IMdR website. You may address any comment on the existing compendium or propose new sheets, by the means most convenient to you, and address it by e-mail to the project coordinator: prlecler@club-internet.fr

Presently, the compendium includes the following sheets:

1. [Characterization of a product mission profile](#)
2. [Functional Analysis \(F.A.\)](#)
3. [Reliability Block Diagrams \(R.B.D.\)](#)
4. [Reliability Allocation](#)
5. [Predictive Reliability Assessment](#)
6. [FIDES](#)
7. [Reliability Estimates from tests or field experience](#)
8. [Predictive Mechanical Reliability Assessment](#)
9. [Mechanical Reliability – the Stress-Strength Analysis method](#)
10. [Choice and application of software dependability*1 analysis methods](#) Update
11. [Software Dependability*1: approach through standards](#) New
12. [Software Dependability*1: means, tools and analysis](#) New
13. [Bayesian approach in reliability](#)
14. [Preliminary Risks Analysis \(P.R.A.\)](#)
15. [Failure Mode Effect and Criticality Analysis \(F.M.E.C.A.\)](#)
16. [Graph of states](#)
- [Fault tree analysis, event tree, cause tree, don't be confused!](#)
17. [Fault Tree Analysis \(F.T.A.\)](#)
18. [Event Tree Analysis](#)
19. [Cause Tree Analysis](#)
20. [Maintenance and Maintenance Capability Trees](#)
21. [HAZard and OPerational Study \(HAZOP\)](#)
22. [Hazard Analysis Critical Control Point \(H.A.C.C.P.\)](#)
23. [Zone Analysis](#)
24. [Reliability Centered Maintenance \(R.C.M.\)](#)
25. [Integration Design and Support \(I.D.S.\)](#)
26. [Design of Experiments \(DoE\)](#)
27. [Accelerated Life Tests](#)
28. [Highly Accelerated Life Test \(H.A.L.T.\)](#)
29. [Burn-in tests](#)
30. [Failure Report and Corrective Action System \(FRACAS\)](#)
31. [Life Cycle Cost \(L.C.C.\)](#)
- [Glossary](#) Update

***1 « SÛRETÉ DE FONCTIONNEMENT » and « DEPENDABILITY »**

The sense used in France (RG - AERO - 0040) about, "Sûreté de Fonctionnement" is the set of attributes of a product that enable it to dispose of specified functional performance, at the specified time, for the expected duration, without damage to itself and its environment.

"Sûreté de Fonctionnement" is generally characterized by the following four attributes: Reliability, Maintainability, Availability, Safety (RAMS).

In few cases, it may include other attributes such as lifetime, survivability, or invulnerability.

The most common translations of "Sûreté de Fonctionnement" are "R.A.M.S." (Reliability, Maintainability, Availability and Safety), "Dependability", "Dependability and Safety". However, none of them fully reflects the above definition.

In the French version of the method sheets, we use the term "Sûreté de Fonctionnement" whereas in the English version the term "Dependability", is accompanied by an (*) to refer to this note.

* 2 Some sheets mention references out of edition, but their content is still valid.

* 3 Direct access to sheets is done by clicking on the name in the summary above. Return to summary is done by clicking on the title in the sheet.

M2OS group chairmen: J.M. Cloarec (Bombardier) and Y. Mortureux (UIC/SNCF)
Project Coordinator: P. R. Leclercq (R.I.S.)

Project M2OS Active Members:

Mme M.M. Oudin-Darribère (IMdR),
MM. Y. Castellany (ESTP/IMdR),
J.M. Cloarec (Bombardier),
A. Delage (IMdR),
R. Grattard (Systra),
T. Jalinaud (CEA),
J. Lafont (ESTP/IMdR),
P. Leclercq (R.I.S.),

D. Merle (IMdR),
P. Moreau (DGA),
D. Morel (DGA),
Y. Mortureux (UIC/SNCF),
J. Ringler (Ringler Consultant),
J. Riout (CETIM),
G. Sabatier (LGM),
M. Testylier (GMAO® Services)

English Version: A. Delage, R. Grattard, P. Leclercq, and D. Merle.

Characterization of a product mission profile

Purpose (What for?)

Validate and complete new product requirement regarding actual life profile and provide inputs as to define optimum operating margins regarding expected operational achievement.

Description (What does the method produce and how?)

Actual life profile characterization includes firstly detailed analysis of the whole of the situations the product could encounter from factory output to discard or recycle. It includes then identifying product-operating conditions (on, off, storage...) and associated environment conditions, in nature and/or level, applied to each identified situation. The analysis results will be reported on adequate flow sheets and synthesis tables.

Method Implementation (How is it settled?)

Product life profile characterization approach requires synergy between various abilities, requirements, design, and dependability. It takes birth at new product feasibility as to validate the requirements, it continues in Design phase as well as in Production and Operation phases as to envision in a finer and finer manner the predefined profile, the test results and the possible field results.

In order to achieve these objectives, the product life profile characterization approach is led in **six successive steps**:

1/ Settlement of the life profile graph of states: define during Feasibility phase system « global states » so called « segments » corresponding to product well determined use categories (i.e.: factory output, storage, operator use...). Split those segments into intermediate states so called « phases » (ex: railway transport, vehicle running...), then into « sub-phases » (ex: vehicle urban running), until obtaining of a breakdown level possibly associate to given environment and configuration (ex: vehicle urban braking). Such an ultimate breakdown level is called « situation ». These situations include incidents or exceptional conditions identified through risk analyses. The output is a product life profile graph state describing product breakdown from « segments » to various identified « situations ».

2/ Settlement of the occurrence table: during Design phase, define indicators as to quantify typical and/or extreme durations of segments, phases and sub-phases as well as situations identified through the life profile graph state. Frequently those events appear as recurrent; it is then advisable to define the number of expected occurrences in the various states identified all along the life profile. The output is an occurrence table (durations, number of occurrences) of the various product states along its life profile.

3/ Establishment of the table of environment agents by situation: precise nature (but not levels yet) of all environmental agents (natural and induced) bared by the product in every identified situation. Initiated during Design phase, this step is performed during design phase taking into account induced events. The output is a table providing for each situation the concerned environmental agents. The environmental agents are grouped under climatic (ex: hot, cold, humidity...), mechanic (ex: vibrations, shocks), electric and electromagnetic (ex: cycles on/off, interferences...), chemical, a.s.o.

4/ Settlement of situation sheets: characterize as finely as possible each situation identified on the graph state. The situation sheet begins in faisability phase, and continues during the design phase knowing technical solutions and induced environments. The identified environmental agents are characterized for each situation in terms of value, frequency and duration. Each situation sheet, whose format is to be adapted to the product nature, to its life profile and to environmental agents nature, provides the occurrence (typical, mini, maxi), the duration (typical, mini, maxi), the encountered environmental agents (nature, value, frequency, duration), the product configuration (product position, protection, handling place...) and the operating state (ex: continuous operation, on/off, sleeping...).

5/ Environment synthesis: during design phase, identify on one hand maximal values got by each environmental agent on the whole of the situation sheets, and on the other hand the templates showing the temporal value distribution of the agents all along the product life. The obtained results are displayed on synthetical templates fitted to product nature and life profile.

6/ Enrichment of life profile during Operation phase: such enrichment presumes a Field EXperience (FEX) of product user towards manufacturer or customer. As the case may be, information allowing enrichment and document updating according life profile are ensured through direct transmission of all operation data by user, or are limited to observed incidents (negative FEX part) or else through manufacturer sampling at users (as often in general public area).

Relevance Area

- Innovative design products,
- Products with great variability of situations and environmental agents associated to life profile,
- Products with possible critical consequences due to some incidents during life profile.

Inputs

- Initial requirements,
- Use conditions,
- Field experience,
- Product design,
- Test results.

Outputs

- Life profile (more and more detailed),
- Recommendations for requirements and use conditions.

Pros

- Good knowledge of actual product life profile,
- Requirement fitted to actual life profile,
- Product design fitted to « just necessary ».

Cons

- Analysis sometimes difficult in case of life profiles with heavy variability of encountered situations and associated environmental agents (general public products),
- Iterative approach.

Bibliography

- Projet IMdR-SdF 9/2003 « Démarche de caractérisation du profil de vie d'un produit » (2004)
- NATO-AETCP 600 « The ten step method for evaluating the ability of materiel to meet extended life requirement » (1999)
- DGA-GAM-EG-13 « Essais généraux en environnement des matériels » (1996)
- CIN-EG-01 « Guide pour la prise en compte de l'environnement dans un programme d'armement » (1999)

Functional Analysis (F.A.)

Purpose (What for?)

Approach to search, set in order, characterize hierarchies and/or valorize functions, (French Standard NF X 50.150).
Such functions are attached to production - material, software, process, service as expected by user.

Description (What does the method produce and how?)

Two kinds of functional analysis are to be expected:

- External Functional Analysis (E.F.A),
- Internal Functional Analysis (I.F.A.).

External Functional Analysis, so called "need functional analysis", aims at describing, for each life profile situation, product expected functions. Other functions, corresponding to reactions of adaptation necessary to take into account product environment, are also to be defined, as well as user justified constraints. The whole of this data package is gathered in the Functional Request for Proposal (F.R.f.P.).

Internal Functional Analysis, or "Technical Functional Analysis", aims at establishing relationships between external functional analysis and solutions to be considered in order to satisfy the expressed need. The functions identified through external functional analysis are declined into functions of lower order, so called « technical functions » which materialize functional solutions and techniques open to be retained, knowing that final goal is to have access to objective comparison elements between various solutions.

Method Implementation (How is it settled?)

The functional analysis approach is conducted under participative manner by dedicated working group who gathers all necessary skills coordinated by a group manager. It relies upon recognized methods among which:

- APTE ®,
- Value Analysis,
- RELIASEP ®,
- SADT,
- SART,
- MERISE,
- GRAFCET...

The choice of method depends on the product to study and the kind of study to do.

Relevance Area	Inputs	Outputs
- All systems: APTE, - Value Analysis: RELIASEP, - Computer Systems: SADT, SART, - Organizational Systems: MERISE, - Automation Systems: GRAFCET. Functional analysis is applicable at each phase of product life cycle.	- External Functional Analysis: user needs and constraints, - Internal Functional Analysis: system architecture.	- Choice criteria for technical solutions to be considered to answer user needs, - Input elements to perform Failure Mode Effects and Criticality Analysis (FMECA) or Reliability Block Diagrams (RBD). As a rule, functional analysis is a preamble to dependability and safety studies.

Pros	Cons	Bibliography
- Functional analysis allows to precise "as best as possible" the real user needs to convert them into functions to be performed and help to optimize product/need adequacy without considering any technical solution. Besides, it makes up a common reference table between designer and dependability/safety analyst. Through recognized methods application, functional analysis permits to improve a program management in terms of costs, deadlines and performances.	- Functional Analysis setting complexity depends on adopted method. The quality of results is highly dependent on the group manager ability to apply retained method.	- DGA/AQ 922 : "Mémento de l'analyse fonctionnelle", - NF X 50.100, 12/1996: "Analyse fonctionnelle – Caractéristiques fondamentales", - Projet ISdF 1/91: "L'analyse fonctionnelle en matière de Sûreté de Fonctionnement".

Reliability Block Diagram (R.B.D.)

Purpose (What for?)


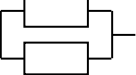
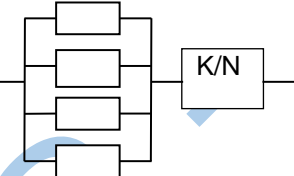
Graphical methodology permitting visualization of system sub-assemblies as to show their contributive participation to functions concurring to mission success. It is used as a basis for the various models built to quantify system reliability or safety.

Description (What does the method produce and how?)

A representative diagram specifying items of equipment contributing to mission success, namely redundancies or elements contributing to a same function and necessary emergency elements.
Mission may be under stationary regime, transient regime or by phases

Method Implementation (How is it settled?)

1. Functional Analysis: connections between items of equipment and functions contributing to mission are established
2. Modeling: representation maybe under the following forms:

- Serial equipment, 
- Parallel equipment, 
- Or partial k/n redundancy, 

Relevance Area

-The Reliability Block Diagram method is a method contributing to Reliability, Maintainability and Safety analysis and hence availability which permits to evaluate compliance of a system face to mission objectives. Owing to the representation with partial redundancies, it permits to determine acceptable degraded modes, the redundancy levels being a negotiation matter.

Inputs

- System functional drawings,
- R.A.M.S. studies, F.M.E.C.A.
- System logistic breakdown and associate maintenance concept.

Outputs

- Reliability or Availability diagrams.

Pros

- Simple and logical display of system functioning,
- Mission profile taken into account in equipment characteristics,
- Visualization of mission performed by the system.

Cons

- Redundancy level acceptable for degraded modes is arbitrary,
- Difficulty to take into account multi-functions elements,
- In such a case, method is to be applied jointly with FMECA.

Bibliography

- **MIL STD-756B**: Reliability modeling and prediction.
- **Sûreté de Fonctionnement des Systèmes Industriels**: Villemeur, Collection de la Direction des Etudes et Recherches d'Electricité de France, Editions Eyrolles.
- **NF EN 61.078** : Techniques d'analyse pour la sureté de fonctionnement - Bloc-diagramme de fiabilité et méthodes booléennes, 2006.

Reliability Allocation (R.A.)

Purpose (What for?)

Reliability allocation consists in declining reliability objectives required at complex product level (i.e. system) into objectives applicable at the various levels of technical or functional product breakdown (« top down » approach type).

Description (What does the method produce and how?)

Reliability allocation is an **iterative approach**. It often requires several attempts to be able to comply with top-level objectives. It should be initiated in **Feasibility phase** as soon as design reliability requirements are derived from requirements stated after operational performances. Normally, a first allocation should be performed before design process as to serve as an input to functional design review to be held during design phase. Recover and updates are to be further performed before each major design review.

Method Implementation (How is it settled?)

1 – Fix complex product breakdown levels as to satisfy at best designer's needs.
If need be, it may be a function (service function or, sometimes, technical function) or a material sub-assembly (i.e. complete equipment subassembly, mechanical organ, electronic board...). Practically, the choice of breakdown level has to rely upon number of criteria: product complexity, design flexibility at various breakdown levels, safety criteria, external sub-contracted entities, a.s.o.

2 – Set a method well adapted to project constraints.

Several methods, among which some may refer to operational research techniques, may be considered in order to determine reliability objectives at various product breakdown levels.

The most common points are the following:

- **Equidistribution reliability method:** It consists in attributing the same reliability objective to each entity of a given product breakdown level. This is the roughest method knowing that it does not take into account neither of nature and configuration of entities, nor of technical feasibility.
- **ARINC method:** It supposes that elements taken into account in system breakdown are serial on a reliability standpoint and are of constant failure rates. Based upon some degree of knowledge of element failure rate (from field experience or provisional evaluations on similar entities) the method consists in determining each entity respective reliability weight on the overall system reliability. The allocated reliability objectives are supposed to comply with this weighing.
- **AGREE method:** This method relies upon the same hypothesis as ARINC method; nevertheless, it takes into account the complexity of entities and its implication in reliability of overall system. Algorithms used are more complex than for ARINC method.
- **Strain minimization method:** allocation of requirements as to minimize strains necessary to comply with global objectives. Strains can be expressed in financial terms, in number of tests to be performed, in number of necessary analysis, a.s.o.

Whatever the algorithm could be, reliability allocation policy shall comply with two main requirements:

- be realistic, i.e. avoid requiring objectives non-feasible regarding size, deadlines...
- be efficient, i.e. aiming to decrease some servitude (costs, deadlines, consumption...) or increase functional performances (accuracy, power, stability, a.s.o.).

The major interest of reliability objectives attribution at various levels of breakdown, in case of complex product, is to provide designers with reference marks as help for design choices or reliability tests management.

