Performance Levels and Degradations with Dependability

Kenza Berrada
Laboratory of industrial techniques, Faculty of Science and Technology of Fez, Sidi Mohamed Ben Abdellah University, Fez.
Kenza.berrada0101@gmail.com

Brahim Herrou
Higher School of Technology BP.2427 Imouzzer road, Fez.
brahimherrou@yahoo.fr

Abstract

The growth of development of new technologies has not stopped since the industrial revolutions of the 18th and 19th centuries. Currently, production systems or controlled equipment (in English "Equipment Under control") designate complex and critical characteristics requiring a high level of performance in constant evolution, while confronting strong economic, human and environmental constraints. Generally, performance is a three-dimensional discipline represented by socio-economic efficiency, the quality of the service rendered and management efficiency. The main issue that characterizes it is that of failure, deduced through malicious acts, referring to dependability. This failure science is modeled by an acronym RMAS ("Reliability", "Maintainability", "Availability" and "Security"), consists of analyzing failures during a change in system behavior through the analysis of the mode of failure. This notion is at the heart of the Analysis of Operational Safety.

With this in mind that our work aims to master technological systems and associated risks in order to objectively know their performance and help optimize them on the production, safety and environmental aspects, to then allow them to maintain their performance over time.

Keywords:

Performance, Failure, Dependability

1. Introduction

In view of the current economic context, the evaluation of production performance system is of an indisputable critical and strategic character. The production performance system is now plural and multidimensional. It must be assessed globally and over the entire life cycle of the system and the products produced. It not only integrates the concepts of cost, deadlines, quality, but also flexibility (ability to quickly change the current planning and / or modification of the production tool), robustness (stable behavior with respect to variations in demand and occurrences of hazards) and of value (linked to customer satisfaction). In addition, human and social factors, long underestimated, are now its parameters preponderant. This results in a strong need for methodologies and tools that can help decision-makers better understand the notion of performance and evaluate it during the design, operation and reconfiguration of a production system (C. Tahon , 2003). Performance must be assessed over the entire life cycle of the system or the products produced. This diversity, motivated by a socio-economic logic of sustainable development, generates a strong need for methodologies, techniques and tools to help the choices of decision-makers in the design, development or operation phases of products and systems. There are many answers; There are also many specialized books and articles that expose these, from a detailed statement of all forms of help to the precise presentation of a particular tool or technique (D.Noyes & F.Peres, 2007).
The search for performance is, in fact, correlated with the constant concern of improving the operational availability of the system and optimizing its overall cost of ownership.

2. Definition of concepts:

2.1 System:

A system can be described as a set of elements interacting with each other and with the environment on which the behavior depends:
- Individual behaviors of the elements that compose it,
- Interaction rules between elements (interfaces, algorithms, protocols),

- The topological organization of the elements (architectures).

The fact that the subsystems are interacting implies that the system is not simply the sum of its components. Strictly speaking, a system in which an element is defective becomes a new system, different from the initial system.

Any system is defined by one or more functions (or missions) that it must perform under given conditions and in a given environment. The purpose of the dependability study is function. A function can be defined as the action of an entity or one of its components expressed in terms of purpose. A distinction must be made between functions and structure;

- Main function: purpose of a system
- Secondary functions: functions performed in addition to the main function
- Protective functions: means to ensure the security of property, people and the environment;
- Redundant functions: several components perform the same function.

2.2 Dependability:

Dependability is the ability of an entity to operate when and as required, it is the ability of a system to perform one or more functions required under given conditions; it mainly encompasses four components: reliability, maintainability, availability and security.

Knowledge of this ability to perform one or more functions allows users of the system to place a justified confidence in the service it provides them.

Operational safety is often referred to as the science of failure; it includes their knowledge, their evaluation, their forecast, their measurement and their control. This is a transversal field which requires a global knowledge of the system such as the conditions of use, the external risks, the functional and material architectures, the structure and the fatigue of the materials. Much progress is the result of experience feedback and accident analysis reports.

2.3 Availability:

Availability is the ability of an entity to be in a position to perform a required function. An entity can both be on standby (not used) and be available.

Availability at time t:

Let A (t) be the availability of an entity at time t.

A (t) = Probability [the entity is able to perform the required function at time t]

Let X (t) be the (random) state of an entity at time t such that:

X (t) = 1 if the entity is able to perform the required function at time t ("running")

X (t) = 0 otherwise (“out of order”) A (t) = Probability [X (t) = 1]

Average availability:

Let U be the average availability of an entity (in a given period of time).

