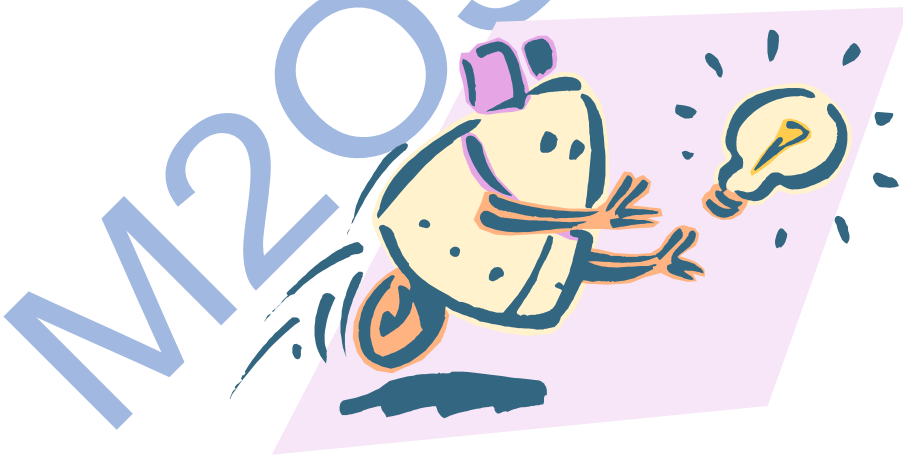
I M d R

Groupe de travail Management, Méthodes, Outils, Standards (M2OS)



Fiches méthodes

INTRODUCTION

Depuis son origine à l'ISdF (Institut de Sûreté de Fonctionnement [*1]) puis à l'IMdR (Institut de Maîtrise des Risques) le groupe de travail M2OS (Management, Méthodes Outils, Standards) fort d'une vingtaine de membres s'est donné pour tâche de publier des ouvrages destinés à servir de références aux personnes soucieuses de Sûreté de Fonctionnement et de Maîtrise des risques. Ceux–ci peuvent être débutants afin les aider à démarrer dans le métier ou plus chevronnés pour se rappeler tels ou tels éléments techniques.

Dans la lignée des ouvrages qu'il a élaborés, M2OS propose ici au lecteur un ensemble de fiches méthodes. Cet ensemble ne se veut pas figer mais évolutif en fonction de son enrichissement, en nombre de fiches, ajout d'annexes (exemples…).
Pour ce faire, il vous invite à y participer, un modèle de fiche vierge éditable est disponible sur le site de l'IMdR.
Il vous est possible d'adresser tous commentaires sur l'existant, proposer de nouvelles fiches par le moyen de votre choix en l'adressant par courriel au coordinateur du projet : prlecler@club-internet.fr .

Actuellement l'ensemble comprend les fiches suivantes:

1. Caractérisation du profil de vie d'un produit
2. **A**nalyse **F**onctionnelle (A.F.)
3. **B**locs **D**iagrammes de **F**iabilité (B.D.F.) – Reliability Block Diagram (R.B.D.) –
4. Allocation de fiabilité
5. Evaluations prévisionnelle de fiabilité
6. FIDES
7. Estimations de fiabilité à partir d'essais ou du retour d'expérience
8. Fiabilité Prévisionnelle en Mécanique
9. Fiabilité en Mécanique – la méthode Contrainte – Résistance
10. Choix et application des méthodes d'analyse de la SdF du logiciel — Mise à jour
11. SdF du logiciel: Les normes — Nouvelle
12. SdF du logiciel: Les moyens, outils et analyses — Nouvelle
13. La démarche bayésienne en fiabilité
14. **A**nalyse **P**réliminaire de **R**isques (A.P.R.) — Nouvelle
15. **A**nalyse des **M**odes de **D**éfaillance et de leurs **E**ffets (A.M.D.E.) – **F**ailure **M**ode **E**ffect **A**nalysis (F.M.E.A.) –
16. Graphe d'état
    Arbre de défaillances, arbre d'événement, arbre de causes, ne confondons pas !
17. **A**nalyse par **A**rbre de **D**éfaillances (A.A.D.) – **F**ault **T**ree **A**nalysis (F.T.A.) –
18. Analyse par arbre d'événements (A.A.E.)
19. Analyse par arbre de causes
20. Arbres de Maintenance et d'Aptitude à la Maintenance
21. Etude de danger et d'exploitabilité **– Haz**ard and **Op**erational Study (HAZOP)
22. **A**nalyse des **R**isques, **P**oInts **C**ritiques pour leur **M**aîtrise (A.R.P.I.C.–M.) – **H**azard Analysis Critical Control Point (H.A.C.C.P.) –
23. Analyse de zone
24. Maintenance Basée sur la Fiabilité (M.B.F.) – Reliability Centered Maintenance (R.C.M.) –
25. Intégration Conception et Soutien (I.C.S.)
26. Plans d'expériences
27. Essais accélérés de durée de vie
28. Essais aggravés
29. Epreuves de déverminage
30. Logique de Traitement des Incidents et Actions Correctives (L.T.I.–A.C.)
31. Coût de Cycle de Vie (C.C.V.), Coût Global de Possession (C.G.P.)
    Glossaire — Mise à jour

* 1 – **« SÛRETÉ DE FONCTIONNEMENT » et « DEPENDABILITY »**

Selon l'acception retenue en France (RG – AERO – 0040), la « Sûreté de Fonctionnement » (SdF) est l'ensemble des aptitudes d'un produit qui lui permettent de disposer des performances fonctionnelles spécifiées, au moment voulu, pendant la durée prévue, sans dommage pour lui-même et son environnement.

La SdF se caractérise généralement par les quatre paramètres suivant : Fiabilité, Maintenabilité, Disponibilité, Sécurité.

Dans certains cas, on peut y inclure d'autres paramètres tels que : Durée de vie, Survivabilité, Invulnérabilité.

Les traductions les plus communes de « Sûreté de Fonctionnement » sont « R.A.M.S. » (Reliability, Availability, Maintainability, Safety », « Dependability », « Dependability and Safety ». Cependant aucune d'entre elles ne rend compte parfaitement de la définition ci-dessus.

Dans la version française des fiches méthodologiques, nous avons retenu « Sûreté de Fonctionnement », alors que dans la version anglaise, c'est le terme « Dependability » accompagnés d'une (*) renvoyant à la présente note.

* 2 – Certaines fiches mentionnent des références non rééditées mais dont le contenu reste d'actualité et non remplacées.

* 3 – L'accès direct aux fiches s'effectue en cliquant sur la désignation dans le sommaire ci-dessus. Le retour au sommaire s'effectue en cliquant sur le titre dans la fiche.

Présidents du groupe M2OS: J.M. Cloarec (Bombardier) et Y. Mortureux (UIC/SNCF),
Coordinateur du projet: P. R. Leclercq (R.I.S.)

Membres actifs de M2OS pour le projet:

Mme M.M. Oudin–Darribère (IMdR),
MM. Y. Castellani (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)

Caractérisation du profil de vie d'un produit

Objectif *(à quoi ça sert ?)*

Assurer la validité et la complétude de la spécification d'un nouveau produit vis-à-vis de son profil de vie **réel** et fournir les entrées permettant de déterminer les marges de fonctionnement optimales vis-à-vis des performances opérationnelles attendues.

Description *(que produit la méthode et comment ?)*

La caractérisation du profil de vie réel d'un nouveau produit consiste dans un premier temps à analyser de manière détaillée l'ensemble des situations que pourra rencontrer ce produit depuis sa sortie d'usine jusqu'à sa mise au rebut ou son recyclage. Elle consiste, dans son second temps, à identifier les conditions de fonctionnement du produit (marche, arrêt, stockage…) et les agents d'environnement associés, en nature et en niveaux, sur chacune des situations identifiées. Le résultat de ces analyses sera consigné sur des organigrammes et des tableaux de synthèses adéquats.

Conduite de la méthode *(comment la met-on en œuvre ?)*

La démarche de caractérisation du profil de vie d'un produit fait appel à la synergie de différentes compétences : spécificateurs, concepteurs, spécialistes de la sûreté de fonctionnement. Elle prend naissance au stade de la faisabilité du nouveau produit afin de valider la spécification et se poursuit au-delà, en conception, en production et en exploitation de manière à cerner de plus en plus finement le profil de vie élaboré initialement. Cette démarche se traduit par la mise au point d'un document « vivant » qui s'appuiera successivement sur les résultats d'analyse, les résultats d'essais et les mesures éventuelles sur le terrain.