Relevance Area

Applies mainly to complex systems. Three kinds of actors can be concerned by allocation policy:

- **The customer (or contracting authority)**, who defines the system mission profiles and associate reliability objectives,
- **The project supervisor** who should normally perform the reliability allocation for the various subsystems, assuming sufficient knowledge of all subsystem design options,
- **The subcontractors** who have to take care of feasibility of design options compliant with reliability objectives, and their development until validation before Production phase.

Inputs

- Objective(s) at system level,
- Accepted breakdown level,
- Subassemblies configuration.

Outputs

- Objective s at sub-assembly level.

Pros

- Breakdown of system reliability objectives into subassembly objectives permits to size efforts to be applied on various subassemblies (technical or functional), to manage design and production actions,
- Should some subassemblies be developed by an external subcontractor, the supervisor allocated objectives become top-level allocations and hence require their own reliability program to be proposed and performed by the subcontractor himself. In any case, a consistent reliability allocation program leads designers to consider reliability as a main design characteristic, as important as any other characteristic such as cost, weight, consumption or any other functional product characteristic.

Cons

- Depends mostly upon reliability data relevance.

Bibliography

- MIL HDBK-338 « Electronic Reliability Design Handbook »
- KC Kapur & LR. Lamberson « Reliability in Engineering Design » (John Wiley & Sons)
- RAC Blueprints for Product Reliability.

Predictive Reliability Assessment (P.R.A.)

Purpose (What for?)

The task aims at evaluating and refining, with increasing accuracy degree along with program advance, the product reliability potential. Techniques and data generally change with design progress and test results collection. Reliability provisional evaluation is an important basis to design choices and allows comparison of predicted reliability potential with required objectives, even before test or operational data collection.

Description (What does the method produce and how?)

Provisional reliability evaluation is an **iterative process**, which is to be initiated during **Feasibility phase**, as soon as product design data becomes available. It is followed and refined during **design phase** along with design process advance, when operation component knowledge gets more and more accurate and maybe when significant test results can be obtained.

Method Implementation (How is it settled?)

1 – Select when project begins the assessment method best adapted to product nature and requirement manner (ex: MTBF, durability...). It is however possible to change method following program advance when design data becomes more and more accurate (i.e. component technology, usage conditions, applied stress...).

2 – Determine the failure classe(s) to be considered as priority in reliability estimate in order to choose the most adequate. The three following failure classes shall be considered

- Youth failures, which result during early operating times in a failure rate decreasing with time,
- Random failures, which result during « useful life » in a constant failure rate,
- Wear out failures beyond useful life result in a failure rate increasing with time.

To that end, the table 1 on following page shows a synthetic description of **the five most classical provisional assessment methods** and their range of covered failure classes.

3 – Let the method change following program phases. The table 2 on following page displays a selection of methods which can be considered following program advance.

Relevance Area

Two generic models of provisional assessment:
- Empirical models based upon failure rates (« part count » or « part stress » types),
- Deterministic models based upon physics of failure.

Table 4 on following page illustrates the various conditions in favor of either model for reliability provisional estimate of a product, a subassembly or a component.

Inputs

- Subassemblies / components list,
 - Definition of operation and environment stresses,
 - Upper level objectives.

Outputs

- Following project nature and objectives fixed by the subscriber, reliability and safety characteristics.

Pros

Numerous benefits are expected from a provisional reliability assessment, namely:

- Quick verification of technical feasibility face to required reliability objective,
- Settlement of reliability allocation,
- Input for critical points ranking...
- Comparison means of competitive technical solutions on a reliability standpoint,
- Guide for component choice (types, technologies...) and their acceptable usage conditions,
- Input for spare parts stocks estimation,
- Input for Product Life Cycle Cost estimate.

Cons

- Strongly dependent upon project data relevance.

Bibliography

- See table 3 next page.

1 - Methods of provisional estimate and aimed failure classes

Method	Youth failures	Random failures	Wearout failures	Method Description
Empirical Models with failure rates	X	X		Relies upon mathematical models of elementary component failure rates (based upon field experience). Two methods in Electronics: - « part count » method taking no account of operation stresses, - « part stress » method taking into account operation stresses (electrical, temperature...).
Translation	X	X		Performs translation from provisional estimate based on empirical models to operational reliability estimate. Implicitly takes into account external factors, which affect operational reliability (not accounted in empirical models).
Physics of failure (determinist)			X	Relies upon physical models, which describe degradation mechanisms evolution for some mechanical or electronic components or for assembly processes. Overall reliability, linked to wearout, is obtained by combination of probability densities associated to each failure mechanism.
Data on similar products	X	X	X	Relies upon empirical reliability data observed on similar products. Similarity shall include complexity, maturity, manufacture process, product functions and use conditions. Generally requires use of conversion factors to integrate variations in complexity, in processes, in usage, etc...
Test data	X	X	X	Database includes data « home made » from tests performed on development samples of considered product. Requires use of translation coefficients to perform extrapolation to field experience reliability.

2 - Methods to be considered following program advance

Program advance	Application level	Possible Methods
Functional Concept (Feasibility phase)	Product or system	Data on similar products, translation. Empirical models (« part count »).
Initial design (Design phase beginning)	Equipment or sub-assembly	Data on similar products, Empirical models (« part count »).
Final design (At the end the design phase)	Circuit or component	Empirical models (« part stress »), test data, failure physics.
Tests (design / production phases)	From component to complete production	Test data, failure physics.

3 – Data sources of various provisional assessment methods

Provisional assessment methods	Sources of models or data
Empirical models with failure rates	- « Part count » method for electronic components: <ul style="list-style-type: none"> MIL HDBK-217F notice 2, Bellcore TR 332, British Telecom HRD5. - « Part count » method for mechanical components and others: <ul style="list-style-type: none"> NPRD-95 « Non electronic Parts Reliability Data », RADC TR-85-194 RADC TR 75-22, « RADC Non-Electronic Reliability Notebook ». - « Part stress » method for electronic components: <ul style="list-style-type: none"> MIL HDBK-217F notice 2, RDF 2000 (UTE C 80-810), FIDES, British Telecom HRD5, SIEMENS-NORM SN 29.500 (part 1)
Translation	RAC Reliability Toolkit: Commercial Practices Edition, RADC TR 89-299.
Failure Physics	RADC TR 90-72, CINDAS Data, Components and mechanical parts (springs, bearings, etc) reliability generic models, manufacturer data.
Data on similar products	Data Bases (external or internal) including necessary information, number of failures, operation durations, off durations, number of cycles, environment...
Test data	« Home made » test results with accurate environment conditions (number of cycles, applied stresses, durations...).

4 - Comparative pros of empirical models and determinist models

Empirical models (failure rate)	Determinist models (physics of failure)
- Recommended for complex products, - Recommended for quick analysis, - Recommended for comparative analysis, - Recommended in case of lack in design flexibility, - Usable for component selection and for stress estimate (electronic components).	- Recommended to estimate degradation mechanisms influence upon component life duration, - To be considered when detailed information related to technology and process are available, - To be considered when design flexibility is sufficient, - Usable to facilitate component failure cause research.

FIDES

Purpose (What for?)

Assess electronic equipment reliability. This method is also applicable to systems operating under severe environments (defense, aeronautics, industrial electronics, transport...), including non-operating phases.
Provide a concrete tool for building and managing reliability studies.

Description (What does the method produce and how?)

FIDES methodology has been developed under DGA (*Direction Générale de l'Armement, Agency of French Department of Defense*) authority by a consortium including AIRBUS, EUROCOPTER, GIAT, MBDA and THALES companies. It is based on failure physics and supported by test data analysis, field experience and existing models. It differs from classical methods developed mainly through statistical exploitations of field experience data.

FIDES methodology deals with the whole of failures to be attributed to requirement, design and manufacture of the final product. Nevertheless the following failures are not considered: failures of software origin, non confirmed breakdowns, failures linked to preventive maintenance operations not performed, failures linked to accidental aggressions, when defined and authenticated (failure propagation, out of requirement range usage, wrong handling).
The method permits to deal with non-operating phases, whatever their nature.

FIDES methodology is applied to components, electronic boards or COTS subassemblies (COTS: Component Of The Shelf), and to specific items when their technical characteristics correspond to the guide's. The goal is ultimately to replace MIL HDBK-217, not updated after 1995 and RDF2000, not adapted to severe environments.

Method Implementation (How is it settled?)

The COTS (component, electronic board, sub assembly) failure rate is assessed from the following expression:

$$\lambda = \lambda_{\text{physique}} \cdot \Pi_{\text{Part manufacturing}} \cdot \Pi_{\text{Process}}$$

$\lambda_{\text{physique}}$ represents the physical contribution. It takes into account COTS life profile (phases, environment conditions), as well as accidental overloads which may occur and are not identified as such (« overstress »).

$\Pi_{\text{Part manufacturing}}$ evaluates quality and COTS manufacture technical control. Its evaluation method depends on COTS nature. Its value is between 0.5 to 2.0 (worst case).

Π_{Process} evaluates quality and technical control of development process, manufacturing and maintenance of the equipment, which includes COTS. The evaluation method is based on a recommendation application level during the whole life cycle and supported by an **audit**. Its value varies from 1 to 8 (worst case).

Relevance Area	Inputs	Outputs
- FIDES methodology is applicable to all areas of electronics use, military, aerospace, automotive, rail, telecommunications, computer... However, some components such as thermistors, variable capacitors, or some subassemblies such as plasma screens, typed in italic in the guide, will be treated later...	- Life profile, environment and use conditions of equipment using COTS, - Data on: <ul style="list-style-type: none"> • Equipment definition, • Equipment life cycle, • Suppliers of items used in equipment. 	- Failure rate, - Audit balance sheet.

Pros	Cons	Bibliography
- FIDES methodology takes into account the whole equipment life cycle, including non-operating situations. It is not limited to the component failures, but is extended to the whole product, - Unlike in ongoing standards, the "reliability" process is evaluated including COTS and recommendations are proposed for the whole life cycle.	- Assessment quality relies upon multiplicative factors, thus special care is to be brought to audit performance leading to « Process » quantification.	- FIDES guide , first edition 2004 « Reliability methodology applied to electronic systems », - Internet address: fides@innovations.net

Reliability assessment from tests or field experience

Purpose (What for?)

- Determine reliability laws parameters from data obtained through tests or field experience as to:
1. Assess operational reliability in order to compare with specific requirements at system or equipment level,
 2. Measure observed reliability level evolution (positive or negative).

Description (What does the method produce and how?)

Various mathematical laws depending on failure nature and degradation phenomena can describe component reliability $R(t)$. The most frequently used are the exponential law and the Weibull law, which can completely be defined by their parameters determination.

The exponential law is characterized by the failure rate (λ) or the Mean Time To First Failure (MTTF).

Weibull law is characterized by the shape factor α , the shape parameter (β), and the position factor (γ).

The observed event reading on operating or on test equipment (failure, survival, preventive maintenance, counter reading...) and their dating allow assessing law parameters, as their associate confidence intervals. The methods used can be graphical or numerical.

Method Implementation (How is it settled?)

Reliability laws parameters assessment is founded upon data of events observed on actual equipment. After the collection, the selection and sort of raw information steps the following tasks are necessary for parameters determination:

1. Chronological event sorting following apparition date *
2. Reliability law non parametrical approach \Rightarrow points layout $Y_i = F(t_i)$ (following median rows, Kaplan-Meier...)*,
3. Computation or graphical assessment (Weibull paper for example) of chosen laws estimators,
4. Confidence intervals computation.

*Nota: Those two steps are optional for exponential law parameters or for a maximum probability type approach...

Relevance Area

- This assessment is relevant when field experience is structured and provides consistent data:

- Defined failure modes,
- Controlled test conditions: temperature, vibrations...
- Similarity of use profiles, mission profiles, life profiles...
- Characterization of times.

Inputs

- Events when operating on a given period (failures, counter captures, maintenance interventions...) Reliability test results, censored or not censored linked to acceleration factor when accelerated tests.

Outputs

- Reliability parameters along with their confidence intervals and by extension, reliability laws, failure rates, observed reliability level, statistical risk in product or decision acceptance...

Pros

- When caution is given, data obtained is by definition the closest of actual,
- Simple computations for exponential law,
- Quality of results (level of reliability, trends, failure mode information...).

Cons

- Limits when not numerous data: rare events, single shot systems,
- Complex computations of Weibull parameters estimate (need of a software for confidence intervals),
- Collection methodology must be meticulous and homogeneous with time, which could require extensive means...

Bibliography

- Projet ISdF 2/96. Estimation de la fiabilité d'un produit (nouveau ou existant) à partir de retours d'expériences multiples et d'expertises.
- NF X 06.501 (AFNOR-1984) – Applications de la statistique. Introduction à la fiabilité.
- **IEC/ISO-31010** – Dependability management – Application guide.
- **CEI/ISO-61124, ed2** : Essai de fiabilité - Plan d'essai pour démonstration de taux de défaillance constant.
- J. Ringler (Octares/ISdF) – Précis de probabilité et de statistiques à l'usage de la fiabilité.
- A. Lannoy – H. Procaccia (Eyrolles) – Méthodes avancées d'analyses de données du retour d'expérience industriel.

Predictive Mechanical Reliability Assessment

Purpose (What for?)

The purpose of Predictive Reliability Methods is to produce a priori estimates of the reliability of a *devices/systems/product*, according to potential failures mechanisms, which could affect them. These estimates can be used during design, in order to demonstrate that the provisional reliability meets the required one, as well as in operation, for instance to improve the safety of the device/system/product, or to extend its operating time. Predictive Reliability Assessment methods were developed initially for electronic systems, and based originally on the assumption of constant failure rate during operating life. This assumption may be applied (very carefully) to « simple » mechanical components, produced in great quantities, with a single failure mode, but is generally not applicable to « mechanical dominant » systems, when failure modes (fracture, distortion, galling, noise...) related to fatigue, wear and ageing appear early in the life cycle. The purpose of « Mechanical Reliability » is therefore to make available to designers a set of *just necessary* predictive reliability assessment methods, taking into account the actual failure mechanisms, and fitted to each particular case

Description (What does the method produce and how?)

At the end of the « classical » steps of qualitative predictive reliability analysis (FMECA, Fault Tree Analysis), three approaches of Predictive Mechanical Reliability Assessment are proposed, for each component:

1. The component is close to similar components described in « constant failure rates » databases, used in similar systems, under similar conditions of operation and maintenance: it is therefore possible to use constant failure rates (with associated confidence intervals as far as possible), after checking the validity of those assumptions. (see in annex 1 a list of available databases)
2. The component belongs to a list or catalogue of « standard components », on which sufficient reliability field data are available to allow manufacturers to supply ad-hoc Predictive Mechanical Reliability Assessment models according to operating conditions (stress spectrum); the data implicitly take into account the conditions of preventive maintenance of reference components. These models supply directly the temporal evolution of the component failure rate and reliability. The main laws of failure used are log-normal and Weibull distributions. This kind of approach is particularly applicable to components such as bearings, springs, gears, electromechanical components...
3. The component is not described as a « standard component », or is used under specific conditions: it is then recommended to use « stress - strength » type methods, allowing to estimate provisional reliability from damage models fit to the physics of stresses of the component (wear, high cycle fatigue, low cycle fatigue...). The use of these methods allow to go further than classical dimensioning methods, by quantifying the risks associated with the use of « safety factors », and optimizing the design according to reliability requirements (see sheet « Stress-Strength Analysis »)

Method Implementation (How is it settled?)