Let MUT (“Mean Up Time”) be the average time (in a given period of time) when the entity is able to perform the required function and MDT (“Mean Down Time”), the average time (in a given period of time), where the entity is unable to perform the required function.

$$U = \frac{MUT}{MUT + MDT}$$

2.4 Failure:

A failure is a cessation of an entity's ability to perform a required function or to function as intended. [CEI61508, 1994]

The failure of an entity is an event resulting in a state of failure of this entity.

Failure mode:

A failure mode is a circumstance of occurrence of a failure.

Examples of failure modes are: does not open, does not close, does not stay in position, internal leak, external leak, untimely operation, does not stop, does not trip, loss of exit, court -circuit, etc.

Failure rate:

The (instantaneous) failure rate (time) is looking for one of the entity's failures to occur in the time interval [t; t + Δt] knowing that the failure did not occur until time t, divided by Δt, and when Δt tends to zero.

Without the condition "the entity has remained" running "until time t", this is the unconditional time (or "failure frequency").

By replacing this same condition with "the entity is" running "at time t", it is the conditional (instantaneous) failure intensity (or "Vesely failure rate")

").

In the so-called “running-in” phase, the decreasing failure rate; in the so-called “useful life” phase, the constant failure rate; and in the so-called “old age” phase, the increasing failure rate.

2.5 Reliability:

Reliability is the ability of an entity to perform a required function, without failure, during a given time interval and under given conditions.
Reliability at time t:
Let R (t) be the reliability of an entity at time t.
R (t) = Probability [the entity remains in a state to perform the required function until time t].
Let T be the (random) time between the (re) start-up of the entity and its next failure.
R (t) = Probability [T> t]
Average (operating) time before failure:
The MTTF ("mean time to failure") is the average time between the (re) start of the entity and its next failure.
The MTTF is the mathematical expectation (the average) of the random variable T. In the case where the failure rate is constant, the MTTF is the inverse of the failure rate. Certain references also define the "average time before the first failure" (MTTFF).

2.6 Maintainability:

Maintainability is the ability of an entity to be maintained or restored to a state allowing it to perform a required function, under the conditions of usage and maintenance data. [IEC 60050,2015]

Average recovery / failure time:
In accordance with standard IEC 61508: The MTTR ("average restoration time") is the average time between the last failure of the entity and its restart.
The MTTR here includes the effective repair time, but also the detection, logistics (for example transportation of maintenance personnel, tools and parts) and shutdown time.
Alternative definition (more common):
MTTR ("average time to repair") is the average time for effective repair.
In any event, the times included and excluded from the MTTR should be specified.

2.7 Security:

Security is the ability of an entity to prevent the occurrence of serious events (events that may lead to harm to the health of persons, to the environment, to reduce the consequences of such events on people, the environment, or property.
Security is analyzed by the publication that an entity avoids revealing, under given conditions, critical or catastrophic events.
Dependability aims to define, design, build and operate systems where the fault is natural, expected and tolerable.

2.8 Performance:

It is the attitude of an actor or an organization to achieve its objectives optimally. Several concepts are linked to the notion of performance, they are grouped according to the following triangle.

Figure 1: Performance triangle

Relevance measures the adequacy between the objectives and the means mobilized.
Efficiency is the ability to achieve the results obtained by the means used.
Efficiency: The ability to achieve optimal results while saving resources.
Overall performance is therefore the combination of these three capacities in figure 1. To measure them, there are several performance indicators used by companies. These indicators can be quantitative (Provide a measure value) or qualitative (satisfaction rating). The overall performance is finally grouped in a forward-looking dashboard whose objective is to facilitate the management of the company as well as the implementation of action plans.
As part of an evaluation process, the performance analysis verifies that the organization performs effectively and relevantly (the right things), efficiently (quickly, at the right time, at the lowest cost) to produce the results were established or assisted and met the needs and expectations of the organization's customers (or even more generally of all of the “stakeholders”).

There are three levels of performance:
 Top Reliability Performance
The service is performed with excellence, while respecting the requirements and standards of the sector. The objectives of the balanced scorecard are successfully achieved and the system's forecast monitoring is well assured;
 Good or sufficient performance
The customer positively evaluates the service provided. No problems were reported.