De manière à atteindre ses objectifs, la démarche de caractérisation du profil de vie nécessite un déroulement d'activités en **six étapes** successives :

1/ Etablissement du graphe d'états du profil de vie : définir en phase de faisabilité des « états globaux » du système appelés « segments » correspondant à des catégories d'usage bien déterminées du produit (ex : sortie d'usine, stockage, utilisation client…). Eclater ces segments en états intermédiaires appelés « phases » (ex : transport par fer, roulage d'un véhicule…), puis en « sous-phases » (ex : roulage urbain pour un véhicule), jusqu'à atteindre un niveau de décomposition auquel pourront être associés un environnement et une configuration donnée (ex : freinage urbain pour un véhicule). Ce niveau de décomposition ultime est appelé « situation ». Ces situations intègrent des incidents ou des conditions réputées exceptionnelles identifiés par les analyses de risques. Il en résulte un graphe d'états du profil de vie du produit traduisant l'arborescence de ce produit, depuis les « segments » jusqu'aux différentes « situations » identifiées,

2/ Etablissement du tableau des occurrences : en phase de conception définir des indicateurs permettant de quantifier les durées typiques et/ou extrêmes des segments, phases, sous-phases et situations mis en évidence sur le graphe d'états du profil de vie. Dans les cas fréquents où ces événements présentent un caractère récurrent, il convient de définir le nombre d'occurrences attendues des différents états identifiés du produit sur l'ensemble de son profil de vie. Le résultat se traduit par un « tableau des occurrences » (durées, nombre d'occurrences) des différents états identifiés du produit sur son profil de vie,

3/ Etablissement du tableau des agents d'environnement par situations : préciser la nature (mais pas encore les niveaux) de tous les agents d'environnement (naturels et induits) auxquels sera soumis le produit dans chacune des situations identifiées. Initiée en phase de conception, cette étape est réalisée en phase de développement avec la prise en compte des événements induits. Il en résulte un tableau indiquant, pour chaque situation, les agents d'environnement concernés. Les agents d'environnement sont regroupés par catégories : climatique (ex : chaud, froid, humidité…), mécanique (ex : vibrations, chocs), électrique et électromagnétique (ex : cycles marche/arrêt, interférences…), chimique…

4/ Etablissement des fiches de situation : caractériser aussi finement que possible chacune des situations identifiées sur le graphe d'états. Elle s'élabore dès la phase de faisabilité, se poursuit en développement avec la connaissance des solutions techniques et des environnements induits. Les agents d'environnement identifiés sont caractérisés, pour chaque situation, en terme de valeurs, de fréquences et de durées. Chaque fiche de situation, dont le format est à adapter à la nature du produit, à son profil de vie et à la nature des agents d'environnement, fait apparaître l'occurrence (typique, mini, maxi), la durée (typique, mini, maxi), les agents d'environnement rencontrés (nature, valeur, fréquence, durée), la configuration du produit (positionnement du produit, protection, lieu de manutention…) et l'état de fonctionnement (ex : fonctionnement continu, marche/arrêt, dormant…),

5/ Synthèse de l'environnement : identifier, en phase de conception, d'une part les valeurs maximales prises par chaque agent d'environnement sur l'ensemble des fiches de situation, et d'autre part les gabarits indiquant la répartition temporelle des valeurs de ces agents tout au long de la vie du produit. Les résultats obtenus sont présentés sur des formats synthétiques adaptés à la nature du produit et à son profil de vie,

6/ Enrichissement du profil de vie en phase d'exploitation : cet enrichissement suppose l'existence d'un Retour d'EXpérience (REX) de l'exploitant du produit à destination du constructeur ou du donneur d'ordre. Selon les cas, les informations permettant d'enrichir et de faire évoluer les documents afférant au profil de vie du produit sont assurées par la transmission directe par l'exploitant de toutes les données d'exploitation, ou se limitent aux incidents observés (partie « négative » du REX), ou encore à partir de sondages du constructeur auprès des utilisateurs (cas fréquent dans le domaine du grand public).

Domaine de pertinence

- Produits de conception très innovante,
- Produits dont le profil de vie est caractérisé par une forte variabilité des situations rencontrées et des agents d'environnement associés,
- Produits pour lesquels certains incidents pourraient avoir des conséquences très critiques dans leur profil de vie.

Entrées	Sorties
- Spécification initiale, - Conditions d'utilisation, - Retour d'expérience terrain, - Conception du produit, - Résultats d'essais.	- Profil de vie (de plus en plus détaillé), - Recommandations sur la spécification et les conditions d'emploi.

Avantages	Inconvénients
- Bonne connaissance du profil de vie « réel » du produit, - Spécification adaptée au profil de vie « réel », - Conception du produit adapté au « juste nécessaire ».	- Analyse parfois difficile dans le cas des profils de vie caractérisés par une forte variabilité des situations rencontrées et des agents d'environnement associés (cas des produits grand public), - Démarche itérative.

Bibliographie

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

Analyse Fonctionnelle (A.F.)

Objectif *(à quoi ça sert ?)*

Démarche qui consiste à rechercher, ordonner, caractériser, hiérarchiser et/ou valoriser les fonctions (**NF X 50.150**).
Ces fonctions sont celles du produit-matériel, logiciel, processus, service attendues par l'utilisateur.

Description *(que produit la méthode et comment ?)*

On distingue deux types d'analyse fonctionnelle :

- l'Analyse Fonctionnelle Externe (A.F.E.),
- l'Analyse Fonctionnelle Interne (A.F.I.).

L'analyse Fonctionnelle Externe, ou "analyse fonctionnelle du besoin", s'attache à décrire, pour chaque situation de son profil de vie, les fonctions attendues du produit. D'autres fonctions, qui correspondent aux réactions d'adaptation nécessaires pour tenir compte de l'environnement du produit, doivent aussi être définies, ainsi que les contraintes justifiées des utilisateurs. L'ensemble de ces données est regroupé dans le Cahier des Charges Fonctionnel ou CdCF.
L'analyse Fonctionnelle Interne, ou "analyse fonctionnelle technique", s'attache à établir des relations entre l'analyse fonctionnelle externe et les solutions envisageables pour répondre au besoin exprimé. Les fonctions identifiées par l'analyse fonctionnelle externe sont déclinées en fonctions d'ordre inférieur, ou "fonctions techniques", qui matérialisent des solutions fonctionnelles et techniques susceptibles d'être retenues, le but final étant de disposer d'éléments de comparaison objectifs entre les différentes solutions.

Conduite de la méthode *(comment la met-on en œuvre ?)*

La démarche d'analyse fonctionnelle est menée de manière participative sous la forme d'un groupe de travail, qui regroupe l'ensemble des compétences nécessaires, dirigé par un animateur. Elle s'appuie des méthodes reconnues, parmi lesquelles les méthodes :

- APTE®,
- Analyse de la valeur,
- RELIASEP®,
- SADT,
- SART,
- MERISE,
- GRAFCET…

Le choix de la méthode dépend du type de produit étudié.

Domaine de pertinence

- Tous systèmes : APTE,
- Analyse de la Valeur, RELIASEP,
- Systèmes informatiques : SADT, SART,
- Systèmes organisationnels : MERISE,
- Automates : GRAFCET.

L'analyse fonctionnelle est applicable sur toutes les phases du cycle de vie du produit.

Entrées	Sorties
- Analyse Fonctionnelle Externe: besoins et contraintes des utilisateurs, - Analyse Fonctionnelle Interne: architecture du système.	- Critères de choix des solutions techniques envisageables pour répondre aux besoins des utilisateurs, - Eléments d'entrée pour la réalisation d'Analyses des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC) ou de Blocs Diagrammes de Fiabilité (BDF). D'une manière générale, l'analyse fonctionnelle est un préalable aux études de sûreté de fonctionnement.

Avantages	Inconvénients
- L'analyse fonctionnelle permet de préciser "au mieux" les besoins réels des utilisateurs, de les traduire sous forme de fonctions à satisfaire et d'aider à optimiser l'adéquation produit/besoin, en faisant abstraction des solutions. Elle constitue, de plus, un référentiel commun pour le concepteur et l'analyste de sûreté de fonctionnement, - Par l'application de méthodes reconnues, l'analyse fonctionnelle contribue à améliorer le management d'un programme en termes de coût, délais et performances.	- La complexité de la mise en œuvre de l'analyse fonctionnelle dépend de la méthode adoptée. De même, la qualité des résultats obtenus dépend de celle de l'animateur, chargé de l'application de la méthode retenue.

Bibliographie

1. **DGA/AQ 922** : "Mémento de l'analyse fonctionnelle",
2. **NF X 50-100** : "Analyse fonctionnelle – Caractéristiques fondamentales" – 12/1996
3. Projet **SdF 1/91** : "L'analyse fonctionnelle en matière de sûreté de fonctionnement".

Blocs - Diagrammes de Fiabilité (B.D.F.)

Termes liés : Reliability Block Diagrams (R.B.D.)