- System Functional Analysis and statement of the Functional Block Diagram,
- Determination of the conditions of use (stresses in each operating condition),
- Qualitative Analysis (Preliminary Hazard Analysis, FMECA, FTA...) and determination of critical components and failures,
- Reliability modeling (Reliability Block Diagrams).
- For each component:
 - collection of field and expertise data,
 - choice of the best adapted Predictive Reliability Assessment method (see here-above) according to the type and criticality of the component,
 - determination of the stresses (mechanical, thermal...), and of their statistical and temporal distribution,
 - collection of component data (and, if necessary, definition and implementation of reliability tests in order to determine the characteristics used in predictive reliability models),
 - component Predictive Reliability Assessment (Bayesian methods may be used for innovative components, or when the component preventive maintenance is modified).
- System Predictive Reliability Assessment.

Relevant Area	Input	Output
<ul style="list-style-type: none"> - The relevant area of each Predictive Reliability Assessment method is strongly dependent on: <ul style="list-style-type: none"> • the robustness of field data on which input data are built, • the context and objectives of the study. - Because of the limits of these methods (see « pros and cons » hereafter), a mechanical reliability assessment deals not to calculate the reliability to the decimal, but rather, in the case of dynamic stresses, to have a more precise approach compared to the use of safety factors, by aiming to take into account most of factors. 	<p><u>System level:</u></p> <ul style="list-style-type: none"> - Mission profile, statistical distribution of stresses, in nominal, degraded, catastrophic mode, - Maintenance policy and conditions, - RAMS requirements, - Regulation requirements, - Technical and functional requirements, - Drawings and calculation files. <p><u>Component level:</u></p> <ul style="list-style-type: none"> - Component FMECA, maintenance model... - Field data in similar conditions of use (failure rates, law of mortality...) or test results, - Failure modes and failure physical mechanisms (distortion, fatigue fracture, wear, corrosion...), - Characteristics of stress resistance, associated with statistical distribution. 	<ul style="list-style-type: none"> - Reliability estimation at system level, - Knowledge of components, critical failure modes, and recommendations about design choices at system level (redundancies) and component level (materials, dimensioning), - Knowledge of risks linked to the use of safety factors, - Design optimization based on RAMS requirements, - If necessary, definition of determination, tests for material characteristics, validation tests, confirmation tests, - Maintenance recommendations (input data for RCM – Reliability Centered Maintenance – approaches).

Pros	Cons	Bibliography
<ul style="list-style-type: none"> - Taking into account failure modes specific to mechanical components, - Taking into account the random nature of the constraints and resistance, - Optimization of design (as opposed to safety factor application), - Risk assessment in the form of a probability, as opposed to the binary decision linked to the safety factor application, - Possibility to perform sensitivity studies and decision support studies. 	<ul style="list-style-type: none"> - « Mechanical Reliability » cannot be reduced to « Weibull distribution » or « Stress-Strength Analysis ». The choice and implementation of reliability assessment methods suited to each component and to each context of study require a good knowledge of the bases of mechanics AND reliability, - The « mathematical rigor » of models and their ability to « produce decimals » must not conceal that the precision of estimates is dependent on: <ul style="list-style-type: none"> • the completeness of the qualitative analysis (a failure is often linked to an « forgotten » cause or combination of causes), • the quality of input data (still limited knowledge of the statistical distribution of real stresses and strengths), • the gap between the model and the physical reality. - Conversely, constant failure rate tables should be used with great caution, being aware of the fact that they generally represent only a first approximation 	<ul style="list-style-type: none"> - CAZAUX, POMEY, RABBE, JANSSEN – La fatigue des métaux – Ed. Dunod. 5ème édition - 1969 - C. MARCOVICI et J. C. LIGERON - Utilisation des Techniques de Fiabilité en Mécanique - Ed. Lavoisier, 1974. - J. C. LIGERON - La Fiabilité en Mécanique - Ed. Desforges, 1979 - Maitriser l'usure et le frottement - Ministère de l'industrie, Programme national d'innovation, 1980. - BARTHELEMY – Notions pratiques de mécanique de la rupture – ed. Eyrolles, 1990 - C. BATHIAS, J. P. BAILON – La Fatigue des Matériaux et des Structures – Ed. Hermès, 1997. - T. R. MOSS - The Reliability Data Handbook – ed. Professional Engineering Publishing, 2005. - SHIGLEY – Mechanical Engineering Design – ed. Mc Graw Hill, 8th edition - 2006 - J. C. LIGERON - Cours de fiabilité en mécanique – Groupe de travail IMdR M2OS – availability: 2009

Annex 1 – List of available databases for mechanical components failure rates

Name	Origin / accessibility	Last updating
FARADA	FAilure RAte DAta bank Developed par the GIDEP (Government Industry Data Exchange Program) – US Renamed « Reliability-Maintainability Data Interchange ».	1973
IEEE Std 500	IEEE Guide to the collection and presentation of electrical, electronic, sensing, component and mechanical equipment reliability data for nuclear power generating stations Available at IEEE (Institute of Electrical and Electronics Engineers).	1983
RADC TR 85-194	RADC Non-Electronic Reliability Notebook Available at Rome Laboratory, ex Rome Air Development Center (RADC), US Air Force laboratory.	Rev. B - 1985
NPRD 95	NPRD 95 Non-electronic Parts Reliability Data Available at RIAC and SPIDR™ (Space Physics Interactive Data resource) ex Alion System Reliability Centre (SRC).	1995
EIReDA	European Industry Reliability Data Handbook With contribution of C.E.C. - J.R.C./ICEI 21020 ISPRA (Varese) Italy et EDF - DER/SPT 93206 Saint Denis (Paris) France.	Handbook: 1998 Updated software : 2000
T-Book	Reliability data of components in nordic nuclear power plants	6 th edition - 2005
OREDA	Offshore REliability DAta Managed by petroleum industry	5 th edition - 2009

Note: this list is not exhaustive. Some databases may not have been updated.

Mechanical Reliability – The Stress-Strength Analysis Method

Purpose (What for?)

To assess the reliability of mechanical parts subject to stresses. This reliability is expressed by the probability that, for each operating phase of the mission profile, the mechanical stress at any point of the part is lower than the strength of the part.

Description (What does the method produce and how?)

The method is based on the application of calculation techniques of mechanical parts for each type of stress experienced by the part:

- Constant stresses,
- High cycle fatigue,
- Low cycle fatigue,
- Wear,
- ...

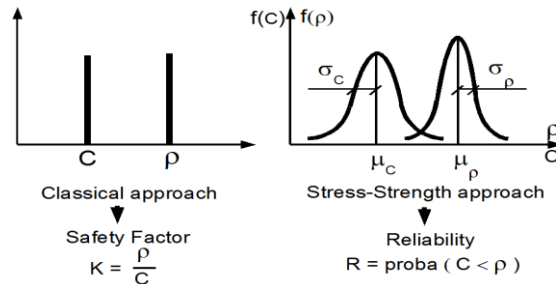
It is based on a statistical description of:

- the applied stress cycle, integrating as far as possible the « exceptional » stresses (peak stresses) and the foreseeable risks associated with the mission
- the statistical characteristics of the strength of the material (corresponding to each type of applied stress (tensile strength, yield strength, fatigue limit, fracture K-factor...), taking into account the uncertainties related to the material (heterogeneity, ageing...), to the manufacturing and implementation of the part (machining, heat treatment, assembly...), and to external factors (temperature, humidity...).

This reliability at each point of the part is expressed by the probability that, for each failure mode, the applied stress ("constraint" C) is lower than the material strength ("resistance" ρ) of the part.

$$R = \text{Proba}(C < \rho) = \text{Proba}(X = C - \rho < 0)$$

In the "textbook case" where stress C and strength ρ are normally distributed random variables with respective characteristics (μ_C, σ_C) and (μ_ρ, σ_ρ), the variable X =



C follows a normal distribution of mean value (μ_C = μ_C) and variance (σ_C² = σ_C²).

Beyond the safety factor k = ρ/C it is possible to calculate the reliability of the part: R = Proba(X > 0).

In other cases (other distributions), it is necessary to use more sophisticated statistical techniques to compare stress and strength:

- Algebra of random variables,
- Monte Carlo simulation,
- Mellin transform,
- Approximation methods (FORM/SORM – First / Second Order Reliability Methods).

Method Implementation (How is it settled?)

- Determination of the envelope profiles of use of the part (specifications, feedback...),
- Analysis of parts failure modes and damaging factors,
- Determination of the stresses and of their statistical characteristics in « critical zones » (measurement, resistance of materials, material fatigue models, theories of damage, fracture mechanics, finite element...),
- Determination of the statistical strength characteristics of the material, associated with each mode of damage ("catalogue" materials data, feedback, determination test results...),
- Comparison of stress and strength in the « critical zones »,
- Predictive Reliability Assessment, compared to reliability requirements, and recommendations for optimization (design, maintenance...).

Relevant Area

- Knowledge needed of:
 - the damaging modes of the part,
 - the statistical distribution of stresses for each damaging mode,
 - the statistical distribution of strength characteristics of the material.
- Even with data of « good quality », the results obtained have to be used very cautiously.

Input

- Mission profile,
- Mechanical calculation results,
- Statistical data on materials strength characteristics,
- Damaging models, for each type of stress.

Output

- Parts estimated reliability,
- Recommendations for complementary tests,
- Recommendations for optimizing the design, implementation, maintenance...

Pros

- The method allows going beyond the application of safety factors that are relevant only in very specific cases of use and that do not take into account the uncertainties on stress and strength characteristics,
- The method allows issuing recommendations for optimizing the design, implementation and maintenance.

Cons

- It is sometimes difficult to collect robust input data on the damaging factors, the statistical distribution of stress and strength,
- The calculation of the stresses (Resistance of Materials, finite elements...) and their limits can make use of models and methods of mechanical calculation to be used by specialists and evolving constantly,
- The predictive reliability assessment can make use of « sophisticated » statistical methods and of important computing means.

Bibliography

- E. B. HAUGEN – Probabilistic Approach to Design – Ed. Wiley and Sons 1980.
- O. DITLEVSEN, H. O. MADSEN – Structural Reliability Methods – Ed. Wiley and Sons 1996.
- N. RECHO – Rupture des structures par fissuration – Ed. Hermès 1995
- H. PROCACIA – P. MORILHAT – Fiabilité des structures des installations industrielles – Ed. Eyrolles 1996.
- A LANNON – Lifetime management of structures - ESReDA DNV, 2004
- M. LEMAIRE et al - Fiabilité des structures: couplage mécano-fiabiliste statique - Ed. Hermes 2005.
- J. BAROTH and al. - Fiabilité des ouvrages, sûreté, sécurité, variabilité, maintenance - 2010

Choice and application of software dependability analysis methods

Purpose (What for ?)

The purpose is to build dependability ^{*1}, to analyse, to reduce and assess a software bug occurrence as early as possible in a new software design. To that end, one must have appropriate activities depending on project advance and development and to apply them consequently.

Description (what does the method produce and how ?)

Dependability building is an **iterative process** to be initiated in feasibility phase during product specification building as soon as design data is available. It is then continued and refined during **design phase** steps, all along design process advance with knowledge more and more precise of components operation conditions and potential acquisition of significant test results. It is continued during test phase and possibly in operation.

Five major activity groups are defined relying upon methods and approaches ranged in chronological order from feasibility to implementation of software

1. Activities in compliance with regulation (qualification development companies, specification of software product). They lead to specify means, tools, analysis methods,
2. Activities based on software metrics (i.e. Reliability prediction methods, RADC TR 85 228, Sofmat...),
3. Activities based on subjective methods (Bayesian),
4. Activities based on tests,
5. Activities based on Reliability Growth Models, i.e. Goel-Okumoto, « S » curve...

Table 1 in appendix provides a succinct description of the various activities. Future sheets will detail some points.

Method implementation (how is it settled ?)

There is not an implementation but implementations that are based on the following factors :

1. Is there or not in a domain where regulation is mandatory?,
2. At the project start, selection of the method(s) best adapted to project nature and to the manner of objectives specification. However change of method remains possible depending program advance when design data is more and more accurate.
3. Determination of bug class to be considered as a priority in reliability assessment taking consequences into account in order to chose the most adequate assessment method.
4. Method evolution, depending upon life cycle phase implementation.

Relevance Area

- The relevance area depends mainly on regulation when applicable and the phase of method implementation.
 - To do this, methods shall be :
 1. Useful and usable,
 2. Accurate enough for the required level,
 3. Applicable early enough to be efficient,
 4. Discriminant to take into account :
 - The human investment as well as material,
 - The development process quality,
 - The architecture, as well software as material,
 - The components diversity (newly developed or Components Off The Shelf "COTS"),
 - Use conditions,
 - A ratio **cost / efficiency** depending on incurred risk.
- Table 2 in appendix shows the phases where each activity is generally applicable.

Inputs

- The specification as required,
- Organization and means of specifier and performer,
- Software specification, analysis file, project organization and development plans,
- Development rules, implemented tools,
- Documented test results and detailed description of encountered bugs.

Outputs

- Validation of software experts rules to be applied to software,
- Identification of most probable bug risks and their consequences.

Pros

See table 3

Cons

See table 3

Bibliography

See table 4

Table 1 : Brief Description of the activities

Activities	Description of the activities
Regulation based, analysis methods	Following application fields, software shall comply with standards. This concerns air, railway and road transport and also many other areas such as nuclear, military, medical and others. The standards define the way with which the software is to be specified developed and tested; they define also the specified acceptable level (SIL class) depending upon consequences of their activation and the field specificities. As for material, analysis methods do exist such as Software Error Effects Analysis (S.E.E.A.). These methods have to be performed with concern in order to avoid to be drowned in too low level.
Software metrics based	There are numerous metrics in software area. Among the oldest and most famous , one finds the metrics allowing cyclomatic number and the metrics based on instructions number for a given " module" of code. Other methods are more finalized and perform the synthesis of a number of metrics and model the software. Their objective is to assess the bug occurrence number, not for itself but in order to compare various development solutions towards designer orientation into a way of minimizing the bug occurrence. SOFMAT method is one of them.
Subjective (Bayesian)	Subjective methods allow to associate developers experience with insufficient test results in a statistical meaning. The Bayesian statistics allow to formalise this association. They are used for material as well as software.
Test based	This is pure statistic. As in the material case, these methods most frequently allow to assess bug frequency occurrence. The objective is then to assess a test characteristic such as the test coverage rate. The main concern is to appreciate the calendar, activation, cycle time.
Reliability growth	Numerous models of reliability growth have been developed. The most famous are Jelinski-Moranda, Littlewood, Goel-Okumoto, Musa, S shaped... They allow to describe software reliability growth during validation as and when bugs occur when errors are corrected.

Table 2 : Activities following program advance

Program Advance	Possible activities				
	Regulation Analysis	Metrics	Subjective	Test	Growth
Functional concept (feasibility phase)	X	X			
Initial design (design phase)	X	X			
Final design (definition and development phase)	X	X	X		
Tests (validation)	X	X	X	X	X
Operation	X		X	X	X

Table 3 :Activities Pros / Cons

Activities	Cons	Pros
Rule based, analysis methods	<ul style="list-style-type: none"> - Standards often inaccurate and qualitative, - What duration taken into account, it is not their purpose - Standards exclude connection between actual reliability and SIL level (Safety Integrity Level) required for software. - Analysis methods may be sometimes hard to be applied, i.e. in case of short operation duration 	- From required software safety level (SIL), methods and technics to be implemented are recommended or even imposed or regulatory..
Software metrics based	- Difficult to validate (see COMSPIS Project – NUREG).	<ul style="list-style-type: none"> - Allow comparison of performance difficulties of various architectures or development processes, - Allow distinction between critical faults and "light" faults (i.e. display in some cases), - Some modelling methods allow assessment of reliability < 10⁻³.
Subjective (Bayesian)	- Do not prevent from test results with their own pros and cons.	- Allow to take into account qualitative data (i.e. Quality of development...).
Test based	<ul style="list-style-type: none"> - The end product is considered and not the development process. - Nothing is proven in lack of bug, - When bug is repaired , operation may continue, - Suppose that tests truly represent operation. 	<ul style="list-style-type: none"> - Is part of the acceptance process, - Gives information on test - Number and distribution of test data may be chosen.
Reliability growth	<ul style="list-style-type: none"> - Big systems are necessary to get sufficient number of bugs, nevertheless is it realistic for a product under operation ... - With proprietary systems such as OS, chronology is difficult to be respected. - Difficult distinction between critical faults and « cosmetic » faults for statistic history is unknown. - Only allow important unreliabilities, at best 10⁻³<<10⁻⁴. 	