 Insufficient performance
Existing problems: the customer negatively assesses the service performed. In this case, it is necessary to consult the Dashboard to determine the improvements you can make to the failing service,

3. Operational safety analysis method:

A predictive operational security analysis is a process of studying a real system in order to produce an abstract model of the system relating to a characteristic of operational security (reliability, availability, maintainability, security).
The elements of this model will be events likely to occur in the system and its environment, such for example:
- System component failures and failures,
- Events related to the environment,
- Human errors in the operational phase.
The model thus makes it possible to represent all the failures and breakdowns of the components of the system which compromise one of the characteristics of dependability
In order to assist the analyst, several methods of analysis have been developed. The main ones are:
APD Preliminary Hazard Analysis,
AMDE Analysis of failure modes and their effects,
MDS Success Diagram Method,
MTV Truth Table Method,
MAC Cause Tree Method,
MCPR Method of Combinations of Summary Faults,
MACQ Method of the Consequence Tree,
MDCC Cause-Consequence Diagram Method,
MEE State Space Method.

3.1 Preliminary Risk Analysis:

Preliminary risk analysis was first used in the United States in the early sixties. Since then, this approach has conquered a number of industrial sectors such as the aeronautical, chemical, nuclear or automotive industries.
The objectives of this method are:
- Identify the dangers of a system and define its causes,
- Evaluate the severity and consequences of dangerous situations and potential accidents.
A question of this study, corrective actions are implemented to allow the control or the elimination of dangerous situations and potential accidents detected. It is recommended to carry out the preliminary risk analysis from the first design phases. This study will then be completed and enriched to measure the progress in the life cycle until the end of the system's life. The APR is generally a preliminary study requiring the performance of additional dependability studies such as the fault tree method useful for determining the causes of undesirable events detected during the preliminary analysis.

3.2 The Failure Trees Method

The fault tree is a graphical tool widely used in the studies of security and reliability of systems. This tool, allows you to graphically predict the possible combinations of events that allow the occurrence of a predefined adverse event. The fault tree is thus formed of successive levels of events which are articulated through gates. By adopting this representation and the
deductive logic (going from effects to causes) and Boolean which is specific to it, it is possible to trace effects in causes of the undesirable event to basic events, independent of each other and probable.
When it comes to studying system failures, the fault tree is based on a dysfunctional analysis of a system that must be performed beforehand: a Failure Mode and Effects Analysis (FMEA). This inductive method (going from causes to effects) therefore appears to be a prerequisite for the construction of a fault tree since the identification of components and their failure modes is generally used at the last level of a tree.
Fault tree analysis is certainly one of the most widely used engineering techniques, along with reliability diagrams (which are based on the same mathematical foundations) to analyze the dependability of a system, but other alternatives exist.

The construction of the fault tree is an important phase of the method because its completeness conditions that of the qualitative or quantitative analysis which will be carried out thereafter.
Qualitative analysis: the fault tree being constructed; two types of qualitative exploitation can be carried out:

- The identification of critical scenarios likely to lead to the feared event. By analyzing the different combinations of failures leading to the summit event, the objective here is to identify the shortest combinations called minimum cuts (cf. "Mathematical foundations").
- The implementation of a barrier allocation procedure.

This second type of qualitative exploitation makes it possible to allocate a certain number of safety barriers (technical or of use) according to the gravity of the feared event and any normative constraints.
Quantitative analysis: A probabilistic study can have two objectives:

- Rigorous evaluation of the probability of occurrence of the feared event;
- Sorting of critical scenarios (starting from minimum cuts with higher probabilities).

➢ These calculations can only be seen if each elementary event can be probabilized from a meticulously configured law and knowledge of the mission time associated with the feared event and / or using data from the return of experience. Characteristics The operational safety characteristics or the RMAS(Reliability-Maintainability-Availability-Safety) behavior of the system have a major influence on its operational performance and, in fact, enter into the evaluation of this performance. Directly, by the expression, for example, of the operational availability of the system or indirectly, by the calculation, for example, of the total cost of ownership, the evaluation of the dependability is closely coupled with the decision-making processes engaged in design and systems management.

4. Structure of a system:

The functions are performed by the system from its components. The structure of the system must be taken into account for reliability analyzes. For this, it is necessary to describe the hardware components, their role, their characteristics and their performance.
It is also necessary to describe the connections between the components, which can be done by an oriented graph for which the set of nodes designates the set of n resources linked together by links represented by the arcs. Finally, it is also important in some cases to specify the location of the components.
Reliability analyzes are based on assumptions about the independence of failures in basic functions. Sharing resources and installing these resources in the same area can violate independence requirements. For example, a tire blowout in an airplane can cause several components to fail.
A reconfiguration is the act of modifying the structure of a failed system, so that the non-failing components can provide acceptable, albeit degraded, service.