Objectif *(à quoi ça sert ?)*

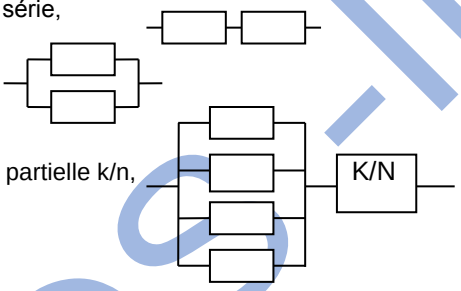
Méthodologie graphique visant à visualiser les sous-ensembles d'un système pour en faire apparaître la façon dont ils contribuent aux différentes fonctions concourant au succès de sa mission. Elle sert de base aux modélisations qui seront faite par ailleurs pour quantifier la sûreté de fonctionnement [*1] du système.

Description *(que produit la méthode et comment ?)*

Il s'agit d'une méthode graphique qui visualise, sous forme d'un diagramme représentatif des équipements participant à la mission, notamment les redondances, les éléments qui contribuent à une même fonction et les éléments de secours nécessaires. La mission peut être sous régime permanent établi, sous régime transitoire ou par phase.

Conduite de la méthode *(comment la met-on en œuvre ?)*

1. Analyse fonctionnelle : on établit les correspondances équipements fonctions intervenant dans la mission,
2. Modélisation : la représentation peut être sous forme :
   - d'équipements en série,
   - en parallèle,
   - ou en redondance partielle k/n,



Domaine de pertinence

- La méthode des Blocs–Diagrammes de Fiabilité est une des méthodes contribuant à l'analyse de la sûreté de fonctionnement pour évaluer la tenue d'un système face à des objectifs au cours d'une mission,
- Grâce à la représentation par redondances partielles, elle permet de déterminer des modes dégradés acceptables. Le niveau de redondance requis est affaire de négociation.

Entrées	Sorties
- Schémas fonctionnels du système, - Etudes FMDS, AMDEC, - Décomposition logistique du système et concept de maintenance associé.	- Diagrammes de fiabilité ou disponibilité.

Avantages	Inconvénients
- Représentation simple et logique du fonctionnement d'un système, - Prise en compte du profil de mission dans les caractéristiques des équipements, - Visualisation de la mission réalisée par le système.	- Le niveau de redondance acceptable pour les modes dégradés est arbitraire, - Difficulté de prise en compte des éléments multifonctions, - Dans ce cas, la méthode doit être menée conjointement à une AMDE(C).

Bibliographie

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

Allocation de fiabilité

Objectif *(à quoi ça sert ?)*

L'allocation de fiabilité consiste à décliner les objectifs de fiabilité spécifiés au niveau d'un produit complexe (ex : système) en objectifs applicables à différents niveaux de l'arborescence technique ou fonctionnelle du produit (démarche de type « *top down* »).

Description *(que produit la méthode et comment ?)*

L'allocation de fiabilité est une **démarche itérative.** Elle nécessite souvent plusieurs tentatives pour pouvoir satisfaire les objectifs au niveau global. Elle doit être initiée en phase de faisabilité, dès que les exigences de fiabilité de conception ont été dérivées des exigences spécifiées sur les performances opérationnelles. Normalement, une première allocation devrait être réalisée avant le début du processus de conception afin de servir d'entrée à la revue de conception fonctionnelle prévue dans la phase de définition.
Ensuite, des reprises et des mises à jour ont à être effectuées avant chaque revue majeure de conception.

Conduite de la méthode *(comment la met-on en œuvre ?)*

1 – Fixer les niveaux de décomposition d'un produit complexe déterminés de manière à satisfaire au mieux les besoins des concepteurs.
Selon les cas, il peut s'agir d'une fonction (fonction de service ou parfois fonction technique) ou d'un sous-ensemble matériel (ex : sous-système, équipement complet, organe mécanique, carte électronique…).En pratique, le choix des niveaux de décomposition doit s'appuyer sur un certain nombre de critères: complexité du produit, flexibilité de la conception aux différents niveaux de l'arborescence, critères de sécurité, entités sous-traitées à l'extérieur…

2 – Mettre en œuvre une méthode adaptée aux contraintes du projet.
Plusieurs méthodes, dont certaines faisant appel aux techniques de la recherche opérationnelle, peuvent être envisagées pour déterminer les objectifs de fiabilité aux différents niveaux de décomposition retenus sur le produit.
Les plus utilisées sont les suivantes :

- **Méthode d'équirépartition de fiabilité :** elle consiste à affecter le même objectif de fiabilité à chaque entité constituant un niveau donné de l'arborescence du produit. C'est la méthode la plus grossière dans la mesure où elle ne tient pas compte de la nature et de la configuration de ces entités, ni de la faisabilité technique,
- **Méthode ARINC :** elle suppose que les éléments pris en compte dans la décomposition du système sont en série du point de vue de la fiabilité et sont caractérisés par un taux de défaillance constant. En se basant sur un certain degré de connaissance des taux de défaillance de ces éléments (à partir de retour d'expérience ou d'évaluations prévisionnelles sur des entités similaires), la méthode consiste à déterminer les poids respectifs de chaque élément sur la fiabilité du système. Les objectifs de fiabilité alloués sont supposés respecter cette pondération,
- **Méthode AGREE :** cette méthode, repose sur les mêmes hypothèses que la méthode ARINC. Elle prend en compte la complexité des différentes entités et leur implication dans la défaillance complète du système. Elle s'appuie sur des algorithmes plus complexes que la méthode ARINC,
- **Méthode de minimisation des efforts :** cette méthode consiste à allouer des exigences qui visent à minimiser les efforts à effectuer pour atteindre les objectifs au niveau global. Les efforts peuvent être exprimés en terme financier, de nombre d'essais à effectuer, de quantité d'analyses nécessaires…

Quel que soit l'algorithme utilisé, la politique d'allocation de fiabilité doit respecter deux impératifs fondamentaux :
- être réaliste, c'est-à-dire ne pas conduire à spécifier des objectifs qui conduiraient à des solutions non envisageables pour des questions de faisabilité, d'encombrement, de délais…
- être efficace, c'est-à-dire en cherchant à minimiser certaines servitudes (coût, délais, consommation…) ou à maximiser certaines performances fonctionnelles (précision, puissance, stabilité…).

L'intérêt majeur de fixer des objectifs de fiabilité à différents niveaux de décomposition d'un produit complexe est de fournir aux concepteurs des repères sur lesquels ils pourront s'appuyer pour les choix de conception correspondants et de suivre les résultats d'essais réalisés à ces niveaux afin de les comparer aux objectifs qui leur ont été affectés et de pouvoir réorienter les choix de conception si nécessaire.

Domaine de pertinence

- S'applique essentiellement aux systèmes complexes. Les acteurs concernés par la politique d'allocation de fiabilité sont en principe au nombre de trois :
  - **le client (ou maître d'ouvrage),** à qui il revient de définir les profils de mission prévus pour le système et les objectifs de fiabilité associés,
  - **le maître d'œuvre** qui a normalement en charge de réaliser l'allocation de fiabilité sur les différents sous-systèmes, ce qui suppose pour lui une connaissance suffisante de toutes les options envisageables pour chaque sous-système,
  - **les sous-traitants** ils ont en charge d'analyser la faisabilité des solutions techniques conduisant à satisfaire les objectifs alloués et développer ces solutions pour les valider avant mise en production.

-

Entrées	Sorties
- Le/les objectifs au niveau système, - Le niveau de décomposition retenu, - La configuration des sous-ensembles.	- Les objectifs au niveau sous-ensembles.

Avantages	Inconvénients
- La déclinaison d'objectifs de fiabilité spécifiés sur un produit complexe en objectifs applicables aux niveaux inférieurs permet de déterminer les efforts à réaliser sur les différents sous-ensembles (techniques ou fonctionnels), de piloter les actions de conception et de production visant à satisfaire ces objectifs. Lorsque certains sous-ensembles sont développés par un sous-traitant externe, les objectifs alloués à ces sous-ensembles par le fournisseur (ou le maître d'œuvre) deviennent pour ce sous-traitant des objectifs de premier niveau et conditionnent le programme de fiabilité qu'il aura lui-même à mettre en œuvre, - Dans tous les cas de figure, un programme cohérent d'allocation de fiabilité amène les concepteurs à considérer la fiabilité comme une caractéristique aussi importante que puissent l'être le coût, le poids, la consommation ou toute forme de caractéristique fonctionnelle du produit.	- Dépend beaucoup de la pertinence des données utilisées pour mettre en œuvre les méthodes possibles d'allocation.

Bibliographie

1. **MIL STD-338** : « Electronic Reliability Design Handbook »,
2. KC Kapur & LR Lamberson « Reliability in Engineering Design »,
3. (John Wiley & Sons)
4. RAC Blueprints for Product Reliability.

Evaluation prévisionnelle de fiabilité

Objectif *(à quoi ça sert ?)*

La tâche a pour objet d'évaluer et d'affiner, avec un degré de précision, croissant avec l'avancement du programme, le potentiel de fiabilité du produit, à l'aide de techniques et de données évoluant généralement avec les progrès de la conception et l'acquisition de résultats d'essais. Elle constitue une base importante pour l'orientation des choix de conception et permet rapidement de comparer le potentiel de fiabilité prévisible du produit avec les objectifs spécifiés, avant même l'obtention de données d'essais ou de données opérationnelles.