Table 4 : Bibliography (chronological order)

Bibliography
1. IMdR –GT 63 , "Démarche et méthodes de Sûreté de Fonctionnement des logiciels" – Version 2 : 3 Avril 2013
2. DO-178C , "Software Considerations in Airborne Systems and Equipment Certification", RTCA/Eurocae, 1 – November 2011
3. Philippe Carer, Philippe Leclercq, "Maîtrise de la fiabilité des nouveaux systèmes numériques à ERDF, Application au futur système « Compteurs communicants » , λμ16, Avignon – Octobre 2008
4. NF X 61-508 : "Sûreté fonctionnelle : systèmes relatifs à la sûreté, Partie 3 : Prescriptions concernant les logiciels" – Mars 2002
5. Michael Lyu, "Handbook of Software Reliability Engineering", Computer Society Press McGraw –Hill – April 1996
6. Jean-Pierre Fournier, "Fiabilité du logiciel : concepts, modélisations, perspectives", Lavoisier – Septembre 1993
7. Philippe Leclercq, "A software assessment model, Annual Reliability and Maintainability Symposium", Las Vegas, January – 1992
8. NF X 71-013 : "Installations fixes et matériel roulant ferroviaires – Informatique – Sûreté de fonctionnement des logiciels – Méthodes appropriées aux analyses de sécurité des logiciels" – décembre 1990
9. Musa/Ianino/Okumoto, "Software reliability Measurement, prediction application", McGraw – Hill Company – 1987
10. RADC TR 85-228 , Vol 1, "Impact of Hardware/Software Faults on System Reliability: Study Results". E.C. Soistman / K. B. Ragsdale – December 1985

Software dependability: approach through standards

Purpose (What for ?)

The objective is not only to build dependability * 1 but meet regulatory requirements for the authorization of implementation, of service, a system, product containing an essential part of software . This demonstrates that it meets the applicable standard conditions, the authorization

Description (what does the method produce and how ?)

Two categories of standards are defined :

{1} When the company capacity of development of a system at a given level is at concern:

Company may be « qualified » at a given level and so justify an organization, an industrial capability and know-how which give credibility namely for calls for tender. Such a “quality” will impact not only products dependability but also the whole of the performances.

In this category, one finds mainly « CMMI » (Capability Maturity Model Integrated) and « SPICE » (Software Process Improvement Capability dEtermination). Those are not standards “stricto sensu” but rather guides or models.

CMMI includes 5 maturity levels divided in key sectors shown hereafter as an example :

1. Initial, does not include any sector,
2. Reproducible, project planning, quality assurance,
3. Defined, processes definition, software products engineering,
4. Masterized, quantitative processes and software quality management,
5. Optimized, technological and processes changes management.

These levels are the steps on the way to mature processes compliant with good practices observed all over the world in companies famed for their good process management. CMMI compliance is required namely for contracts with the American department of defense.

{2} When standards are by themselves part of the specifications.

A standard in that case declines and defines the know-how of the developers community in an application area to comply namely with safety objectives.

The standard is either for every application area, or for a specific one (Aerospace, Railways, Automotive..).

Method implementation (how is it settled ?)

Both categories defined here above lead to two different product managements.

{1} The first one is not tight to any particular project. It comes along the company life to define at its own expense the credibility from recognition date by an accreditation body, to extinguish at the company activity closure date, if occurred. At a given interval specified by the standard, the accreditation shall be renewed by the dedicated body to maintain continuity.

{2} On the contrary, the second is related to a specific project as soon as feasibility phase being a customer and ends at product removal at operator,

Relevance area	Inputs	Outputs
<p>{1} Companies qualification standards are relevant mostly for companies aiming at big contracts with public or private bodies and wanting to differentiate from competitors.</p> <p>{2} Standards required in specifications concern safety mainly in the fields :</p> <ol style="list-style-type: none"> 1. Aerospace, 2. Railways, 3. Automotive, 4. 	<ul style="list-style-type: none"> - {1} Implemented procedures at various levels and departments of the company. - {2} Organization and means of the specifier as well as the performer 	<ul style="list-style-type: none"> - {1} Company certification at a given level.. - {2} The file intended for the body in charge of operation allowance. - The software specification, the analysis file, the project organization and development plans, - The development rules, the implemented tools, - Documented test results and accurate description of encountered bugs.

Pros	Cons	Bibliography
<ul style="list-style-type: none"> - {1} Allow to justify a know-how, - CMMI is by itself an actual standard - {2} Provide a referential towards operation allowance. 	<ul style="list-style-type: none"> - {1} No guarantee offered for a defined project, the company may reduce its production costs and then apply only partially its know-how. - CMMI is seldom accused of lack of theoretical bases due to its definition through r « <i>good practices</i> ». - {2} May in some cases prevent implementation of various solutions not taken into account in the standards (new technologies...). 	<p style="text-align: center;">Bibliography</p> <p>{1} Capability Maturity Model® Integration (CMMI), SEI (Software Engineering Institute), Carnegie Mellon university.</p> <p>{2} EN 61-508 : “Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité (E/E/PES)”- 2011.</p> <p>Normes dérivées :</p> <ol style="list-style-type: none"> 1. CEI 61.511-2, procédés industriels – 07-2003 2. CEI 62.061, sécurité des machines – 01-2005 3. EN 50-126-2 / EN 50-128 / EN 50-129 : secteur ferroviaire – 2007-2011 4. CEI 61.513 ed2, secteur du nucléaire – 08-2011 5. ISO 26.262-1, secteur de l’automobile – 12-2011 <p>Eurocae DO-178C/ED-12B, « Software Considerations in Airborne Systems and Equipment Certification – 11-2011</p>

Software dependability: means, tools and analysis

Purpose (What for ?)

The objective is to build dependability by the choice of means, tools and analysis allowing to ensure the required dependability level at the various phases of the life cycle.

Description (what does the method produce and how ?)

It leads to define :

- The organization implementation :
 - The teams training to required technics, standards,
 - The means and organization of teams (staff and tools for adaptation of resources to development charges) to be compliant with schedule and costs.
 - Test teams and their means , their independence regarding development,
 - Experience background capability to track identified defects and repair them.
- The tools :
 - Specification tools,
 - Development workshops,
 - Tests workshops.
- The analysis :
 - By implementing :
 - Inductive and/or deductive methods allowing to define consequences of defects emergence (AEEL, ADD, Event tree,...),
 - Metrics based methods (ex : reliability estimateto be aware of :
 - Elements / defects most significant or frequent,
 - Identify means to reduce consequences and/or occurrence when necessary.
 - To identify defects :
 - Their cause(s),
 - Their nature,
 - Emergence conditions.
 - Most significant and/or frequent,
 - Their consequences and/or occurrence,
 - To check implementation of development rules, of coding for example,
 - In order to :
 - Order dysfunctions which deserve a design remake,
 - Identify means to reduce dysfunctions (redundancies, firewalls,...),
 - Assess impacts and consequences after corrections implementation.

Method implementation (how is it settled ?)

Implementation is continuous all along the life cycle and must be fitted to every project phase specific charges. Methods inductive and deductive, of assessment, verification are implemented in an iterative way all along the life cycle. They should be implemented as soon as possible in order to avoid costly redesign when a risk not identified previously is revealed.

Relevance area	Inputs	Outputs
Every area where defect activation consequences can lead to consequences important / serious on availability and even safety related to product.	Financial resources, skill.	<ul style="list-style-type: none"> • Products compliant with specifications within time and budget. • Critical defects of the project, their identification, their consequences, their occurrence

Pros	Cons	Bibliography
<ul style="list-style-type: none"> • High project success rate. • Allows dysfunction risk identification, • Hierarchize efforts to mitigate consequences. 	<ul style="list-style-type: none"> • Depends upon manager experience in concerned area. • Depends on the project innovation degree in terms of functionalities, technology, • May be onerous when applied at wrong level. • Are not a guarantee of exhaustivity. • Quantitative estimates are hardly known and recognized. 	<ul style="list-style-type: none"> • CEI 61025 - 2006 ed.2: Fault Tree Analysis. • CEI 60812 - 1985 : Techniques d'analyse de la fiabilité des systèmes / Procédures d'analyse des modes de défaillance et de leurs effets (AEEL). • RADC TR 85-228, Vol 1 - December 1985, "Impact of Hardware/Software Faults on System Reliability; Study Results". E.C. Soistman / K. B. Ragsdale • Wang, John X. and Marvin L. Roush – 2000: <i>What Every Engineer Should Know About Risk Engineering and Management</i>. London: CRC Press.

Bayesian approach in reliability

Purpose (What for?)

Improve through integration of previous knowledge the estimate of a product reliability characteristic when field data is not sufficient or biased by design, operation or maintenance modifications.
Reduce reliability tests volume.

Description (What is product output and how?)

The so called « frequential » statistical traditional approach deals with estimating the unknown parameters of probability laws to which are submitted some events considered as random (e.g.: number of failures observed on a given number of equipment) from the only empirical data. On the contrary, Bayesian approach relies both on this empirical data as well as an « a priori » knowledge. This « a priori » knowledge depends on cases can be based upon previous data observed in a context different of the present one, or on the proper « a priori » analyst judgement or at least on an expert panel judgement. In this approach, unknown parameters are considered as random variables and previous knowledge is represented by a probability distribution so called « a priori distribution ». Objective data is then aggregated to the « a priori distribution » using a mathematical transform based on Bayes theorem: these results in a new statistical distribution so called « a posteriori distribution ». This latter allows a new estimate of the parameter under concern which reflects both a priori knowledge and objective data. As far as reliability is concerned, the estimate is mostly done upon constant failure rates and probability of good operation of mono-shot mechanisms. Following the example of other application fields, the reliability Bayesian approach is all the more efficient, related to « frequential » approach, since field data is scarce or « polluted » by design or operation modifications of material under concern, provided that the « a priori » model be pertinent. Besides unknown parameters estimate, Bayesian approach in the reliability field is applied to establish « Bayesian test plans » for reliability validation or for monitoring reliability in production phase.

Method Implementation (How is it settled?)

Bayesian approach requires easy analytical processing as far as « a posteriori » probability distribution of parameter to estimate keeps a stable form (i.e. same family as the « a priori » distribution) after integration of observed empirical data. In the reliability field, the two following cases comply with this condition:

- **Case of probability of good functioning of one shot systems: the events scenario is governed by a 2 states Bernoullian scenario « the system runs » and « the system does not run ».** In this case the estimate is done for the probability « p » of good system operation. In order to ensure « p » « a posteriori » distribution stability, it is convenient to adopt as « a priori » distribution a 2 parameters beta type law (first species Eulerian function)
- **Case of a system whose life duration is governed by an exponential law : the « λ » failure rate is then considered as constant and the estimate deals with this parameter.** In order to ensure the « a posteriori » distribution of « λ », it is convenient to adopt as an « a priori » « λ » distribution a two parameters gamma law (second species Eulerian function).

In both cases, good « a priori » distribution parameters is of utmost importance; in fact it will influence the « a posteriori » distribution form, and hence the « a posteriori » estimate of the parameter under study. In order to determine « a priori » distribution parameters, two kinds of approaches can be considered, depending of context:

- Similarity coefficients method: recommended when experimental data upon similar systems or systems operated differently is available at start. It consists in defining and quoting « similarity coefficients » between present system and previous « a priori » reference system. These coefficients must lie upon technical criteria considered as impacting system reliability; they are then given in terms of « a priori » virtual data equivalence which permits to adjust « a priori » distribution parameters of reliability characteristic.
- Expert judgement: experts aware of system characteristics as well as similar systems behaviour are required to provide a professional judgement. Such a judgement is taken into account under oral or written questionnaire form. Collected answers are processed and weighed by the analyst who will provide virtual « a priori » data, as in the similarity coefficients method ».

In any case, the « a priori » law parameters induces centring of the law around a value considered as most probable and dispersion as high as « a priori » data is uncertain. Once melted with a first series of objective data, the analytical processing leads to an « a posteriori » distribution whose dispersion is lower than the initial dispersion when « a priori » values are realistic (in contrary case, it is better not to go through « a priori » data and return to traditional frequential approach). An « a posteriori » estimate of the parameter to be considered can be established, either in a punctual way by adopting for example the distribution mathematic expectation, or by «credibility interval» reflecting the size dispersion of this distribution. When sequentially a new objective data series is available, the process can be redone adopting as a new « a priori » distribution the previous « a posteriori » distribution.

When the used models do not allow to get « a posteriori » distribution stability, the analytical method is not possible any longer and computer computation becomes necessary. This occurs frequently in complex systems whose failures can be both of random nature or wear caused.

In the area of monitoring of equipment under production reliability through sampling, one can find « bayesian » type test plans, applicable to oneshot equipment or constant failure rates equipment. Using these plans, compared to classical test plans permits to reduce necessary test volume, in terms of sample size and/or test duration.

Relevance Area

- Few available data on new equipment.
- Significant objective data volume on similar equipment or having been operated in different conditions.
- Strong expert knowledge on expected operation of new or similar equipment.

Inputs

- . A priori data (experts knowledge, biased data results).
- . Reliability law of equipment under survey.
- . Field experience data on equipment under survey.

Outputs

- . « a posteriori » distribution of reliability characteristic.
- . « a posteriori » estimate of reliability characteristic (punctual and by credibility interval).

Pros

- Possible estimate of reliability characteristics with scarce data.
- Tightening of confidence intervals
- Allows use of a priori knowledge.

Cons

Needs heavy processing when reliability laws do not have linked bayesian laws.
May induce significant estimate bias when a priori judgement is not relevant.

Bibliography

- Projet ISdF n°4/94 « Guide d'application des méthodes bayésiennes aux traitements de retour d'expérience »
- H. Procaccia, L. Piépszownik, et C.A. Clarotti « Fiabilité des équipements et Théorie de la décision statistique fréquentielle et bayésienne » (Eyrolles)

Preliminary risk analysis (P.R.A.)

Purpose (What for?)

Identify and assess / prioritize, from the definition phase, the risk to a system or facility during its life profile and define measures to reduce or eliminate. The causes of the dangers associated with both internal system failures or the installation, the profile of the life environment, the elements constituting the system, the use scenarios and human errors.

Description (What is product output and how?)

The preliminary risk analysis (PRA) is, firstly, to identify potential hazards associated with the system under study. The typical approach is to use the APR lists of risks, based primarily on the experience associated with the system components and their combinations. These lists, require to question the existence of known hazards associated with each element in each phase of the life profile of the system in its environment, opportunities to occur, the foreseeable consequences and known how to control the risks associated. This initial phase may also, in some cases, implement methods like FMEA, HAZOP, fault trees, etc.. which are more typical of detailed risk analysis.

In a second stage, accompanying the advancement of design, the PRA must:

- Establish and describe accident scenarios (those that will require further investigation),
- Evaluate the orders of magnitude of risk,
- Identify measures to control risks and relevance.

At this stage the PRA provides to the project a characterization of tasks to perform dependability and elements to organize.

The PRA then merges in all risk analyzes (systems, sub-systems, processes, etc.), identification, evaluation, comparison with acceptance criteria to the risk management actions while providing a spine and a calendar (to update as and when the project progresses) dependability tasks.

Method Implementation (How is it settled?)

The PRA is an iterative process initiated early in the definition phase in order to guide early design criteria. At this stage, the results are incomplete or inaccurate. It must therefore be updated and refined during the development phase, as process system design progresses and risk reduction.