4.1 Taxonomy:

Operational safety handles a certain number of concepts which we specify in this part by giving precise definitions. Operational safety can be seen as consisting of the following three elements:
- Attributes: points of view for evaluating operational safety;
- Obstacles: events that can affect the operating safety of the system;
- Means: means to improve operating safety. These concepts are summarized in the figure 2 below (C. Pagetti,2012):

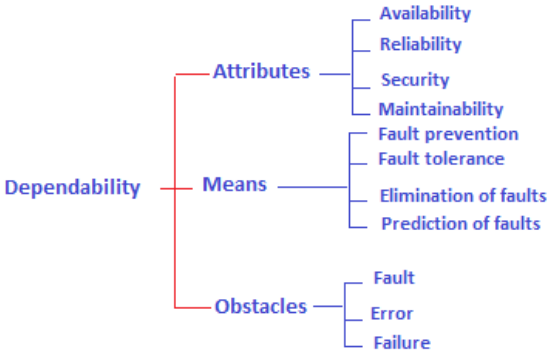

Figure 2: Operational safety tree

The hindrances are divided into 3 concepts: faults, errors and failures that are linked as shown in Figure 2. The definitions are recursive because the failure of a component is a fault for the system that contains it.
(Fault): The cause of the error is a fault (for example a short-circuit on a component, an electromagnetic disturbance or a software development fault).
(Error / Defect) The cause of the failure is an error affecting part of the system state (for example, an erroneous variable).
(Failure) is the termination of an entity's ability to perform a required function.
(Breakdown) is the inability of an entity to complete a mission. A breakdown always results from a failure.

Failures in a system can have different effects (Figure3). Some failures do not directly affect the functions of the system (Table 1) and only require corrective action; others, however, affect availability or security

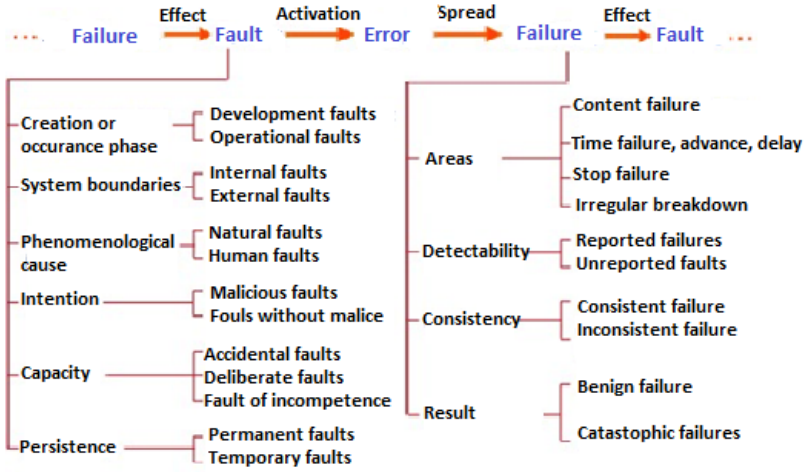

Figure 3: Propagation of error

Minor failure	Failure that impairs the proper functioning of a system by causing negligible damage to the it or its environment without presenting any risk to humans
Major failure	Failure which interferes with proper functioning without causing significant damage or presenting a significant risk to humans
Hazardous failure	Failure that results in the loss of essential system function and causes significant damage to the system with only a negligible risk of death or injury
Catastrophic failure	Failure which results in the loss of essential system function by causing significant damage to the system or its environment and / or results in death or personal injury

Table 1 : Classification Failure

(Failure mode): A failure mode is the effect by which a failure is observed. More specifically, these are the possible states of a failed entity for a given required function (Table 2).

Failure mode	Explanation
Premature functioning	Works when not planned at this time
Doesn't work when expected	Doesn't start when solicited
Don't stop at the scheduled time	Keep running when it's not planned
Failure in functioning	

Table 2: Classification failure mode

5. Performance evaluation during phase design:

To assess the performance of the system during its design, it is necessary to define the overall performance of the company first.
The overall company performance assessment model highlights the overall performance drivers specific to the company in which the design system fits. We thus define 3 main axes for this evaluation: Actor axis, environment axis and technological axis.
The overall assessment steps can be summarized as follows (R.Vincent, 2008):
Step 1: Modeling the company and highlighting the overall performance vectors,
Step 2: Monitoring the development of the company,
Step 3: Modeling of the design system and highlighting local performance vectors,(Table3)
Step 4: Monitoring the progress of the design process and activities,