Description *(que produit la méthode et comment ?)*

L'évaluation prévisionnelle de fiabilité est un **processus itératif** qui doit être initié en phase de faisabilité, dès que les données conceptuelles du produit sont disponibles. Elle se poursuit et s'affine en phases de définition et de développement, au fur et à mesure de l'avancement du processus de conception, de la connaissance de plus en plus précise des conditions de fonctionnement des composants, et de l'acquisition éventuelle de résultats d'essais significatifs.

Conduite de la méthode *(comment la met-on en œuvre ?)*

1 – Sélectionner, en début de projet la méthode d'évaluation prévisionnelle la mieux adaptée à la nature du produit et à la manière dont les objectifs de fiabilité sont spécifiés (Ex : en terme de MTBF, de durabilité…). Il est cependant possible de changer de méthode en fonction de l'avancement du programme, lorsque les données de conception (Ex. : technologies des composants utilisés, conditions d'utilisation, contraintes appliquées…) deviennent de plus en plus précises.

2 – Déterminer la (ou les) classe(s) de défaillances qui doivent être considérées de manière prioritaire dans l'évaluation de fiabilité afin de choisir la méthode d'évaluation la plus adéquate. On distingue ainsi les trois classes de défaillance suivantes :

- Les défauts de jeunesse. Ils se traduisent dans les premiers temps de fonctionnement, par un taux de défaillance décroissant avec le temps,
- Les défauts aléatoires. Ils se traduisent en période de « vie utile » par un taux de défaillance constant,
- Les défauts d'usure. Ils se traduisent au-delà de la période de « vie utile » par un taux de défaillance croissant avec le temps.

A cet effet, le tableau 1 de la page suivante présente une description synthétique des **cinq méthodes d'évaluation prévisionnelle** les plus classiques. Il met en évidence les classes de défaillances couvertes par chacune d'elles.

3 – Faire évoluer la méthode, fonction de la phase du programme au cours de laquelle elle est réalisée. Le tableau 2 de la page suivante présente une sélection de méthodes. Elles sont envisageables en fonction de l'avancement de programme.

Domaine de pertinence

- Les deux modèles génériques d'évaluation prévisionnelle, à savoir les modèles empiriques à taux de défaillance (du type « **part count** » ou du type « **part stress** »), et les modèles déterministes (basés sur la physique de défaillance) ont chacun leurs domaines préférentiels d'application,
- A cet effet, le tableau 4 de la page suivante met en évidence les différentes conditions favorisant l'utilisation de l'un ou l'autre de ces modèles dans l'évaluation prévisionnelle de fiabilité d'un produit, d'un sous-ensemble ou d'un composant.

Entrées	Sorties
- La liste des sous-ensembles/ composants, - La définition des contraintes de fonctionnement et d'environnement, - Les objectifs de niveau supérieur.	- Les caractéristiques de fiabilité, sécurité dépendant de la nature du projet des objectifs fixés par le maître d'œuvre.

Avantages	Inconvénients
- Les bénéfices attendus d'une évaluation prévisionnelle de fiabilité sont nombreux. - Ils incluent plus particulièrement : ➢ La vérification rapide de la faisabilité technique en regard de l'objectif de fiabilité spécifié, ➢ La mise en œuvre d'une allocation de fiabilité, ➢ Une entrée pour le classement des points critiques, ➢ Un moyen de comparaison de solutions techniques concurrentes, du point de vue de la fiabilité, ➢ Un élément de choix des composants (types, technologies…) et de leurs conditions acceptables d'utilisation, ➢ Une entrée pour l'estimation des lots de rechange, ➢ Une entrée pour l'évaluation du coût de cycle de vie du produit.	- Dépendent beaucoup de la pertinence des données applicables au projet.

Bibliographie

Voir tableau 3, page suivante.

1 – Méthodes d'évaluation prévisionnelle et classes de défaillances visées

Méthode	Défauts de jeunesse	Défauts aléatoires	Défauts d'usure	Description de la méthode
Modèles empiriques à taux de défaillance	**X**	**X**		S'appuie sur des modèles mathématiques de taux de défaillance de composants élémentaires (basés sur le retour d'expérience). Pour l'électronique, se décompose en : ➢ méthode « part count » : sans prise en compte des contraintes de fonctionnement, ➢ méthode « part stress » : avec prise en compte des contraintes de fonctionnement (électriques, température…).
Translation	**X**	**X**		Fait la translation d'une évaluation prévisionnelle basée sur des modèles empiriques en une estimation de fiabilité opérationnelle. Prend en compte implicitement les facteurs externes affectant la fiabilité opérationnelle (non comptabilisés dans les modèles empiriques).
Physique de défaillance (déterministe)			**X**	S'appuie sur des modèles physiques traduisant l'évolution de mécanismes de dégradation de certains composants mécaniques ou électroniques ou de procédés d'assemblage. La fiabilité globale, liée à l'usure, est obtenue par combinaison des densités de probabilités associées à chaque mécanisme de défaillance.
Données sur produits similaires	**X**	**X**	**X**	S'appuie sur des données de fiabilité empiriques observées sur des produits similaires. Cette similarité doit inclure la complexité, la maturité, les procédés de fabrication, les fonctions du produit et les conditions d'utilisation. Nécessite en général de faire appel à des facteurs de conversion pour tenir compte des différences de complexité, de l'évolution des procédés, des écarts sur les conditions d'utilisation…
Données d'essais	**X**	**X**	**X**	Prend pour base des données provenant d'essais « maison » réalisés sur des exemplaires de développement du produit considéré. Nécessite de faire appel à des coefficients de translation pour obtenir une extrapolation à la fiabilité opérationnelle observable sur le terrain.

2 – Méthodes envisageables selon l'avancement du programme

Avancement du programme	Niveau d'application	Méthodes possibles
Concept fonctionnel (phase de faisabilité)	Produit ou système	Données sur produits similaires, translation. Modèles empiriques (« part count »).
Conception initiale (début de la phase de conception)	Equipement ou sous-ensemble	Données sur produits similaires. Modèles empiriques (« part count »).
Conception finale (fin de la phase de conception)	Circuit ou composant	Modèles empiriques (« part stress »), données d'essais, physique de défaillance.
Essais (développement/production)	Du composant au produit complet	Données d'essais, physique de défaillance.

3 – Sources de données des différentes méthodes d'évaluation prévisionnelle

Méthode d'évaluation prévisionnelle	Sources de modèles ou de données
Modèles empiriques à taux de défaillance	• Méthode « part count » pour composants électroniques : - **MIL HDBK-217 F notice 2**, Bellcore **TR 332**, British Telecom **HDR 5**. • Méthode « part count » pour composants mécaniques et divers : - **NPRD-95** « Nonelectronic Parts Reliability Data », **RADC TR-85-194** • Méthode « part stress » pour composants électroniques: - **MIL HDBK-217 F notice 2**, **RDF-2000** (**UTE C-80-810**), FIDES, British Telecom **HDR 5**, SIEMENS–NORM **SN-29.500 (part 1)**.
Translation	• RAC Reliability Toolkit: Commercial Practices Edition, **RADC TR-89-299**.
Physique de défaillance	• **RADC TR-90-72**, CINDAS Data, Modèles génériques de fiabilité de composants et pièces mécaniques (ressorts, roulements, paliers…), données constructeurs.
Données sur produits similaires	Bases de données (externes ou internes) contenant les informations nécessaires: nombre de défaillances, durées opératoires, durées d'arrêt, nombre de cycles, environnement…
Données d'essais	Résultats d'essais « maison » avec les conditions d'environnement précises (nombre de cycles, contraintes appliquées, durée…).

4 – Avantages comparatifs des modèles empiriques et des modèles déterministes

Modèles empiriques (taux de défaillance)	Modèles déterministes (physique de défaillance)
- Recommandés pour les produits complexes, - Recommandés pour les analyses rapides, - Recommandés pour les analyses comparatives, - Recommandés en cas de manque de flexibilité de la conception, - Utilisables pour la sélection des composants et pour l'évaluation des contraintes (composants électroniques).	- Recommandés pour évaluer l'influence des mécanismes de dégradation sur la durée de vie des composants, - Envisageables quand les informations détaillées sur la technologie et sur les procédés sont disponibles, - Envisageables si la flexibilité de conception est suffisante, - Utilisables pour faciliter la recherche de la cause de défaillance des composants.

FIDES

Objectif *(à quoi ça sert ?)*
Estimer la fiabilité des équipements électroniques, y compris pour les systèmes qui rencontrent des environnements sévères (systèmes de défense, aéronautique, électronique industrielle, transport…) en intégrant les phases de non fonctionnement. Fournir un outil concret pour la construction et la maîtrise de cette fiabilité.