Achieving the PRA is subject to a work group where each member brings his experience on the identification of potential risks. This work is facilitated by the use of lists of dangerous entities guides and dangerous situations developed for a specific area, as well as functional analysis carried out upstream. It is important in an innovative project for the entity that leads to associate at this stage any information or possible expertise external to the entity.

The conduct of the method is to:

- Use all the knowledge available on the system (functions required environmental profile life composition: materials, energy, structures, etc.),
- Review what might induce undesirable consequence, in the light of existing experience (internal or external to the organization) on each of the components of the system,
- Exclude (in keeping memory) the "unrealistic" risks or unimportant,
- Enrich the analysis for each of the risks identified, to identify what needs to be treated and how to treat,
- Review and update the analysis as and when the progress of the project and system life,
- Establish the hazard record, monitoring and closure actions risk reduction, the basis for audits,...

The table on the following page illustrates a common way of presenting the results of an PRA. It is especially suitable for a technology project designed from scratch. Other presentations may be more suited to a proposed change in an system in operation.

Relevance Area	Inputs	Outputs
Tous domaines d'activité lorsque des risques liés à la sécurité existent. Ex : transports, espace, chimie, nucléaire, énergie, défense, ... L'APR est généralement l'élément de base d'un dossier de sécurité et de son actualisation pendant la vie du système.	- Profil de vie du système - Dossier de définition du système - AMDEC, HAZOP, AAD, AAE, ... - Liste des situations dangereuses - Liste des dangers potentiels - Liste générique de dangers	Rapport d'APR incluant : <ul style="list-style-type: none"> • les tableaux d'analyse, • des conclusions / recommandations, • la cartographie des risques, • le plan de veille, d'audits, de suivi, le registre des dangers.

Pros	Cons	Bibliography
Improved consistency of approach to managing risks of different phases of the system life by posing as broad and comprehensive as possible foundations.	The comprehensive nature of the approach depends very much on the experience of similar events and careful study.	- CEI 60300-3-9 : Management de la sûreté de fonctionnement – Partie 3 – Guide d'application – Section 9 : Analyse de risque de systèmes technologiques. - DEF STAN 00-56 : Safety Management Requirements for Defence Systems. - Mill-STD-882: System Safety Program Requirements. - A.Desroches, D.Baudrin, M.Dadoun Hermes « L'analyse préliminaire des Risques, Principes et pratiques » (Lavoisier, 2010) - A. Villemeur « Sûreté de fonctionnement des systèmes » (Eyrolles). - C. Lievens « Sécurité des systèmes » (Cepadues-Editions) - Y. Mortureux « Analyse préliminaire de risques » (Techniques de l'ingénieur SE 4010 octobre 2002 - IMdR GTR 55 « Les analyses préliminaires de risques appliquées aux transports terrestres guidés » avril 2000

TABLE OF TYPICAL PRA

The results of an PRA generally present in a table with 11 or 12 columns reminiscent of the FME (C) A:

(1) System or function	(2) Phase	(3) Dangerous entities	(4) Events causing a dangerous situation	(5) Dangerous situation	(6) Event causing a potential accident	(7) Potential accident	(8) Effects or consequences	(9) Classification by severity	(10) Preventive measures	(11) Implementation of these measures

The 11 columns of the table can be explained as follows:

1. System or function: identification studied items,
 2. Phase: identification phases or modes of use of system or function for which certain entities may cause danger,
 3. Dangerous entities: identification system entities or function which can be associated an inherent danger,
 4. Events causing a dangerous accident: identification conditions, adverse events, failures or errors that can turn a dangerous entity in dangerous accidents,
 5. Dangerous situation: identification of situations resulting from the interaction of a dangerous entity and the entire system following an event described above,
 6. Event causing a potential accident: identification conditions, adverse events, failures or errors that can turn a dangerous situation in accident,
 7. Potential accident: identification of opportunities for accidents resulting from dangerous situations as a result of an event described above,
 8. Effects or consequences: identification of potential effects or consequences of accidents when they occur, occurrence effective estimation of the probabilities of accidents,
 9. Classification by severity: assessing the severity of the effects or consequences in a classification of "minor", "significant", "critical", "catastrophic" type,
 10. Preventive measures: inventory of proposed measures to eliminate or control the risks identified (potential dangerous situations or accidents),
 11. Implementation of these measures: collection of information on preventive actions (eg: Did these measures have been incorporated in the system, have they been effective?, etc...),
- A 12th column dedicated to the estimation of probability of occurrence of accidents can be added.
 - PRA can be extended to a study of accident scenarios by adding columns of criticality and cost / risk

F.M.E.A.: Failure Modes and Effects Analysis

F.M.E.C.A.: Failure Modes, Effects and Criticality Analysis

Purpose (What for?)

FMECA is a method of analysis, inductive and rigorous, aiming at identifying failures whose consequences may affect system or sub-systems operation. It aims also at organizing them into a hierarchy following their criticality level as to control them.

Description (What does the method produce and how?)

In a first step, listing of system potential weaknesses (in a product under design, a manufacturing process or a production means) by searching for each system component the likely failure modes, the possible causes, the system effects on operation, depending on mission and life cycle phase.

Each failure is then quote in criticality terms regarding the required objective (Reliability, Quality, Availability, Maintainability, Maintenance, Safety...) Two or three criteria are checked: failure mode occurrence (frequency or apparition probability), effect severity, failure detection probability.

Quotation grids are used to perform the assessment, the resulting criticality is often defined as the product of figures given for each criterion. The failure risks are then listed by criticality order, so as to define possible critical points.

Finally, preventive and/or corrective maintenance actions have to be found to reduce criticality in case of critical or unacceptable failures. The actions can be held all over the life cycle.

Method Implementation (How is it settled?)

FMECA is a simple and thorough methodology of failure risk analysis.

A preliminary system functional analysis is required, which permits to describe the system mission, the nominal operation modes the various service functions to be ensured and ultimately the technical functions.

Generally, FMECA is performed by a working group. Attendants are chosen given their system knowledge or on analogous systems. A manager attendance is essential. The group relies upon available information at study time: drawings, documents, breakdown history on equivalent systems...

After analysis has been performed, the manager shall establish a synthesis of results under list form of failures, or symptoms. In particular, an action plan is decided providing nominative responsible and deadline commitments.

Once actions settled, updates of analysis shall be emitted after validation of results.

Relevance Area

- FMECA is widely spread in every activity area... (hardware systems in mechanics, hydraulics, electrical, electronics...),
- In case of software, an equivalent analysis is performed, so called Software Effect Error Analysis (S.E.E.A).

Inputs

- New system design file,
- Existing system breakdown history,
- Functional and structural system description (output of Functional Analysis),
- Knowledge of system environment and use conditions,
- P.H.A., HAZOP...

Outputs

- Identification of potential dysfunctions and their criticality,
- Preventive action plan or corrective improvement action plan...

Pros

- FMECA is simple and easily accessible,
- It is a powerful tool with broad application field. It can be settled during design as well as during operation,
- As an inductive method, it offers a systematic analysis and hence the best guarantee of sufficiency,
- At last, the analysis table ensures a good traceability of ideas and a help for decision of actions to be undertaken...

Cons

- A bit heavy in volume and time consumption,
- Difficult to take into account combinatory or dynamic phenomena, multiple breakdowns, in such a case, other methods are recommended (fault tree...),
- "Common failure modes" not taken into account,
- Better adapted to mechanical and analogical systems than digital,
- At present time, no database available for organ failure modes, causes, effects, aso...

Bibliography

- MIL STD-1629-A: "Procedures for performing a Failure Modes and Effects Analysis", notice 1, 1983.
- CEI-60.812: "Techniques d'analyse de la fiabilité des systèmes. Procédures d'Analyse des Modes de Défaillance et de leurs Effets (A.M.D.E.)".
- EN NF X 60.510: "Techniques d'analyse de la fiabilité des systèmes. Procédure d'analyse des modes de défaillance et de leurs effets (A.M.D.E.)", 1986.
- CETIM, "Guide de l'AMDEC machine", 1994.
- ISdF, Condensé pédagogique n°4, "AMDEC".

State Graph

Objective (What for?)

Assess the main characteristics of Reliability and Availability of a repairable system.

Description (What does the method produce and how?)

System possible states (nominal state, degraded operation state, full breakdown state...) are modeled using circles linked between each other by arrows showing the possible transitions between those states. These transitions are conditioned by either failure processes or repair of failed entities whose intensity is shown (failure rate or repair rate). Mathematically, the state graph gives place to a system of differential equations, so-called Markovian when failure and repair rates are constant. Solving this differential system allows to compute the various probabilities associated to the identified states and hence the system dependability main characteristics.

Method Management (How is it settled?)

The analysis of dependability characteristics using state graph is performed through 4 main steps:

- Collection and hierarchization of all possible functional states (nominal, degraded, breakdown). When two possible states are studied (operation and breakdown) the maximum number of states for each element is 2,
- Collection and identification of all possible transitions between the identified system states. The transitions are governed by failure processes or reset in operation after repair of failed items,
- Drawing of a state graph including circles and arrows between circles, whose purpose is to scheme all the states identified in step 2 and their associate links,
- Settlement and solution of the linear differential equations system linked to the state graph. Solving leads to obtain either instantaneous availability (time function) or asymptotic availability (in steady state) or the main system dependability characteristics such as M.T.T.F., M.T.B.F., M.T.T.R., mean system breakdown frequency, etc.

Relevance Area

-Cost/ availability trade-off of architecture of constant failure and repair rate repairable systems whose states are not affected by external events occurrence at preset instants.

Inputs

-System states,
-Transition rates,
-Dependability objectives.

Outputs

-Availability (instantaneous and/or asymptotic),
-Dependability Characteristics: M.T.T.F., M.T.B.F., M.T.T.R., breakdown frequency...

Pros

- Interest of graphical display,
- Possible analysis of dependant elements systems (For example: passive redundancy),
- Take into account non-exponential laws for repair durations (fictitious states method).

Cons

- Limited to wear less devices,
- Unable to take into account deterministic events with externally fixed date,
- Exponential growth of number of graph states with number of system elements,
- Dedicated computer use is necessary when number of states becomes significant.

Bibliography

- Pagès & M. Gondran, "Fiabilité des systèmes", Eyrolles.
- A. Villemeur, "Sûreté de fonctionnement des systèmes", Eyrolles.
- AFNOR X 60.503, "Introduction à la disponibilité".
- **NF EN 61165**: "Application des techniques de Markov".

FAULT TREE, EVENT TREE, CAUSE TREE

DO NOT BE CONFUSED!

One may think that these three different methods are either similar or relevant of a same approach, but they are in fact quite different. Fault Tree and Event Tree Analyses are **provisional analysis approaches** whereas Cause Tree is an **a posteriori description** of an accident.

Fault Tree is built from consequences towards causes, i.e. the whole of failure combinations and possibly circumstances, which may cause the studied feared event.

On the opposite, Event Tree is built from cause - the event - towards possible consequences, taking into account all possible alternatives able to modify these consequences.

Cause Tree starts from the actual accident; it describes the cause sequences (failures, circumstances, actions, abnormal behaviors...) which combined to create this accident. This method is particularly used in analysis of accidents at work.

Confusion between words issued from historical gaps edited in reference publications has generated misunderstandings on these words. It is of main concern not to be confused on the three methods whose approaches are different; **they are not variants of a same approach!**

No matter for you to use different names when you are aware of the confusion risk between the approaches. Please, read carefully the sheets about each method and identify clearly the approach of your concern!

Fault Tree Analysis (F.T.A.)

Objective (What for?)

Fault Tree method allows a « deductive » analysis of technical or operational causes, which may provoke situations not compliant with a required objective, concerning safety (feared situation) or availability (undesirable event).
The method is so called deductive for it allows identification of situation causes.

Description (What does the method produce and how?)

This logical method is Boolean type:

- a. "This situation could occur **when** the operation is performed and when the default happens due to an accident",
- b. "This event could occur **when** checking is not performed in due time **or when** system failure is not repaired quickly enough ".

Such a deductive analysis is of « top-down » kind, i.e. from feared event starting, originating causes are searched step by step, from general event to elementary events. The events are consequences of product internal or external events, among which product defects.

Method Management (How is it settled?)

This method can be settled after the following main steps:

- Define the undesirable situation under study,
- Define combinations leading to that situation,
- Build the tree using logical operators (gates « AND », « OR »...),
- Search minimal cut sets (shortest way to the undesirable event).

Relevance Area	Inputs	Outputs
- The method is well adapted to combination of events. - However, it is tricky when events are sequential.	- Product undesirable events list. Such a list can be established either as soon as design upstream phase, or result of manufacturer or customer field experience or free thinking of working group. Law aspects are often to be considered as far as system situation or unbearable user risks are concerned (safety study case).	Document includes: <ul style="list-style-type: none"> • Fault trees related to feared events under study... • Minimal cut sets analysis.

Pros	Cons	Bibliography
- Method allows knowing how many events are required to lead to feared event (minimal cut sets).	- Result quality reminds mainly on experience and imagination of the person in charge of the analysis, - A computer program is necessary when event combination number is over some tens to compute probability of occurrence of undesirable event and minimal cut sets.	- DEF STAN 00-56: "Safety Management Requirements for Defense Systems". - CEI 1025: "Analyse par arbre de pannes". - RAC: "Application Guide". - Ian S. Sutton: "Process Reliability and Risk Management", Van Nostrand Reinhold, 1992.

Event Tree Analysis (E.T.A.)

Objective (What for?)

Identify and assess possible consequences of an initial event after circumstances or dysfunctions with which it is combined.

Description (What does the method produce and how?)

Based upon binary logic (the event happens or not, the component or system fails or not), such a method allows to determine possible consequences of an initiating events by searching possible paths leading to it. The paths are associated with an occurrence probability allowing consequences probability calculation.

Scenario or system (i.e. safety system) includes several elements combining in order to prevent severe consequences. Starting from the event under study two branches are considered depending upon first element acts or not; in each branch, an alternative is considered depending upon second element acts or not and so on until final consequence. Each alternative branch can be affected with a success probability so that on the end each found branch probability could be computed.

Method Management (How is it settled?)

1. Identify initiating event: it can be system, component failure or external event. Event happening frequently is then defined (which may result of a Fault Tree or other Event Tree Analysis),
2. Identify prevention mechanisms: automatic safety systems, operators alarms, operator actions, safety fences... their efficiency is assessed through a success/failure rate,
3. Tree building, from left side (initiating event), to right side (consequences) while sequencing prevention mechanisms represented by branches: upper branch for success and lower branch for failure,
4. Assess each branch probability (through help of a fault tree event for failure as an example),
5. Assess each consequence probability combining branches probabilities,
6. Rank consequences following probabilities.

Relevance Area

- Provide mean severity to an event difficult to avoid (Attack, breakdown...),
- Compare efficiencies of various measures (of prevention or protection) dedicated to initial event impact reduction,
- Modeling tool useful for study and assessment of accident risks as well as sequencing successive aggravations, a list of consequences for system, staff, neighbors and environment can be provided,

Inputs

- System and environment elements impacting the path of event under study effects,
- As far as a quantitative approach are concerned, probabilities of events and conditions affecting paths of feared event.

Outputs

List of possible consequences of the event, probabilities of each, list consequences for each of these combinations of elements that can cause it, then identify opportunities to prevent these consequences.

Pros

- Natural approach easy to appropriate. Some important advices easy to assimilate. A well trained (1 or 2 days) manager is advised; nevertheless, this method does not require long or hard to acquire competences. Conclusions quality depends on quality and comprehensiveness of list of elements taken into account,
- Ciphering relies upon availability and precision of elementary alternative events,
- Allows assessing factor influence by variation of happening probability,
- Allows following an accidental scenario progress and assessing avoiding methods influence on consequence frequency,
- Linked to fault trees, allows to know the minimal number of events leading to each given consequence (minimal cut sets).