Design model	Form of piloting	Evaluation criteria	Forms of assessment
Hierarchical succession of phases	Steering based on project management rules.	• Costs, • Quality • Deadlines	Indirect quantitative assessment of drifts on the steering parameters.
Iteration of an elementary cycle	Management integrated into the process.	Expected results at each iteration: • Simulations • Prototypes	Technical evaluation based on the results of the iteration and on a redefinition of the objectives and specifications.
Production process	Management centered on human resources, based on the methods used in production management.	• Availability • Reliability • Variability • Reactivity	Complex direct evaluation, based on criteria of costs and use of human resources.
Innovative design	Steering centered on resources, process, organization.	• Costs • Quality • Timeframes • Design process • Market • Requirements	Evaluation of the design results and process.
	Management by level and focused on the risks inherent in the process.	Levels: strategic, tactical, operational Risks: Functional, uncertain, organic	Relative assessment of the objective to be achieved, the technical solution and the organization put in place.

Table 3: design assessment (Step 3 details)

In terms of system design, it is important to be able to answer questions such as:
- Which component should be improved as a priority to increase the reliability of the system?
- Which parameters of the components have the most influence on the reliability of the system?

6. Evaluation of operating performance:

In the operating phase, we go through several stages to assess performance:
1. Data search:
 Reliability tests
 Collection in use
2. Data processing:
 Operational safety parameters:
- Failure rate in operation (λ)

- Failure rate at stop (λa) [E fails on [t, t + Δt] knowing that it was at stop, in working order on [0, t]]
- Failure rate on request (γ) [E refuses to change state when requested in the form of a request]
- Repair rate (μ)
- MTTF, MTTR, MUT, MDT, MTBF

3. Parameter results law:
 Choice of law
- Curve λ = f (t) "in bath" → useful life, well suited to electronic components + electromechanical components if preventive maintenance
-Log-normal law: well suited to repair times
 Hypothesis tests
-Is the random variable well governed by this law?
-Test X^2
4. Confidence interval:
 Principle: Evaluation of the bounds [λinf, λsup] of an interval (called confidence) surrounding the estimator λ
Let α = P [λ ∉ [λinf, λsup]] Then 1- α is called confidence level
 Interval calculation
5. Modeling of λ:

Principle $\lambda = \lambda_b \times \pi_E \times \pi_A \times \pi_Q \times \pi_n$, with:

λ_b: base rate obtained from reliability tests under standardized constraints (environment, etc.)
π_E: environmental cost. Ex (component e-given): - 0.2: normal, use on the ground - 4: subjected to vibrations and shocks, on the ground - 10: severe conditions (boarding on missile)
π_A: adjustment coefficient for use (sec. constraints)
π_Q: quality coefficient (for design)
π_n: adjustment coefficient (other factors: repeated cycles)
At the operational level, it is interesting to answer questions such as:
- What are the most important cuts?
- Knowing that the system is broken, which component should be repaired as a priority?
The purpose of the importance calculation is to answer these questions. Several main probabilistic factors of importance were used and their different interpretations:
- The factor of marginal importance which allows to measure the variation of the unavailability of the system according to the unavailability of its components (Z.Birnbaum, 1968).
- The critical factor which represents the response that a component has caused the system to fail knowing that the system has failed (J.B Fussell, 1975).
- The critical cut factor representing the response that a minimum cut has caused system failure knowing that the system has failed (H.E.Lambert, 1975).
- The diagnostic importance factor which represents the revelation for a component to be faulty at the moment t knowing that the component is faulty at this time (W.E.Vesely, 1996).

7. Result of an application case:

The example of an electronic system whose predictive reliability at design has been approved according to an AMDE method. The experimental reliability started with an operation of the system for a reliability test.

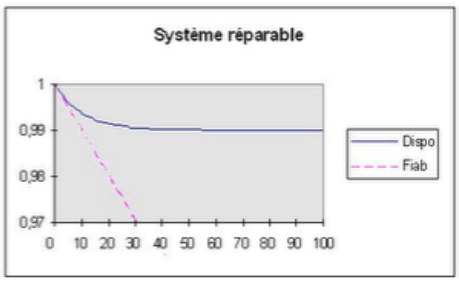

Figure 4: Reliability curve of an electronic system

The collection in operation made it possible to identify design flaws, which explains the drop in reliability in Figure 4. The system is then in the youthful period of the "bathtub" curve. The operating safety parameters make it possible to calculate the different failure rates to define the degree of failure and to estimate the repair rate and the average times recognized.