Description *(que produit la méthode et comment ?)*

La méthodologie FIDES a été développée sous l'égide de la DGA par un consortium formé par les sociétés AIRBUS, EUROCOPTER, GIAT, MBDA et THALES. Elle est fondée sur la physique des défaillances et étayée par des analyses de données d'essais, de retour d'expérience et de modélisations existantes et se distingue, en conséquence, des méthodes classiques développées principalement à partir d'exploitations statistiques de retour d'expérience.

La méthodologie FIDES traite de l'ensemble des défaillances imputables à la spécification, la conception et la fabrication du produit final. Ne sont toutefois pas prises en considération les défaillances d'origine logicielle, les pannes non confirmées, les défaillances liées à des opérations de maintenance préventive non effectuées, les défaillances liées à des agressions accidentelles, lorsqu'elles sont définies et avérées (propagations de pannes, utilisation hors spécification, mauvaises manipulations). Elle permet de traiter les phases de non fonctionnement, quelle que soit leur nature.

La méthodologie FIDES s'applique aux composants, cartes électroniques ou sous-ensembles sur étagère (COTS : Component Of The Shelf, composants sur étagère), mais aussi aux articles spécifiques dans la mesure où leurs caractéristiques techniques correspondent à celles décrites dans le guide. Son but est de se substituer à terme à la MIL–HDBK–217, qui n'est plus remise à jour depuis 1995, et au RDF 2000, inadapté aux systèmes soumis à des environnements sévères.

Conduite de la méthode *(comment la met-on en œuvre ?)*

Le taux de défaillance d'un COTS (composant, carte électronique, sous-ensemble) est estimé à partir de l'expression suivante :

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

$\lambda_{physique}$ représente la contribution physique. Il prend en compte le profil de vie du COTS (phases, conditions d'environnement), ainsi que les surcharges accidentelles susceptibles d'être subies par lui et non identifiées comme telles (« overstress »).

$\Pi_{Part\_manufacturing}$ traduit la qualité et la maîtrise technique de fabrication du COTS. Sa méthode d'évaluation se décline selon la nature du COTS considéré. Sa valeur évolue de 0,5 à 2 (pire cas).

$\Pi_{Process}$ traduit la qualité et la maîtrise technique du processus de développement, de fabrication et de maintenance de l'équipement contenant le COTS. Sa méthode d'évaluation se base sur le niveau d'application de recommandations qui portent sur l'ensemble du cycle de vie et s'appuie sur un **audit**. Sa valeur évolue de 1 à 8 (pire cas).

Domaine de pertinence	Entrées	Sorties
- La méthodologie FIDES est applicable à l'ensemble des domaines utilisant de l'électronique : militaire, aéronautique, spatial, automobile, ferroviaire, télécommunications, informatique… Toutefois, certains composants tels les thermistances, les condensateurs à capacité variable, ou certains sous-ensembles, tels les écrans plasmas, en *italique* dans le guide, seront traités ultérieurement.	- Profil de vie, conditions d'environnement et d'emploi de l'équipement contenant le COTS, - Données sur : ➢ la définition de l'équipement, ➢ le cycle de vie de l'équipement, ➢ les fournisseurs des articles utilisés dans l'équipement.	- Taux de défaillance, - Bilan d'audit.

Avantages	Inconvénients
- La méthodologie FIDES prend en compte l'ensemble du profil de vie de l'équipement, y compris les situations de non-fonctionnement. Elle ne se limite pas aux seules défaillances des composants, mais intègre toutes celles propres au produit complet, - Contrairement aux normes en cours, elle évalue le processus « fiabilité » de l'équipement incluant le COTS et propose des recommandations sur l'ensemble de son cycle de vie.	- La qualité des évaluations dépend de celle des différents facteurs multiplicatifs. Ainsi, un soin particulier devra être porté lors de la réalisation des audits servant à la quantification des « Process ».

Bibliographie

Guide FIDES 1ière éd 2004
« Méthodologie de fiabilité pour les systèmes «électroniques » accessible à l'adresse Internet : fides@innovations.net

Estimations de fiabilité à partir d'essais ou du retour d'expérience

Objectif *(à quoi ça sert ?)*

Déterminer les paramètres de lois de fiabilité à partir de données traitées de retour d'expérience ou d'essais pour :

1. estimer la fiabilité opérationnelle afin de la comparer aux performances spécifiées au niveau système et/ou équipements,
2. mesurer l'évolution positive ou négative d'un niveau de fiabilité observé.

Description *(que produit la méthode et comment ?)*

La fiabilité R(t) d'un composant peut être exprimée selon différentes lois mathématiques selon la nature des défaillances et des phénomènes de dégradation. Les lois les plus couramment utilisées sont la loi exponentielle et la loi de Weibull. Ces lois peuvent être complètement définies par la détermination de leurs paramètres. La loi exponentielle est caractérisée par le taux de défaillance (λ) ou le temps moyen à première défaillance (MTTF). La loi de Weibull est caractérisée par le facteur de forme β, le paramètre d'échelle η, et le facteur de position γ.

Les relevés d'évènements observés sur des équipements en exploitation ou en essai (défaillance, survie, maintenance préventive, relevé de compteurs…) et leur datation permettent, par des méthodes graphiques ou numériques, d'estimer ces paramètres ainsi que les intervalles de confiance associés.

Conduite de la méthode *(comment la met-on en œuvre ?)*

L'estimation des paramètres de lois de fiabilité se base sur des données d'évènements observés sur des équipements réels. Après les étapes de recueil, de sélection et de tri des informations brutes, les tâches suivantes sont nécessaires à leur détermination:

1. tri des évènements chronologiquement selon la date d'apparition*,
2. approche non paramétrique de la loi de fiabilité -> tracé des points $Y_i = F(t_i)$ (selon méthodes des rangs médians, Kaplan-Meier…)*,
3. calcul ou évaluation graphique (papier Weibull par exemple) des estimateurs des lois choisies,
4. calcul des intervalles de confiance.

*Nota : Ces deux étapes sont facultatives pour la caractérisation du paramètre de la loi exponentielle ou par une approche de type maximum de vraisemblance.

Domaine de pertinence	Entrées	Sorties
- Cette estimation est pertinente lorsque le retour d'expérience est structuré et assure la fourniture de données cohérentes : ➢ modes de défaillance définis, ➢ conditions d'essais maîtrisées : vibration, température… ➢ similarité des profils d'utilisation, de mission, de vie… ➢ caractérisation des temps.	- Evènements en exploitation sur une période donnée (défaillances, relevés de compteurs, interventions de maintenance…), - Résultats d'essais de fiabilité censurés ou non censurés associés au facteur d'accélération dans le cas d'essais accélérés.	- Paramètres de fiabilité avec leurs intervalles de confiance avec par extension: ➢ lois de fiabilité, ➢ taux de défaillances, ➢ niveau de fiabilité observé, ➢ risque statistique en acceptation de produit ou de décision…

Avantages	Inconvénients
- Si les précautions sont prises, les données obtenues sont par définition les plus proches de la réalité, - Calculs simples pour la loi exponentielle, - Richesse des résultats (niveau de fiabilité, tendances, information sur les modes de défaillances…).	- Limites en cas de données peu nombreuses : évènements rares, systèmes mono-coup, - Calculs compliqués sur les estimations de paramètres de Weibull (nécessite un logiciel pour les intervalles de confiance), - La méthodologie de recueil des données doit être rigoureuse et homogène au cours du temps, cela peut donc nécessiter des moyens conséquents.

Bibliographie

1. Projet **SdF 2/96 :** Estimation de la fiabilité d'un produit (nouveau ou existant) à partir de retours d'expériences multiples et d'expertises.
2. **NF X 05-501** – Applications de la statistique. Introduction à la fiabilité.
3. **CEI/ISO-31010** – Gestion de la sureté de fonctionnement – Guide d'application.
4. **CEI/ISO-61124, ed2 :** Essai de fiabilité - Plan d'essai pour démonstration de taux de défaillance constant
5. J. Ringler – Précis de probabilité et de statistiques à l'usage de la fiabilité, Octares/ISdF.
6. A. Lannoy & H. Procaccia – Méthodes avancées d'analyses de données du retour d'expérience industriel, Eyrolles.