Cons

- Aggravation factors can be confused with failures,
- Aggravation factor assessment strongly relies upon analyst ability,
- Method requires a computer program, as soon as fault tree includes more than some tens of events, to compute event probability and list minimum cut sets.

Bibliography

- CEI 62502 : "Techniques d'analyse de la SdF, analyse par arbre d'évènement".
- Techniques de l'ingénieur, Sécurité et gestion des risques, SE 4,050, "Arbres de cause, arbres de défaillance et arbres d'évènement", 2004.
- Railtrack, Yellow Book 3, "Engineering Safety Management".

Cause Tree

Objective (What for?)

Gather in a synthetic and logical display all factors contributing to a proved incident

Description (What does the method produce and how?)

Starting from the actual incident, events or conditions whose compilation provoked incident are linked together. The breakdown is then redone for each event until integration of all elementary events and conditions recognized as incident contributors.

Method Management (How is it settled?)

First, freely gather all elements: facts, circumstances, steps of the scenario.
 Second, classify them as « normal », « abnormal », « internal » or « external ». Depending on the reference adopted, classification criteria can be more or less numerous.
 Third, logical or chronological links are established (C is the consequence of A+B...).
 Fourth, associate events with symbols corresponding to their classification (circles, squares, a.s.o.), logical links with lines.
 The result is a tree diagram form where the event under study is the unique final point whereas facts or contributing circumstances are deployed upstream at a position representing their role in the scenario.

Relevance Area

- Incidents a posteriori analysis,
- The more available the information about incident is, the more relevant the Cause Tree is. The method leads to ask adequate questions to deepen the enquiry,
- Focus on single cause or culprit should be avoided and more discrete elements or secondary lessons are to be searched in a profitable way.

Inputs

- Knowledge of incident and actual system operation.

Outputs

- Open explanation of incident linking all contributing events and not limited to the identification of a single « cause » or minimal cutset of « causes ».

Pros

- Promote teamwork while performing the synthesis of various standpoints,
- Well spread method,
- The management has to be strict and mastered so as the result should not be reduced to a cheap heartening conclusion.

Cons

- Takes into account temporal logical sequences, but fails to show continuous data such as duration.

Bibliography

INRS Publications:
 - ED 833, « Face aux accidents: analyser, agir », 1999,
 - ND 1736, « Quelques facteurs de réussite ou d'échec de l'introduction dans l'entreprise de la méthode des arbres des causes ». Etude comparative dans deux établissements d'un groupe industriel.

Maintenance and Maintainability Tree

Objective (What for?)

Maintenance Tree or Maintainability Tree provides users a way to define, optimize or update their production tools maintenance policy. It also provides means of adaptation of the whole of durable goods constituting the technical heritage of the company, regarding their qualitative and quantitative evolution.

Description (What does the method produce and how?)

Each component of durable goods will be assigned an operational maintainability level weighed by an heterogeneity factor whose data is determined as follows:

1. By the technical quality manuals of each sustainable goods' type,
2. By a dispersion coefficient of each type issued from company durable goods' inventory.

Method Management (How is it settled?)

1. Dispose of a system and a doctrine of configuration management as well as a breakdown of types which are concerned,
2. Dispose of an inventory and follow up of hard and soft investments management system of the company,
3. Define non-maintainability criteria of sustainable goods depending on available logistic and maintenance means,
4. Establish production tools maintainability mapping,
5. Define configurations, suitable for internal and external, preventive and corrective operations.

Relevance area

- Processing of maintenance policy choice criteria,
- Depending on activity area:
 - Company Internal Maintenance Service,
 - Sub-contractors for multi-brand maintenance Services.
- The method can be applied to every company technical holdings, producing goods or services (key account or little companies),
- The method is particularly suitable for developing countries or companies with obsolescence problems.

Inputs

- Inventory of identified Hardware and Software,
- Nomenclature and price of items (compounds and components),
- Breakdown of inventory items,
- Maintainability thresholds and adequate maintainability level for internal maintenance.

Outputs

- Evolution of maintainability mapping applied to company technical holdings,
- Spares and maintenance policy decision criteria,
- Decision helps statistical processing.

Pros

- Allows mastering a dynamical maintenance policy capable of item mission profile evolution. For Commercial Off The Shelf (COTS) users, allows progressive know how transfer for maintenance and spare parts policy (namely obsolescence problems),
- Allows to justify technically and economically a possible decision of subcontracting maintenance.

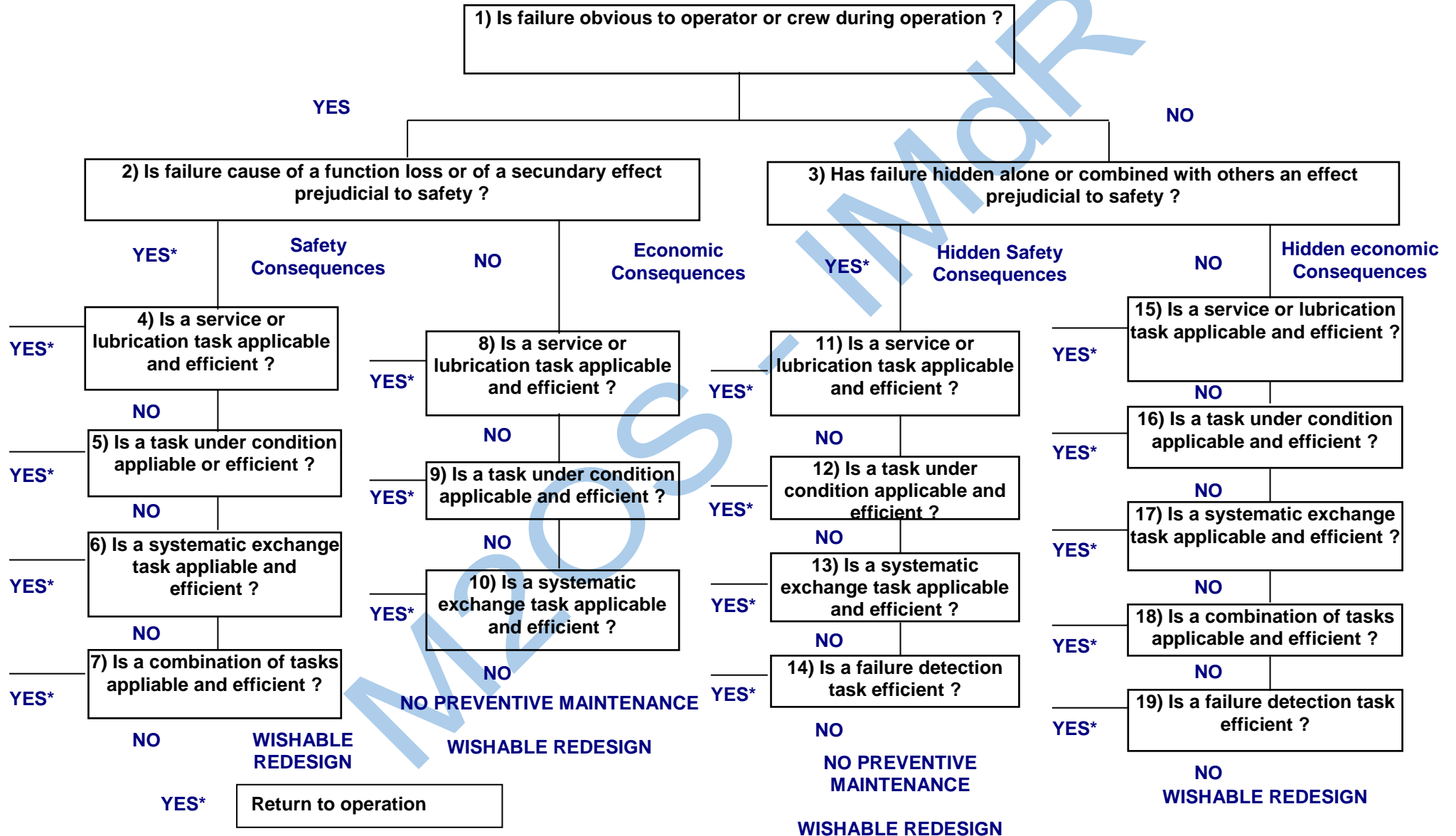
Cons

- Obligation of software follows up regarding database and maintenance feedback experience,
- Obligation of settling a breakdown with unique item designation, avoiding doubles due to different supplier references,
- Need to resort to « Maintainology » (study of logistic support, sustainable maintainability, consistency of maintenance operations and typology of probable failures).

Bibliography

- ISO 9.004 – 2: "Recommandations pour les services".
- NF X 60.000: "Fonction maintenance".
- ISdF 5/98: "Eléments d'aide à la décision de renouvellement d'un matériel".
- ISdF 3/97: "Plan d'amélioration de la maintenabilité des équipements".
- ISdF 6/95: "Optimisation économique de la maintenabilité".
- ISdF 6/92: "Rapport d'études sur les critères de maintenabilité d'un bien".
- ISdF 7/92: "Recueil des méthodes et des moyens de maintenabilité".
- ISdF-GTR 45: "Maintenance et soutien logistique: Aspect Managérial".

Method Illustration : Maintenance Alternatives



HAZard and OPERational Study (HAZOP)

Objective (What for?)

Detailed examination of system components in order to determine what could happen when one component should operate out of its normal use range.

Description (What does the method produce and how?)

Each component is attributed one or several parameters (pressure, flow, electric power...). With HAZOP, each parameter is considered and guide-words are used to characterize the possible abnormal behavior, such as "more", "less", "upper", "lower", "none"... The effects of such a behavior are then assessed.

Method Management (How is it settled?)

HAZOP goes through the following steps:

1. Definition of study field and objectives,
2. Settlement of a working group,
3. Search of design information, presentation of system under study by designer,
4. Elements identification and characteristics, performances...
5. Choice of guide-words and deviation attribution (in case of a doubt, do not discard any risk),
6. Exploration of the possible occurrence ways, search of causes and consequences,
7. Proposal of recommendations, search of protection or alarm mechanisms existing or under project, study of their efficiency (decreasing of risk probability or consequence),
8. Impact over design.

Guide-words:

- NO: No display of any data element or signal,
- MORE: Quantitative increase,
- LESS: Quantitative decrease,
- AS WELL AS: Action correctly performed, but with extra results,
- PART OF: Only a function part is performed,
- REVERSE: Function reversion,
- OTHER THAN: The obtained result is different of the expected one,
- EARLY/ BEFORE: Something happens earlier than expected,
- LATE / THEN: Something happens later than expected.

Relevance area	Inputs	Outputs
- The aim is to identify risk causes and find remedies. - HAZOP should not be used as a design study. When design is incorrect or not comprehensive, the study relevance should be jeopardized.	- Design file, - Functional analysis, - Environment description, - PHA, FMECA, fault trees.	- Risk identification, - Risk reduction action, - Hazard Log,

Pros	Cons	Bibliography
- Multidisciplinary teamwork, - Systematic and detailed analysis, - Takes into account several standpoints (designer, user, maintainer, supplier...), - Possibility of "black boxes » study, - Possibility of work over components interaction when failure modes are unknown or complex, - Design audit.	- When study perimeter is too big, risk of non-comprehensiveness, - Approach sometimes heavy to settle, - Take care of the guidewords choice. When the list is reduced or limited, the analysis relevance is reduced... - Adapt the guidewords to the field under analysis.	- DEF STAN 00-56: "Safety Management Requirements for Defense Systems". - DEF STAN 00-58: "HAZOPS Studies on Systems Containing Programmable Electronics".

Hazard Analysis Critical Control Point (H.A.C.C.P.)

Objective (What for?)

HACCP method is a mean to guarantee food healthiness. It relies upon forecast and prevention of biological, chemical and physical hazards.
 The aim is to provide a systematic approach to identify, locate, assess and master the potential risks of goods healthiness degradation within the food chain.
 European Directive 93/43 about foodstuffs health has established HACCP application to the whole of agribusiness channels.

Description (What does the method produce and how?)

HACCP method settlement includes successive steps grouped in the following 6 families:

- Definition of product and fabrication process,
- Identification of hazards for any fabrication step,
- Establishment of Control Critical Points (C.C.P.),
- Establish critical points survey system,
- Record and keep records,
- Verification of system efficiency.

Method Management (How is it settled?)

HACCP settlement requires a working group constitution.
 A decision tree is elaborated to qualify a fabrication step.
 This tree analysis leads to critical points identification.
 The critical points management ensures their mastering.
 This method can be integrated in agribusiness companies' quality management systems.

Relevance area

- HACCP system is a food safety management tool,
 - Method can be applied to every sector of food or beverage processing, distribution, sale, catering.

Inputs

- Product related data,
 - Fabrication operations synopsis.

Outputs

- Process survey system,
 - Corrective actions plan,
 - Records.

Pros

- HACCP method provides a clear methodology to develop a Quality Assurance Plan:

- Principles internationally recognized,
- Hazard analysis comprehensiveness.

-

Cons

- Difficulty to identify Risks and Critical Points (RPC),
 - Difficulty to assess hazard gravity and occurrence.

Bibliography

- La sécurité alimentaire par le HACCP – DGAL (Direction Générale de l'Alimentation) – Publication du Ministère de l'Agriculture, de la Pêche et de l'Alimentation.
 - HACCP: Guide pratique – Polytechnica

Zone Analysis

Objective (What for?)

Show evidence of problems resulting from physical interaction between neighbor elements or disturbing flows generated by external sources.

Description (What does the method produce and how?)

Zone analysis results in identifying and analyzing, through systematic investigation performed on mock-up, problems resulting from physical interaction (thermal emission, acoustic noise, vibration nodes, EMC, a.s.o.) between various product "zones" or between some "zones" and external ambient. The problems cannot be identified through technical manuals and hence require a specific enquiry on models which are themselves parted into "zones".

Method Management (How is it settled?)

The approach results in successively identifying the following, through available mock-ups examination:

- Geographical zones to which belong the various material elements,
- The flows of any kind possibly emitted by each material element of a same zone, being normally operating or not (i.e. thermal emission, degassing, electrolyte expenditure...),
- External sources emitted flows into each zone (i.e. EMC, vibrations, human errors),
- Effect of these various flows (internal and external) on each zonal element, and then on product main functions and/or technical functions of the product.

Interactions effects consequences are then classified into 2 categories:

- Minor consequences, without any further analysis,
- Significant consequences giving place to modifications proposals or recommendations, for example such as:
 - Isolation device addition,
 - Man machine interface improvement,
 - Evacuation device improvement (i.e.: thermal); recommendations about maintenance procedures,
 - Recommendations about operation procedures, a.s.o.

Zone analysis, successively applied on mock-ups more and more representative of final product, can in fine lead to definition of tests to be undertaken (i.e. compatibility tests) and dedicated studies preparation (i.e. specific risk analysis: fire, explosions, contamination...).

Relevance area	Inputs	Outputs
- Each system in which physical interactions between « zones » may harm correct operation (such interactions cannot be studied in classical analysis such as FMECA, FTA...), - Each system where common cause failures should be expected, - Man/machine Interfaces.	- Mock-up compounds, - Technical files.	- Effects of disturbing flows on various product zones or ambient... - Common cause failures, - Corrective actions or tests to be undertaken.

Pros	Cons	Bibliography
- Show evidence of problems undetectable through paper analysis.	- Need to use mock-ups more and more representative of final product.	- C. Lievens: "Sécurité des systèmes", Cepadues-Edition. - A. Villemeur: "Sûreté de fonctionnement des systèmes industriels", Eyrolles, 1988.

Reliability Centered Maintenance (R.C.M.)

Objective (What for?)

Methodology aiming at optimizing maintenance while controlling equipment safety, availability and life duration.

Description (What does the method produce and how?)