The limits of the confidence interval were then defined according to the curve λ = f (t) | for a constant rate failure period] surrounding the estimator λ. The modeling of λ prompted us to plan an additional reliability test plan that uses the study of degraded modes at the system level or increase the number of redundancies at the equipment level.
The major improvement therefore consists in improving the design while basing on the reduction of the component λ, through:
• Stronger integration of components by equipment,
• Improvement of the design of the components,
• A design with margin

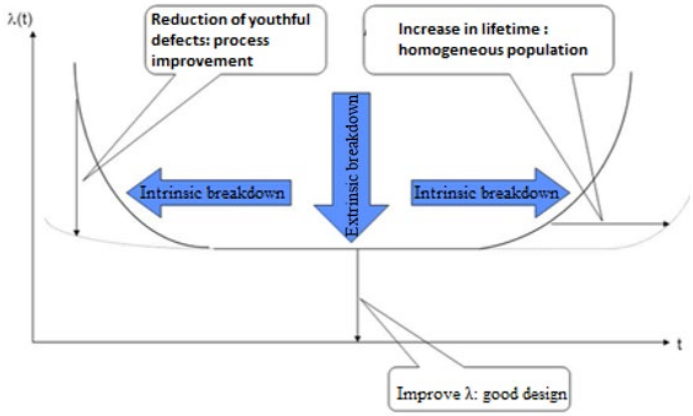

Figure 5: Variation λ composant

8. Conclusion:

The evaluation of the performance of industrial systems is an essential element in the management of companies in their recurring search for greater competitiveness. Dependability is inseparable from this system performance. Dependability describes and analyzes the mechanisms that lead to system incidents and failures and proposes and evaluates the solutions to be implemented to deal with these problems. It accounts for the ability of the system to fulfill its mission and to resist hardware, software and human failures as well as the aggressions of its environment and, in this, it characterizes the performance of a system, intervening in a major way in the achievement of this performance.
A wide range of tools is available both in design (to strengthen the system and maximize the performance / cost ratio) and in operation (to maintain quality of service and control risks that may affect its operation).

References

C.Tahon. *Évaluation des performances des systèmes de production.* Ed Hermes, Paris, 2003, 302p.

D.Noyes and F.Peres*Analyse des systèmes - Sûreté de fonctionnement. Techniques de l'Ingénieur*. http://www.techniques-ingenieur.fr/base-documentaire/genie-industriel-th6/methodes-de-production-42521210/analyse-des-systemes-ag3520/.10 Juillet 2007

CEI 61508. (2010). *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, Parties 1 à 7*.2010

IEC 60050 International Electrotechnical Commission– International Electrotechnical Vocabulary. Chapter 191: "*Dependability and Quality of Service*", Geneva, 1990

C. Pagetti-ENSEEIHT, « *Module de sûreté de fonctionnement* », 2010.

R.Vincent. *Evaluation de la performance des systèmes de conception pour la conduite de l'ingénierie des*

produits ; prototype logiciel d'aide aux acteurs. Sciences de l'ingénieur [physics]. Université Sciences et Technologies - Bordeaux I, 4 Apr 2008

Z. Birnbaum, "*On the Importance of Different Components in a Multicomponent System in Multivariate Analysis-II*," P.R. Krishnaiah, Editor, Academic Press, WASHINGTON UNIV SEATTLE LAB OF STATISTICAL RESEARCH, New York, 20 May 1968.

J. B. Fussell. -*How to hand-calculate system reliability charateristics*. IEEE Transactions on Reliability, Vol R24:169–174, Issue 3,Aug. 1975

H. E. Lambert. *Fault tree for decision making in system analysis*. PhD thesis, Lawrence Livermore Laboratory, United states https://www.osti.gov/servlets/purl/4169124 .9 October 1975.

W. E. Vesely. -*Fault tree handbook*. Technical report, U.S Nuclear Regulatory Commission, Washington, https://inis.iaea.org/collection/NCLCollectionStore/_Public/27/045/27045929.pdf January 1996

Biographies

Kenza Berrada is a PhD student in the industrial technique's laboratory of the faculty of science and technology, Sidi Mohammed Ben Abdellah university, Fes Morocco. She has a state engineer degree in Mechatronics industrial engineering, she has experience in the automotive sector as a quality manager.

Brahim Herrou is a doctor engineer in industrial and mechanical engineering. He is professor in Sidi Mohammed Ben Abdellah university ,Fes Morocco.