Fiabilité Prévisionnelle en Mécanique

Objectif *(à quoi ça sert ?)*

Les méthodes de fiabilité prévisionnelle ont pour objectif de produire des estimations a priori de la fiabilité de dispositif, appropriées aux mécanismes de défaillance susceptibles de les affecter. Ces estimations peuvent être utilisées en phase de conception pour démontrer que la fiabilité prévisionnelle est meilleure que la fiabilité allouée, ou en exploitation lorsque l'on souhaite par exemple améliorer la sureté d'une installation ou en étendre la durée de fonctionnement. Développées initialement pour les systèmes électroniques, ces méthodes ont été fondées à l'origine sur l'hypothèse que le taux de défaillance des composants est constant pendant leur période d'utilisation. Si cette hypothèse peut permettre de prendre en compte (avec précautions) des composants mécaniques simples, produits en grand nombre, susceptibles d'un mode de défaillance simple, elle n'est en général pas applicable aux systèmes à dominante « mécanique » pour lesquels les modes de défaillance (rupture, déformation, grippage, bruyance…) liés à la fatigue, à l'usure et au vieillissement apparaissent dès le début du cycle d'utilisation. L'objectif de la « Fiabilité en Mécanique » est donc de mettre à disposition des concepteurs un ensemble de méthodes d'estimation de la fiabilité prévisionnelle juste nécessaires, prenant en compte les mécanismes réels de défaillance et adaptées à chaque cas particulier.

Description *(que produit la méthode et comment ?)*

A l'issue des étapes « classiques » d'analyse prévisionnelle qualitative de la fiabilité (AMDEC, arbres de défaillances), trois approches de la fiabilité prévisionnelle de chaque composant sont proposées :

1. Il s'agit de composants traités dans des recueils de données de type « taux de défaillance constant » relatifs à des composants similaires, utilisés sur des systèmes similaires, dans des conditions et avec un profil d'utilisation et de maintenance similaires il est alors possible, sous réserves de vérifier la validité des hypothèses, d'utiliser des taux de défaillance (avec éventuellement intervalle de confiance associé). *(Voir en Annexe 1 une liste de bases de données disponibles).*
2. Il s'agit de composants « standardisés » sur lesquels les fabricants disposent de données suffisantes pour fournir « sur catalogue » des méthodes de calcul de la fiabilité prévisionnelle paramétrées selon les conditions d'utilisation (spectre de charge). Les données prennent implicitement en compte les conditions de maintenance préventive des composants de référence. Ces méthodes donnent directement l'évolution du taux de défaillance et de la fiabilité du composant en fonction du temps. Les principales lois de mortalité utilisées sont la loi log-normale et la loi de Weibull. Ce type d'approche est applicable en particulier à des composants comme les roulements, ressorts, engrenages, composants électromécaniques…
3. Le composant ne fait pas l'objet de standardisation, ou ses conditions d'utilisation sont spécifiques, il est alors préconisé d'appliquer des méthodes de type « contrainte-résistance » permettant de calculer la fiabilité prévisionnelle en prenant en compte les modèles d'endommagement adaptés à la physique des contraintes subies par le composant (usure, fatigue à grand nombre de cycles, fatigue oligocyclique…). L'application de ces méthodes permet alors d'enrichir les approches classiques du dimensionnement des composants mécaniques en quantifiant les risques liés à l'utilisation de « coefficients de sécurité » et en optimisant le dimensionnement en fonction des objectifs. *(Voir fiche pédagogique « Méthode Contrainte-Résistance »).*

Conduite du processus *(comment le met-on en œuvre ?)*

- Analyse fonctionnelle du système et établissement du bloc diagramme fonctionnel.
- Détermination des conditions d'utilisation (sollicitations dans chaque condition de fonctionnement),
- Analyse qualitative (Analyses préliminaires de risques, AMDEC, Arbres de défaillances…) et détermination des composants et défaillances critiques,
- Modélisation de la fiabilité du système (bloc diagramme de fiabilité),
- Pour chaque composant :
  - ➢ Recherche de données de retour d'expérience et d'expertise,
  - ➢ Choix de la méthode d'estimation de la fiabilité prévisionnelle la mieux adaptée (cf. ci-dessus) en fonction du type et de la criticité du composant,
  - ➢ Détermination des contraintes (mécaniques, thermiques…) et de leur distribution statistique et temporelle,
  - ➢ Recherche de données (et si besoin, définition et réalisation d'essais de fiabilité pour connaître les caractéristiques nécessaires à la conduite des calculs prévisionnels),
  - ➢ Calcul de la fiabilité du composant (utilisation des méthodes bayésiennes pour les composants innovants ou dont on a modifié le programme de maintenance préventive).
- Estimation de la fiabilité du système.

Domaine de pertinence

- Le domaine de pertinence de chaque approche de la fiabilité en mécanique est fortement dépendant :
  - ➢ de la robustesse du retour d'expérience sur lequel s'appuient les données d'entrée,
  - ➢ du contexte et des objectifs de l'étude.
- Du fait des limites des méthodes (voir « inconvénients » ci-après), une étude de fiabilité en mécanique n'a pas pour but de calculer la fiabilité d'un composant à la décimale près, mais plutôt d'effectuer dans le cas de systèmes sollicités dynamiquement une approche qui est beaucoup plus précise que l'utilisation de coefficients de sécurité, car elle tente de prendre en compte la plupart des facteurs.

Entrées

Niveau système :
- Profil de mission, distribution statistique des contraintes, en modes nominaux, dégradés, catastrophiques,
- Politique et conditions de maintenance,
- Objectifs FMDS,
- Exigences réglementaires,
- Spécifications techniques et fonctionnelles,
- Dossiers de plans et calculs.

Niveau composant :
- AMDEC composant, modèle de maintenance…
- Données issues du retour d'expérience dans des utilisations similaires (taux de défaillances, lois de mortalité…) ou de résultats d'essais,
- Modes et mécanismes physiques des défaillances (déformation, rupture par fatigue, usure, corrosion…),
- Caractéristiques de résistance aux contraintes avec distribution statistique associée.

Sorties

- Estimation du niveau de fiabilité du système,
- Connaissance des composants et modes de défaillances critiques et recommandations sur les choix de conception au niveau système (redondances…) et composant (matériaux, dimensionnement…),
- Connaissance des risques lés à l'utilisation des coefficients de sécurité,
- Optimisation du dimensionnement en fonction des objectifs FMDS,
- Détermination des essais de détermination des caractéristiques du matériau, de validation, de confirmations nécessaires,
- Préconisations de maintenance (données de base pour les démarches OMF–RCM).

Avantages

- Prise en compte des modes de défaillance propres aux composants mécaniques,
- Prise en compte de l'aspect aléatoire des contraintes et des résistances,
- Optimisation du dimensionnement (par opposition à coefficient de sécurité),
- Evaluation du risque sous la forme d'une probabilité, par opposition à la décision binaire liée à l'application d'un coefficient de sécurité,
- Possibilité de réaliser des études de sensibilité et d'aide à la décision.

Inconvénients

- La « fiabilité en mécanique » ne se réduit pas à « la loi de Weibull » ou à la « méthode contrainte résistance », le choix et la mise en œuvre des méthodes de prévision adaptées à chaque composant et à chaque contexte d'étude nécessitent une bonne connaissance des bases de la mécanique ET de la fiabilité,
- La « rigueur mathématique » des modèles et leur aptitude à « produire des décimales » ne doit pas faire oublier que la précision des estimations est dépendante :
  - ➢ de l'exhaustivité des analyses qualitatives (c'est bien souvent une cause ou une combinaison de causes « oubliée » qui conduira à la défaillance),
  - ➢ de la qualité des données d'entrée (connaissance toujours limitée de la répartition statistique réelle des contraintes et des résistances),
  - ➢ de l'écart entre le modèle et la réalité physique.
- A contrario, les tables de taux de défaillance doivent être utilisées avec beaucoup de précaution en étant conscient du fait qu'elles ne représentent en général qu'une première approximation.

Bibliographie

1. CAZAUX, POMEY, RABBE, JANSSEN – La fatigue des métaux – Ed. Dunod. 5ème édition – 1969
2. C. MARCOVICI et J. C. LIGERON – Utilisation des Techniques de Fiabilité en Mécanique – Ed. Lavoisier – 1974.
3. J. C. LIGERON – La Fiabilité en Mécanique – Ed. Desforges – 1979
4. Maitriser l'usure et le frottement – Ministère de l'industrie, Programme national d'innovation – 1980.
5. BARTHELEMY – Notions pratiques de mécanique de la rupture – Ed. Eyrolles – 1990
6. C. BATHIAS, J. P. BAILON – La Fatigue des Matériaux et des Structures – Ed. Hermès – 1997.
7. T. R. MOSS – The Reliability Data Handbook – Ed. Professional Engineering Publishing – 2005.
8. SHIGLEY – Mechanical Engineering Design – Ed. Mc Graw Hill, 8th edition – 2006
9. J. C. LIGERON – Cours de Fiabilité en Mécanique – Groupe de travail IMdR M2OS – 2009

Annexe 1 – Liste des bases de données mécanique		
Nom	**Origine/accessibilité**	**Dernière mise à jour**
FARADA	**FAilure RAte DAta Bank** Développé par le GIDEP (Government Industry Data Exchange Program) – US Rebaptisée « 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** Disponible auprès de IEEE(Institute of Electrical and Electronics Engineers).	1983
RADC TR 85-194	**RADC Non–Electronic Reliability Notebook** Disponible auprès du Rome Laboratory, ex Rome Air Development Center (RADC), laboratoire de l'US Air Force.	Rev. B – 1985
NPRD-95	**NPRD-95 Non–electronic Parts Reliability Data** Disponible auprès du RIAC et du SPIDR™ (Space Physics Interactive Data ressource) ex Alion System Reliability Center (SRC).	1995
EIReDA	**European Industry Reliability Data Handbook** Contribution de C.E.C.– J.R.C./ICEI 21020 ISPRA (Varese) Italy et EDF – DER/SPT 93206 Saint Denis (Paris) France.	Recueil : 1998 version informatique actualisée : 2000
T-Book	**Reliability data of components in nordic nuclear power plants**	6ième édition – 2005
OREDA	**Offshore REliability DAta** Financé et géré par les acteurs l'indusie pétrolière.	5ième édition – 2009

Nota: La liste ci-dessus n'est pas exhaustive. Certaines bases de données peuvent ne pas avoir été mises à jour.