The method defines optimum preventive maintenance program related to stakes linked to systems and equipment failure consequences. Maintenance tailoring should be performed depending on function failure consequence (system approach) rather than component (object approach). This method can influence equipment design.

Method Management (How is it settled?)

RCM method is performed through the following steps:

1. Elaboration of a RCM plan (objectives, methods, scheduling and organization),
2. Determination of initial data elements (RCM candidates selection criteria, design characteristics, functional definitions, dependability, cost and environment data elements),
3. RCM Analysis itself:
 - Failure Consequences Analysis (safety, economic consequences...),
 - Structural, Analysis,
 - Definition of maintenance tasks to improve candidate reliability or safety,
 - Identification of maintenance alternatives,
 - Analysis and hierarchization of maintenance tasks following parameters trade-off (availability, reliability, safety, maintenance cost ...),
 - System Analysis under logical tree form,
 - Determination of thresholds and maintenance intervals consistent with analysis parameters,
 - Internal and external field experience exploitation after Production and Operation phase of comparable systems.

Relevance area

-RCM method joined with dependability and logistic support analysis studies allows defining maintenance organization towards optimum safety and availability at minimum cost,
-This method is applied to complex, expensive and of long life duration systems.

Inputs

- System similar maintenance plan,
-RAMS studies, FMECA
-System logistic breakdown and associate maintenance concept.

Outputs

- Optimized Maintenance Plan,
-Periodicity of homogenized tasks.

Pros

-Justification organized and structured of tasks types to be undertaken and periodicity,
-Takes into account function impact on safety, availability and life duration,
-Visualization of mission performed by system,
-Optimization depending on:

- Product, subsystem, function exploitation,
- Function criticality in terms of:
 - Safety,
 - Availability,
 - Cost.

Cons

-Approach sometimes heavy to settle,
-The method relies upon FMECA.

Bibliography

- **CEI 60300-3-11, Ed.2.0** : "Gestion de la sûreté de fonctionnement - Partie 3-11: Guide d'application - Maintenance basée sur la fiabilité".
- **MIL STD-2173**: RCM Requirements for naval aircraft, weapon systems and support equipment.
- Méthode OMF élaborée par EDF.
- **Projet ISdF 6/99**: "Guide de l'Ingénierie de Maintenance".
- **DEF STAN 02-045**: Requirements for the Application of Reliability-Centred Maintenance.
- Techniques to HM Ships, Submarines, Royal Fleet Auxiliaries and other Naval Auxiliary Vessels.
- Gilles Zwingelstein, "La maintenance basée sur la fiabilité: Guide pratique d'application de la RCM", Editions HERMES, 1996.
- Daniel Richet, Marc Gabriel, Denis Malon, Gaëtan Blaison, "Maintenance basée sur la fiabilité: un outil pour la certification", Editions Masson, 1996.

Integration Design and Support (I.D.S.)

Objective (What for?)

Decision supports to select a preferred solution for designing durable and maintainable equipment, taking into account criteria of COST, AVAILABILITY and EFFICIENCY.

Description (What does the method produce and how?)

- « IDS » process provides ranking of designs to be considered following:
- Various parameters included in the basic factors « LCC », « AVAILABILITY » and « EFFICIENCY » definition as well as associate computation methods (these parameters are to be keyed in an appropriate database),
 - Performance of simulations to find optimum trade off and selection criteria of preferred solution a priori accepted for equipment design.

Method Management (How is it settled?)

Initiate « IDS » process, including:

- « IDS » presentation to Customer,
- Consideration of schedule of conditions,
- « IDS » introduction at possible subcontractors.

Define possible design solutions, including:

- Technical and technological tasks attributed to research department,
- Dependability consideration ("RAMS" headings),
- LSA (Logistic Support Analysis) consideration, taking into account « USER » logistics,
- Cost and associate logistic data collection.

Compute « IDS » basic factors: « LCC », « AVAILABILITY », and « EFFICIENCY » (the latest linked to ESSENTIALITY notion).

Select preferred solution, including:

- Basic indicator computation (MERIT FACTOR),
- Decision support indicators computation,
- Feedback on design,
- Final decision (validation).

Relevance Area	Inputs	Outputs
<p>- « IDS » process, based on trade off « COST - AVAILABILITY - EFFICIENCY » is simple and operational for persons in charge of system or equipment design,</p> <p>- « IDS » being systemic and multidisciplinary is dedicated as well as customer bodies and major industrial groups as small companies, sub-contractors, consultants and teachers specialized in logistic engineering,</p> <p>- « IDS » is a tool allowing to enhance products competitively and to reinforce supplier's image.</p>	<p>- Schedule of conditions + COST and LOGISTIC data.</p>	<p>- Value of basic factors and indicators,</p> <p>- Ranking of solutions to be considered,</p> <p>- Selection of preferred solution.</p>

Pros	Cons	Bibliography
<p>Settling of a pragmatic ILS approach including:</p> <ul style="list-style-type: none"> - Speed of task performance, - Easy use with simple means, - Consideration of couple « COST/PERFORMANCES », - Introduction of merit factor and other indicators for decision help, - Process adaptation to company specific rules, without extra costs other than limited training costs. 	<ul style="list-style-type: none"> - Need to perform advanced FMECA... - Possible difficulties to assess «ESSENTIALITY» factors. 	<p>GTR – ICS / IMdR, « ICS » handbook, version n°3, 01/01/2006.</p>

Design of Experiments

Objective (What for?)

To allow designers to control the design parameters, using a minimum number of tests. Adjusting these parameters allows to optimize product or process performance and/or to reduce their sensitivity to different causes of variability.

Description (What does the method produce and how?)

Design of Experiments (DoE) is a testing method based on a structured test protocol. The values (or levels) of several input factors are varied simultaneously from a test to another. The impact of these variations on one or more performance (output variable) of a product or process is then observed. Thus, it is in opposition to the "classical" experimental design, in which the research of the effect on performance of the controlled input factors is obtained by varying one factor at a time from a test to another. The structuring of this experiment and the treatment of the results are based on the application of statistical tests using analysis of variance (ANOVA).

Method Management (How is it settled?)

A number of conditions defines the feasibility of the Design of Experiments:

- The number of units of the tested entity (product or process) is compatible with the required experiment scheme,
- The planning is sufficient for a complete testing,
- The budget is consistent with the experimental protocol,
- A multidisciplinary team is available to complete the implementation of the experiment, and includes as a minimum:
 - A Design of Experiments expert (e.g. statistician, expert in reliability...) whose main role is to develop the experimental protocol, to validate and exploit the results,
 - Engineers and/or technicians with extensive knowledge of the product (or process) and its use profile,
 - Technology experts in areas related to the rationale for the design of experiments (e.g., electrical technologies, mechanical technologies, expertise on the environment...),
 - Experimenters in charge of conducting the tests in accordance with the chosen protocol, and perform the necessary measurements with the required accuracy.

When these conditions are fulfilled, the Design of Experiments can be implemented and involves the following steps:

- The choice of a method of experimentation: selected factors, nature of these factors, choice of the modes or levels of these factors and interactions taken into account (order 2 or more), nature of the Design of Experiments (full, fractional, simple or crossed, definition the test matrix for the selected plan, order of the tests).
- The performance of the experiment itself: it consists in implementing the test sequence according to the protocol adopted in the previous step. The value of the results is strongly depending on the care to the quality of the experiments and of the precision of measurements.
- The analysis of the results is complemented by a series of checks by the "pilot" of the experiment:
 - Checking the consistency of the results and examination of suspect values,
 - Looking for significant effects (ANOVA) and response modeling using the linear model (recommended use of specific Software),
 - Looking for ambiguities at the "effects" level (e.g. possible mixture of "contrasts" and effects in the use of fractional plans),
 - Subsequent check of the results area of interest (i.e. consider the interest of any further experimentation in a new area),
 - Analysis of "Alias" between main effects and interaction effects (possible interest of an additional plan),

Examining the validity of the 1st degree model (possible interest of additional plans, for example, to consider a quadratic model).

A replay of the experiment must be considered if necessary. Depending on cases, this replay may lead to:

- Resolve ambiguities (alias, uncertain measurements, bias...),
- Add in the model new input factors not taken into account in the original plan,
- Using a non-linear (e.g. quadratic) model,
- Highlight the searched optimum,
- Search a "robust" solution (i.e., insensitive to fluctuations of uncontrolled factors),
- Etc

Relevance Area

- Search for optimizing the performance of a new product, by highlighting the values or modes of the design parameters of the product design,
- Construction of the robustness of a new product by setting design parameters to reduce the sensitivity of its performance to different sources of variability.

Inputs

- Identification of product performance.
- Identification of design parameters (quantitative or qualitative) that may have a significant effect on product performance.

Outputs

- Identification of design parameters having a significant effect on product performance.
- Values or modes of design parameters allowing to optimize the performance and/or to reduce their sensitivity to the sources of variability.

Pros

- Reduction of the number of tests to be performed,
- Identification of the single effects and of the interaction effects of design parameters on product performance,
- Optimization of product performance,
- Assist to design of the robustness of a new product.

Cons

- May require an experimental protocol difficult to implement,
- Often requires the use of specific software to determine the experimental protocol to process the results (ANOVA).

Bibliography

- NF X 06.080 « Plan d'expériences (vocabulaire et indications générales) ».
- M. Vigier « Pratique des plans d'expériences - Méthodologie Taguchi » (Les Editions d'organisation).
- J. Goupy « La méthode des plans d'expériences » (Dunod).
- J. Demonsant « Comprendre et mener des plans d'expériences » (AFNOR).
- .WG Cochran & G. Cox « Experimental Design » (John Wiley & Sons)
- .ASTE « Le rôle des essais dans la maîtrise de la fiabilité ».
- .RAC Blueprints for Product Reliability.

Accelerated Life Tests

Objective (What for?)

To predict, economically and on a short period of time, the evolution in time of one (or more) functional performance(s) and the lifetime of a material entity in its normal conditions of use, from tests performed under stress values above the levels specified in normal use.

Description (What does the method produce and how?)

Accelerated Life Tests involve submitting one or more material entities (component, board, sub assembly, full assembly) to one or several simultaneous constraints, in levels above the levels specified in normal use, until the end of their life. The results are then extrapolated to the normal conditions of use of the product, using analytical models validated by experience. In general, the considered entity is a component, an assembly of materials, or simple structures.

Method Management (How is it settled?)

Performing an accelerated test involves the following steps:

- **Test planning:** It is the fundamental step to obtain the desired results. This is primarily to identify the performance and/or characteristics of the entity to be measured, to evaluate mechanisms failure rate and to identify the nature of the stress (or stresses) which will accelerate predominantly these mechanisms. The (amplified) level of each applied stress during the test is then specified. To facilitate the planning of tests, the following recommendations should be taken into account:
 - The tested units of the entity have to be representative of the final product,
 - Only the stresses with a predominant action on the failure mechanisms have to be amplified; the other stresses has to be maintained "normal" or "non-existent" level (e.g. absence of vibrations),
 - The levels of amplified stresses must not exceed the limits specified by the entity's technologies. Moreover, the selected levels has to be such that the failure modes they generate are representative of the failure modes can be observed in the normal use of the entity.
- **Conducting the test:** the accelerated lifetime test is performed on all units identified in the planning stage, using test utilities generating the specified environment. To extrapolate the lifetime of the entity under normal conditions of use, it is essential to continue the test until the failure of each unit tested. When the analytical model chosen to give the acceleration of the probability of failure at the applied stress level appears as insufficiently validated by experience, it is recommended to supplement the basic test by further tests on other units, applying stresses of same nature but at different levels. The lifetimes observed at these different levels can then ensure that the analytical model originally chosen for the extrapolation of results in normal conditions is valid and, if necessary, to use another model.
- **Analysis and prediction:** the analysis performed from the lifetimes observed after the accelerated test in order to predict the lifetime under normal conditions of use are based on the chosen analytical model. Additionally, smoothing techniques on appropriate functional scales may be necessary to validate this model. Among the models most frequently used, the following ones may be applied:
 - The Arrhenius model: mainly applicable to electronic components,
 - The Eyring model: a generalization of Arrhenius model, it uses an exponential law to modeling the evolution of failure rate vs. both temperature and humidity changes,
 - The inverse power law of the type $N = K \times S^b$, where S corresponds to a given stress level and N to the number of stress cycles until to failure of the entity. This law may be applied specifically to the case of mechanical structures subject to repetitive stresses (Basquin law).

Relevance Area

- In principle, on some a priori critical sets of prototypes available in the **Feasibility phase**, in order to consider the necessary corrective actions to be performed before the design is frozen. When they are realized in the **Design phase**, accelerated lifetime tests are rather used to help solve some technological problems already identified.

Inputs

- Life profile of the product,
 - Normal levels of stress,
 - A priori critical elements,
 - Most critical stresses,
 - Acceleration models.

Outputs

- Lifetime in test conditions,
 - Extrapolated lifetimes under normal conditions of use,
 - Potential weaknesses of the product.

Pros

- Reduces significantly the time required by the implementation of tests under "normal" stresses, to predict the lifetime and the evolution of characteristics in time, for a material entity under its specified conditions of use,
 - Identifies weaknesses in design (product and process) under some stresses.

Cons

- Difficulty to apply simultaneously during the test all the stresses existing in the profile of use,
 - Uncertainties about the nature of mathematical acceleration models or about the value of their parameters (e.g. energy activation in the Arrhenius model).

Bibliography

- ASTE « Le rôle des essais dans la maîtrise de la fiabilité ».
 - RAC Reliability Toolkit (Commercial practices edition).
 - Wayne Nelson « Accelerated Testing » (Éd. John Wiley).
 - Revue Phoebus n°13 « Les essais accélérés » (Éd. Préventique).
 - Annales journées SIA de mai 2000 « Les essais accélérés ».
 - IEEE Transaction of Reliability.

Accelerated Degradation Tests Highly Accelerated Life Tests (H.A.L.T.)

Objective (*What for?*)

To explore the operating margins of a product under development and to identify the defects inherent in the design (product and processes) that reduce these margins to values considered insufficient, at the earliest, in order to correct them.

Description (*What does the method produce and how?*)

Highly Accelerated Life Tests involve submitting a material entity of a new design (part, component, assembly...) to environmental and / or operating stresses, under increasing levels, in order to meet the ultimate limits of the used technologies. By principle, these stresses are increased to levels higher than specified values. Once the resistance limits are met, the tests are interrupted before deciding what action to take: margins considered sufficient, redesigns, specific corrections...

Method Management (*How is it settled?*)

The principle adopted to know the operating limits of the entity subject to test and to detect the earliest assignable causes of failure (i.e.: causes non related to the technological limitations and in principle able to be corrected), is to apply stresses to the selected entity on a staggered basis, starting from a level at least equal to the level specified in use, and increasing that level by successive steps.

If, in the absence of failure (according to previously defined criteria), a level of stress is reached so that the maximum predictable dispersion of variability sources (e.g. manufacturing processes, internal characteristics of materials, environment...) has no effect on the compliance of performance vs. specification, the operating margin is considered sufficient and the test may be stopped.

In case of occurrence of a failure (according to the defined criteria) under a given level of applied stress, it is necessary to conduct a thorough technological analysis to determine the root cause. Then, two situations can arise:

- The cause of failure is «assignable» (i.e. inadequate tolerancing, poorly calibrated component, manufacturing problem...): a corrective action to eliminate that cause or to reduce its effects (known as a "bypass" process) is then initiated. This corrective action being incorporated, the iterative process of Highly Accelerated Tests is taken again from the stress level under which the failure occurred,
- The cause of failure is inherent in technology used, in the nature itself of the product concept or in manufacturing processes. It is considered that the technological limit of the product is reached, this limit may be sufficient regarding the specification, or otherwise inadequate, which must result, as appropriate, in:
 - Either a review of the specification,
 - Or a change of the design of the entity.

Whatever is the decision, the Highly Accelerated Test involving the considered stress is stopped.

The demonstration of efficiency Highly Accelerated Tests may be naturally measured in terms of profitability. The method for assessing the profitability is to compare:

- The additional costs generated by implementation of Highly Accelerated Tests (testing resources, possible destruction of prototypes, time of operators...),
- Gains (in economic terms) resulting from the detection of early failures and correct them.

Relevance Area

- As a priority, product or processes elements that are critical considering their function or some characteristics of novelty: new design, new technologies, new profile of use, processes not yet mature...

Inputs

- Life profile of the product,
- Specified stress values,
- A priori critical elements (FMECA outputs),
- Stresses considered efficient.

Outputs

- Operating margins,
- Potential weaknesses of the product.

Pros

- Determination of operating margins,
- Identification of design defects of the product (assignable causes of failures),
- Construction of the robustness of the product.

Cons

- Need of the availability of specific tests facilities (e.g., 6 axis vibrators),
- Impossibility to assess product reliability,
- Destruction of the tested entities (in general).

Bibliography

- **ASTE**: « Le rôle des essais dans la maîtrise de la fiabilité ».
- **Projet ISdF**°4/99 : « Recommandations pour l'usage industriel des essais hautement accélérés ».
- **BN Ae – RG Aéro 000 29** : « Guide pour la définition et la conduite d'essais aggravés ».
- G.K. Hobbs « Accelerated Reliability Engineering « John Wiley & Sons » 2000.
- Harry W. McLean « HALT, HASS & HASA explained: Accelerated Reliability Techniques » - ASQ Quality Press (Milwaukee – Wisconsin).

Burn-in tests

Objective (What for?)

To highlight the early failures of a product, to be corrected before delivery.

Description (What does the method produce and how?)

Burn-in proofs involve submitting units (or some of their sub-units) of a material out of production, to adapted stress cycles (electrical, mechanical, thermal...) in order to precipitate latent defects (present in the product) in obvious defects (observable). The applied stress level can be, as appropriate, lower or equal than the values specified in use (**classical burn-in**) or greater than these values (**highly accelerated burn-in**). **In all cases, the basic principle is to stimulate rather than to simulate, but not to destroy.**

Method Management (How is it settled?)

The decision and planning of burn-in proofs has to be established ahead of the Production phase, on the basis of economic and technical feasibility criteria... The debugging (burn-in) process of is the result of a recurring process that has to be broken down as follows:

- At the beginning of the Design phase, initial planning of burn-in proofs:
 - Economic interest of burn-in,
 - Part(s) of the system(s) to be submitted to burn-in (i.e.: boards, equipment, subsystems...),
 - Considered debugging profile: nature of stresses, levels of stresses, duration of stresses application...
- At the end of the Design phase: experimentation (e.g. using DoD - Design of Experiments) of the burn-in profile initially planned to burn a few units with a configuration close to the final configuration. Based on the results, the initial environment profile can be modified to make debugging more efficient,
- During the Production phase, Burn-in proofs should continue to be driven on the basis of statistical analysis on the defects revealed by these tests, and of feedback data on products in operation. Based on the results of this analysis, the following decisions may be considered:
 - To continued burn-in according to the same profile: if burn-in defects rates remain significant, if the processes appear still immature and if few failures in operation are observed,
 - To change the burn-in environmental profile: if too many failures in operation are observed (i.e.: the current debugging process is not efficient enough),
 - To stop burn-in: as soon as the processes are mature, and the burn-in defects rates and failures rates in operation become very low. Another decision could be not to stop burn-in completely, but to apply it only on samples taken periodically to ensure that there are no significant deviations in manufacturing processes or in the quality of the input products.

The burn-in efficiency depends mainly on the environmental profile selected at each application level boards, equipment...). To choose the nature of applied stresses, it is recommended to analyze prior to any decision the full life profile of the product and to characterize the environmental stresses associated with different situations of that profile. The initial debugging profile should be designed to stimulate latent defects whose apparition during the life profile may be correlated with the identified operation and environment stresses, in compliance with the operating margins of the entity. The most efficient and most used debugging profiles are constituted by repetitive sequences of **thermal cycles** and **random vibration cycles**, with the addition of stimuli and "on-off" sequences in the case of electronic equipment.

In the case of highly accelerated burn-in, the stress levels are applied beyond the specified values. This requires having performed upstream Highly Accelerated Tests ensuring the robustness of the product, allowing and to know the **operating limits** of the product (i.e., limits of the area in which performance remains nominal) and **destruction limits** (i.e.: d limits of the area in which performance is degraded but reversible). Levels applied in this type of burn-in are generally between these two limits, in order to achieve the maximum efficiency without significantly cut into the potential lifetime of the product. In this case, validation tests of the selected burn-in profile will burn will be performed before transfer to the production, in order to check, on the one hand, the **harmlessness**, and, on the other hand, the **efficiency** of this profile.

Relevance Area

- Electrical or electronic equipment (complete assemblies, sub assemblies, boards, components). At a fine level of assembly of the system (e.g. boards), stresses applied may be more easily customized to the needs, and may therefore prove to be more efficient,
- Innovative technologies equipment and/or innovative or poorly controlled manufacturing processes, defects generated in the assembly operations (e.g., welds, connections, tolerances not met...),
- Critical sub-assemblies (e.g., space, medical...),
- Materials submitted to a severe operating environment.

Inputs

- Nature of the product,
- Manufacturing processes,
- Manufacturing work-flow,
- Operating limits and destruction limits (highly accelerated burn-in),
- Life profile of the product,
- feedback data on similar products,
- Available testing facilities.

Outputs

- Highlighting of latent defects,
- Correction and / or replacement of defective units before delivery.

Pros

- Reducing the number of corrective actions after delivery to customers,
- Customer satisfaction.
- Improving the brand image.

Cons

- Cost and time associated with the burn-in operation (availability of test facilities, specific energy consumption, and labor).

Bibliography

- ASTE « Guide pour le déverminage des matériels électroniques » (1987).
- ASTE « Guide pour le déverminage des matériels électroniques : apport de la démarche aggravée » (2006).
- BNAe RG Aéro 000 29 : « Guide pour la définition et la conduite d'essais aggravés ».
- CEI 61163-1: « Déverminage sous contraintes Partie 1 : Assemblages réparables fabriqués en lots » (2008).
- G.K. Hobbs « Accelerated Reliability Engineering « John Wiley & Sons » (2000)
- Harry W. McLean: « HALT, HASS & HASA explained: Accelerated Reliability Techniques »
- ASQ Quality Press (Milwaukee - Wisconsin).

Failure Report and Corrective Action System (F.R.A.C.A.S.)

Objective (*What for?*)

To provide all information required to identify the causes of dysfunction of a product, occurring during its design or in use, the objective being to implement, at the right time, the appropriate corrective actions. To provide indicators for assessing the reliability growth of the product during Design phase or during use.

Description (*What does the method produce and how?*)

Failure report and corrective Action System (FRACAS) involves establishing, at both the supplier in the product design phase, and the user during operation, a feedback loop to record, document and analyze all incidents occurring during the life cycle of the product. This feedback loop is based on an appropriate organization of the development team (at the supplier) and the operation or maintenance monitoring team (at the user).

Method Management (*How is it settled?*)

FRACAS hinges primarily on:

- The formalization of structured operating rules using different skills within the program or project, based on the internal organization of the industrial or operator,
- The existence of appropriate documentation,
- The implementation of incident management tools and databases,
- The achievement of in-depth expertise to analyze the incidents and determine the causes.

Incidents being recorded as and when they appear in the database, a major objective of FRACAS is to highlight those that suggest a reproducibility, in order to investigate the causes and correct them. It is suitable for this purpose:

- Favor the degree of investigation over the causes of all incidents, even if they are not critical for the program (or quality of service),
- Classify each cause of incident according to two types of criteria:
 - the cause is assignable (a priori reproducible incident),
 - the cause is not assignable (fortuitous incident).
- Decide which incidents have to be investigated further,
- Decide incidents for which corrective actions have to be undertaken,
- Develop in due course the pertinent corrective actions,
- Verify the efficiency of these corrective actions (after sufficient operating after introduction).

A key to the efficiency of FRACAS is the structure itself of the database and the nature of the input data. These data are entered into the database before being supplemented by further investigation.

Failure analyses can be conducted at different levels and often require the participation of the supplier of a part or of a "bought as is" specific module. The failure analyses are normally required in the case of the most critical incidents (i.e. recurring incidents, incidents difficult to repair, incidents involving safety, etc).

The database, which is the heart of FRACAS, allows to issue of periodically summary reports for the incident management system:

- History of incidents recorded over a given period,
- Critical Points List,
- Indicators of reliability growth,
- Histograms, Pareto charts...

Relevance Area

- Implementation at the supplier, throughout the Design phase, when the first models or prototypes of the product are available, and in Production and Operation phases,
- Implementation at the user, during Operation phase and withdrawal phases, under the responsibility of the user who is able to feed the database, via feedback from incidents arising during these phases.

Inputs

- Data on the observed failures (via incident files),
- Results of expertise.

Outputs

- Planned corrective actions
- Indicators of reliability growth, histograms,
- Change of maintenance procedures,
- Critical Points List.

Pros

- Identify and correct causes of failure before the start of production,
- A key element in reliability growth.

Cons

- Requires a structured project organization,
- Difficult to know the duration of use in Production and Operation phase.

Bibliography

- RE Aéro 703 06: « Guide pour le pilotage de la croissance de fiabilité ».
- RG Aéro 000 33: « Logique de traitement des incidents dans le cadre d'un programme ».
- MIL STD 2155: « Failure Reporting, Analysis & Corrective Action System (FRACAS) ».
- DGA/AQ 6008: « Guide pour le pilotage de la croissance de fiabilité ».
- RAC Reliability Toolkit (Commercial practices edition).

Life Cycle Costing (L.C.C.)

Objective (*What for?*)

The objective of Life Cycle Cost (LCC) Analysis is to optimize and control the overall global owning cost of a product, machine or facility. It is an economic input to facilitate the strategic choices of product design and development, and cost controlling. The Design to Cost is an essential methodological tool in this approach. This analysis can guide **dependability** studies, maintenance and Integrated Logistics Support studies.

Description (*What does the method produce and how?*)

Life Cycle Cost (LCC) Analysis aims to guide decision-making of designers and purchasers, with a view as broad as possible on costs induced by the equipment, from its acquisition until its dismantling. It helps to identify the most important cost centres. The approach can be structured in 4 stages:

- Analysis plan of LCC: scope, objective, expected results,
- Development of the LCC model: level of analysis, life cycle phases, cost tree, cost categories,
- Analysis of the LCC model: gathering information,
- Management of the analysis of LCC: documentation, analysis of results, update.

Method Management (*How is it settled?*)

Life Cycle Cost (LCC) Analysis involves forecasting the costs associated with various phases of the life cycle of the product:

- Statement of the need,
- Preliminary design,
- Detailed design and qualification,
- Industrialization,
- Production,
- Use,
- Withdrawal of service.

Each phase generates costs. All of these phases are concerned by LCC control. The analysis has to be performed from the upstream phases, because they induce costs on the phases of development, production and use. LCC is calculated at a given date and for a defined period. Calculations must perform in terms of updated costs, because the durations considered are relatively large (lifetime of the product).

Relevance Area

- During Design phase, the approach allows make design choices by identifying influential factors,
- During Operation phase, the approach can help guide management decisions for the facility from the changes of energy costs, the increase of maintenance tasks, as the decline in system performance.

Inputs

- Phases of life cycle,
- Cost categories (labor, material, energy...),
- Collection of cost items,
- Dependability performance,
- Reference duration considered...

Outputs

- Trends in operating costs,
- Average cost over a given reference period,
- Most important Cost centers...

Pros

- LCC analysis allows highlighting the key cost drivers (energy, reliability, maintenance...),
- It provides an overall view and allows a justified decision.

Cons

- The realism of LCC analysis depends on the relevance of forecasted reliability, on the price trends, on the impact of failures...

Bibliography

- Standard XP X 50-155: Management par la valeur – Coût global, décembre 1997.
- Standard CEI 60.300-3-3: Dependability management – Application guide – Life cycle costing, juillet 2007.

Glossary

English acronym	Definition	Acronyme français	Définition
C.C.P.	C ontrol C ritical P oints		
C.M.M.I.	C apability M aturity M odel I ntegrated		
C.O.T.S.	C ommercial O ff T he S helf		
C.T.A.	C ause T ree A nalysis		
C.T.M.	C onsequence T ree M ethod		
D.o.E.	D esign of E xperiments		
E.F.A.	E xternal F unctional A nalysis		
E.T.A.	Event T ree A nalysis	A.A.E.	Analyse par A rbre d' E vénements
F.A.	F unctional A nalysis	A.F.	Analyse F onctionnelle
FEX	F ield E Xperience		
F.M.E.A.	F ailure M ode and E ffects A nalysis	A.M.D.E.	Analyse des M odes de D éfaillances et de leurs E ffets
F.M.E.C.A.	F ailure M odes, E ffects and C ritical A nalysis	A.M.D.E.C.	Analyse des M odes de D éfaillances de leurs E ffets et de leur C riticité
F.R.A.C.A.S.	F ailure R eport A nd C orrective A ction S ystem	L.T.I.-A.C.	L ogique de T raitement des I ncidents et A ctions C orrectives
F.R.f.P.	F unctional R equest for P roposal		
F.T.A.	F ault T ree A nalysis	A.D.	A rbre de D éfaillances
G.C.O.	G lobal C ost of O wnership	C.G.P.	C oût G lobal de P ossession
H.A.C.C.P.	H azard A nalysis C ritical C ontrol P oint	A.R.P.I.C.-M.	Analyse des R isques, P oints C ritiques pour leur M aîtrise
H.A.L.T.	H ighly A ccelerated L ife T est		
HAZOP	H AZard and O Perability study	HAZOP	Etude de danger et d'opérabilité
I.D.S.	I ntegration D esign and S upport		
I.E.C.	I nternational E lectrotechnical C ommission	C.E.I.	C ommission E lectrotechnique I nternationale
I.F.A.	I nternal F unctional A nalysis		
I.L.S.	I ntegrated L ogistic S upport	S.L.I. I.C.S.	S outien L ogistique I ntégré I ntégration C onception et S outien
I.N.R.S.			I nstitut N ational de R echerche et de S écurité
I.S.d.F.	I nstitut de S uret� de F onctionnement		
L.C.C.	L ife C ycle C ost	C.C.V.	C oût de C ycle de V ie

English acronym	Definition	Acronyme français	Définition
M.T.B.F.	Mean Time Before Failure		
M.T.T.F.	Mean Time To Failure		
M.T.T.R.	Mean Time To Repair		
O.A.S.	Office of Aerospace Standardisation	B.N.Aé.	Bureau de Normalisation Aéronautique
P.H.A.	Preliminary Hazard Analysis	A.P.R.	Analyse Préliminaire de Risques
P.M.R.A.	Preliminary Mechanical Reliability Assessment		
P.R.A.	Preliminary Reliability Assessment		
P.S.A.	Probabilistic Safety Analysis		
R.A.	Reliability Allocation		
R.A.M.S.	Reliability, Availability, Maintainability and Safety		
R.B.D.	Reliability Block Diagrams	B.D.F.	Blocs Diagrammes de Fiabilité
R.C.M.	Reliability Centered Maintenance	M.B.F.	Maintenance Basée sur la Fiabilité
S.E.E.A.	Software Effect Error Analysis	A.E.E.L.	Analyse de l'Effet des Erreurs du Logiciel
S.I.L.	Safety Integrated Level		
S.P.I.C.E.	Software Process Improvement Capability dEtermination		
S.T.A.E.	Scientific and Technical Association of the Environment	A.S.T.E.	Association Scientifique et Technique de l'Environnement
T.B.D.	To Be Defined		

Page intentionally blank

M2OS - IMdR