Fiabilité en Mécanique – La méthode Contrainte – Résistance

Objectif *(à quoi ça sert ?)*

Évaluer la fiabilité d'une pièce mécanique soumise à des contraintes. Cette fiabilité s'exprime par la probabilité que, sur l'ensemble de la mission, la contrainte mécanique subie en tout point de la pièce reste inférieure à la résistance de la pièce.

Description *(que produit la méthode et comment ?)*

La méthode est fondée sur l'application des techniques de calcul de pièces mécaniques pour chaque type de contrainte subie :

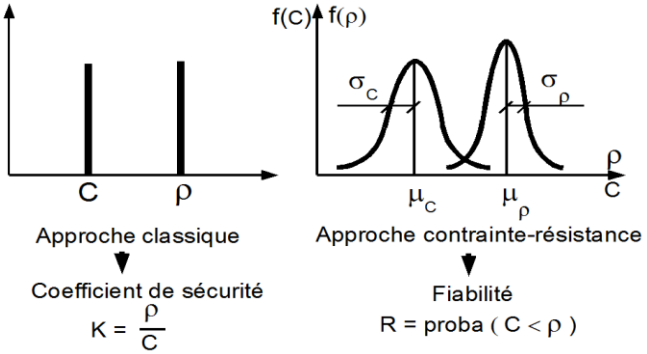
- contraintes statiques,
- fatigue à grand nombre de cycles,
- fatigue oligocyclique,
- usure…

Elle consiste à décrire de manière statistique:

- le cycle de contraintes appliquées, en y intégrant autant que possible les contraintes « exceptionnelles » (pics de contraintes) et les aléas prévisibles liés à la mission,
- les caractéristiques statistiques de résistance du matériau correspondant à chaque type de contrainte appliquée (résistance à la rupture, limite élastique, limite de fatigue, facteur K de fissuration…), en prenant en compte les aléas liés au matériau (hétérogénéités, vieillissement…), à la réalisation et au montage de la pièce (usinage, traitements thermiques, assemblage…), aux facteurs externes (température, humidité…).

La fiabilité de la pièce en chaque point s'exprime par la probabilité que, pour chaque mode de défaillance, la sollicitation appliquée (« contrainte » C) soit inférieure à la sollicitation admissible (« résistance »).

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



Dans le « cas d'école » où la contrainte C et la résistance ρ sont distribuées selon des lois normales de caractéristiques respectives (μ_C ; σ_C) et (μ_ρ ; σ_ρ), la variable $X = \rho - C$ suit une loi normale décrite de moyenne ($\mu_X = \mu_\rho - \mu_C$) et de variance ($\sigma^2_X = \sigma^2_\rho + \sigma^2_C$).

Au delà du coefficient de sécurité $k = \mu_c / \mu_\rho$, on peut alors calculer la fiabilité de la pièce: $R = \text{Prob}(X > 0)$.

Dans les autres cas (autres distributions), il est nécessaire de faire appel à des techniques statistiques plus élaborées pour comparer contrainte et résistance :

- algèbre des variables aléatoires,
- simulation de Monte Carlo,
- transformées de Mellin,
- méthodes d'approximation (FORM/SORM – First/Second Order Reliability Methods).

Conduite du processus *(comment le met-on en œuvre ?)*

- Détermination de l'enveloppe des profils d'utilisation de la pièce (cahier des charges, retour d'expérience…),
- Analyse des modes de défaillance de la pièce et des facteurs d'endommagement,
- Détermination des contraintes et de leurs caractéristiques statistiques dans les « zones critiques » (mesure, résistance des matériaux, modèles de fatigue des matériaux, théories du dommage, mécanique de la rupture, calculs par éléments finis…),
- Détermination des caractéristiques statistiques de résistance du matériau associées à chaque mode d'endommagement, (données matériaux « catalogue », retour d'expérience, résultats d'essais de détermination…),
- Comparaison de la contrainte et de la résistance dans chaque « zone critique »,
- Estimation de la fiabilité, comparaison aux objectifs et préconisations d'optimisation (dimensionnement, maintenance…).

Domaine de pertinence

- Connaissance requise :
  - des modes d'endommagement de la pièce,
  - de la distribution statistique des contraintes pour chaque mode d'endommagement,
  - de la distribution statistique des caractéristiques correspondantes de résistance du matériau.
- Même avec des données « de qualité » il faut être prudent sur l'exploitation de résultats obtenus pour de très faibles niveaux de probabilités de défaillance.

Entrées	Sorties
- Graphe de mission, - Dossier de calcul mécanique, - Données statistiques sur la résistance des matériaux, - Modèles d'endommagement selon le type de contraintes.	- Fiabilité des pièces, - Préconisations d'essais complémentaires, - Préconisations pour l'optimisation du dimensionnement, de la réalisation, de la maintenance…

Avantages	Inconvénients
- La méthode permet d'aller au-delà de l'application de coefficients de sécurité qui ne sont pertinents que dans des cas d'utilisation très spécifiques, et ne prennent pas en compte les incertitudes sur contrainte et résistance, - La méthode permet d'émettre des préconisations pour l'optimisation du dimensionnement, de la réalisation, de la maintenance.	- Il est parfois difficile de rassembler des données d'entrée robustes sur les facteurs endommageant, la distribution statistique des contraintes et des résistances, - Le calcul des contraintes (Résistance des Matériaux, éléments finis…) et de leurs limites peut faire appel à des modèles et des méthodes de calcul mécanique affaire de spécialistes, et en constante évolution, - L'estimation de la fiabilité peut faire appel à des méthodes statistiques « sophistiquées » et des moyens de calcul importants.

Bibliographie

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

Choix et application des méthodes d'analyse de la SdF du logiciel

Objectif *(à quoi ça sert ?)*

L'objectif est de construire la sûreté de fonctionnement [*1], d'analyser, de réduire et d'évaluer l'occurrence de bogues d'un logiciel et si possible le plus tôt dans le développement d'un nouveau logiciel. Pour ce faire, il est nécessaire d'avoir des activités appropriées, en fonction du stade d'avancement du projet de développement et de l'appliquer en conséquence.

Description *(que produit la méthode et comment ?)*

La construction de la sûreté de fonctionnement est un **processus itératif** qui doit être initié en phase de faisabilité, lors de la construction de la spécification du produit et dès que les données conceptuelles de celui-ci sont disponibles. Elle se poursuit et s'affine durant les étapes de **la phase de conception**, au fur et à mesure de l'avancement du processus de conception, de la connaissance de plus en plus précise des conditions de fonctionnement des composants, de l'acquisition éventuelle de résultats d'essais significatifs et se poursuit en phase de test, voire en opération.

Il existe cinq grands groupes d'activités qui s'appuient sur des méthodes et approches classées par ordre chronologique depuis la faisabilité jusqu'à la mise en œuvre du logiciel :

1. Activités en réponse à la réglementation (qualification des entreprises de développement, spécification du produit logiciel). Elles conduisent à spécifier des moyens, outils, méthodes d'analyse,
2. Activités basées sur des métriques du logiciel (ex. Méthodes de prévision de la fiabilité, RADC TR 85 228, Sofmat…),
3. Activités basées sur des Méthodes subjectives (Bayesienne),
4. Activités basées sur les tests,
5. Activités basées sur les Modèles de croissance de fiabilité, ex Goel-Okumoto, courbe en « S »…

Le tableau 1 en annexe présente une description succincte des différentes activités. Des fiches venant à la suite en détailleront certains points.

Conduite du processus *(comment le met-on en œuvre ?)*

Il n'y a pas une conduite mais des conduites qui s'appuient sur les facteurs suivants :

1. Est-on ou non dans un domaine où une réglementation s'impose ?,
2. Sélection, en début de projet de la / des méthodes la/les mieux adaptée(s) à la nature du produit et à la manière dont les objectifs sont spécifiés. Il est cependant possible de changer de méthode(s) en fonction de l'avancement du programme, lorsque les données de conception deviennent de plus en plus précises,
3. Détermination de la (ou les) classe(s) de bogues qui doivent être considérées de manière prioritaire dans l'évaluation de fiabilité, compte tenu des conséquences, afin de choisir la méthode d'évaluation la plus adéquate.
4. Evolution de la méthode, fonction de la phase du cycle de vie au cours de laquelle elle est mise en œuvre.

Domaine de pertinence

- Le domaine de pertinence est principalement fonction de la réglementation si elle s'applique, de la phase dans laquelle la méthode est mise en œuvre.
- Pour ce faire les méthodes se doivent d'être :
  1. Utiles et utilisables,
  2. Suffisamment précises pour être du niveau recherché,
  3. Applicables suffisamment tôt pour être efficaces,
  4. Discriminantes pour tenir compte :
     - De l'investissement tant humain que matériel,
     - De la qualité du processus de développement qui le met en œuvre,
     - De l'architecture tant logicielle que matérielle,
     - De la diversité des constituants (nouveaux développements ou composants sur étagères « COTS »),
     - Des conditions d'emploi,
     - D'un rapport **coût / efficacité fonction du risque encouru.**

Le tableau 2 en annexe indique les phases où chacune des activités est généralement applicable.

Entrées	Sorties
- Les spécifications / cahier des charges réglementaires lorsqu'elles sont requis, - L'organisation et les moyens tant du « spécificateur » que de celui qui réalise, - La spécification du logiciel, le dossier d'analyse, les plans d'organisation du projet et de développement, - Les règles de développement, les outils mis en œuvre, - Les résultats documentés de tests et la description circonstanciée des bogues rencontrés.	- La validation du respect des règles métiers s'appliquant au logiciel, - L'identification des risques de bogues les plus probables et leurs conséquences.

Avantages	Inconvénients	Bibliographie
Voir tableau 3	Voir tableau 3	Voir tableau 4

Tableau 1 : Description succincte des activités

Activités	Description des activités
Basée sur la réglementation, méthodes d'analyse	Selon les domaines d'application les logiciels doivent respecter des normes. C'est le cas dans les transports aériens, ferrés et routiers mais aussi dans le nucléaire, le militaire, le médical et bien d'autres domaines. Ces normes définissent la façon dont doit être spécifié, développé et testé le logiciel, le niveau de probabilité jugé acceptable des défauts spécifié par une classe de SIL selon les conséquences de leur activation et selon les spécificités de ces différents domaines. Tout comme pour le matériel des méthodes d'analyse existent comme par exemple les analyses des effets des erreurs du logiciel (A.E.E.L.). Celles-ci doivent s'effectuer avec discernement de façon à conserver une efficacité sans se noyer dans un niveau trop bas.
Basées sur des métriques du logiciel	Il existe de nombreuses métriques dans le domaine du logiciel. Parmi les plus anciennes et les plus connues figurent celle qui permet d'évaluer le nombre cyclomatique et celle basée sur le nombre d'instructions pour un « module » de code donné. D'autres méthodes sont beaucoup plus abouties et effectuent la synthèse d'un nombre important de métriques et modélisent le logiciel. Leur objectif est d'évaluer le nombre d'occurrences de bogues non tant pour eux-mêmes mais surtout de façon à comparer diverses solutions de développement afin d'orienter le concepteur vers des solutions minimisant leurs occurrences. La méthode SOFMAT est l'une d'elles.
Subjectives (Bayesienne)	Les méthodes subjectives permettent d'associer l'expérience des développeurs à des résultats de test insuffisants en terme statistique. Les statistiques Bayesiennes permettent de formaliser cette association. Elles s'utilisent aussi bien en logiciel qu'en matériel.
Basés sur les tests	Ici il s'agit de statistique pure. Tout comme dans le cas du matériel, le plus souvent ces méthodes permettent d'évaluer la fréquence d'occurrence des bogues. L'objectif est alors d'évaluer une caractéristique des tests comme par exemple le taux de couverture des tests. La principale difficulté réside alors dans l'appréciation du temps, de cycle, d'activation, calendaire.
Croissance de fiabilité	De nombreux modèles de croissance de fiabilité ont été développés. Les plus connus sont ceux de Jelinski-Moranda, Littlewood, Goel-Okumoto, Musa, en S… Ils permettent de décrire la croissance de la fiabilité du logiciel au cours de la validation du logiciel au fur et à mesure l'occurrence de bogues lorsque les fautes sont corrigées

Tableau 2 : Activités selon l'avancement du programme

Avancement du programme	Activités possibles				
	Réglementation Analyse	Métrique	Subjective	Test	Croissance
Concept fonctionnel (phase de faisabilité)	X	X			
Conception initiale (phase de conception)	X	X			
Conception finale (phases de définition et de développement)	X	X	X		
Essais (validation)	X	X	X	X	X
Opération	X		X	X	X

Tableau 3 : Avantages / inconvénients des activités

Activités	Inconvénients	Avantages
Basées sur la réglementation, méthodes d'analyse	- Standards souvent imprécis et qualitatifs, - Quel est le temps pris en compte, ce n'est pas leur objet? - Les normes excluent la connexion entre la fiabilité réelle et le niveau de SIL (Safety Integrity Level) demandé pour le logiciel, - Les méthodes d'analyse peuvent être parfois difficiles à appliquer, ex. durée en exploitation courte….	- A partir de l'allocation au logiciel d'un niveau de sécurité (SIL) requis, les méthodes et techniques à mettre en œuvre sont préconisées (voire imposées, réglementations).
Basées sur des métriques et modèles du logiciel	- Sont difficiles à valider (voir COMPSIS Project – NUREG).	- Permettent d'effectuer des comparaisons des difficultés de réalisation, des différentes architectures, de processus de développement, - Permettent de distinguer les fautes critiques, des fautes « légères » (ex : affichage dans certains cas), - Certaines méthodes de modélisation permettent des évaluations de dé fiabilité < 10^{-3}.
Subjectives (Bayesienne)	- Ne dispense pas de résultats de test avec leurs propres avantages et inconvénients.	- Permettent de tenir compte de données qualitatives (i.e. Qualité du développement…).
Basées sur les tests	- Considère le produit fini et non le processus de développement, - S'il n'y a pas de bogue ne démontre rien, - Si on corrige le bogue on peut recommencer, - Suppose que les tests sont vraiment représentatifs de l'opération.	- Fait partie du processus d'acceptation, - Fourni des renseignements sur la qualité des tests - On peut choisir le nombre et la distribution des données de test.
Croissance de fiabilité	- Il faut d'assez grands systèmes pour avoir un nombre suffisant de bogues, mais est-ce bien « raisonnable » pour un produit en opération… - Avec les systèmes propriétaires comme les OS, il devient difficile de respecter la chronologie, - Distingue difficilement les fautes critiques des fautes « cosmétiques » car le patrimoine statistique est faible par essence, - Ne permettent de démontrer que des dé fiabilités importantes, au mieux de 10^{-3}<<10^{-4}.	

Tableau 4 : Bibliographie (ordre chronologique)

Bibliographie
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 Maintenability 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

SdF du logiciel: Les normes

Objectif *(à quoi ça sert ?)*

L'objectif n'est pas seulement de construire la sûreté de fonctionnement[*1] mais de répondre à des exigences réglementaires à respecter pour obtenir l'autorisation de mise en œuvre, en service, d'un système, produit contenant une part essentielle de logiciel. C'est la démonstration que celui ci répond à la norme applicable qui conditionne, entre autre, cette autorisation.

Description *(que produit la méthode et comment ?)*

Nous distinguerons deux catégories de normes :

{1} Celles qui concernent la capacité d'une entreprise à développer un système d'un niveau donné.
L'entreprise peut, si elle le souhaite, se faire « qualifier » à un niveau donné et ainsi justifier d'une organisation, une capacité industrielle, un savoir faire pour prétendre à une certaine crédibilité lors notamment d'appels d'offre. Cette « qualité » n'aura pas de conséquences sur la seule SdF des produits mais sur l'ensemble de leurs performances.
Dans cette catégorie figurent principalement « CMMI » (Capability Maturity Model Integrated) et « SPICE » (Software Process Improvement Capability dEtermination). Ce ne sont pas à proprement parler des normes mais des guides ou modèles.
CMMI comporte 5 niveaux de maturité divisés en secteurs clés indiqués à titre d'exemple :

1. Initial, ne contient pas de secteur,
2. Reproductible, planification de projet, assurance qualité,
3. Défini, définition des processus, ingénierie des produits logiciels,
4. Maîtrisé, gestion quantitative des processus et de la qualité logicielle,
5. Optimisé, gestion des changements technologiques et des changements de processus.

Ces niveaux constituent les étapes sur le chemin menant à des processus matures, conformes à un ensemble de bonnes pratiques observées à travers le monde dans des entreprises réputées pour bien gérer leurs processus. La conformité à CMMI est notamment requise pour contracter avec le département américain de la défense.

{2} Celles qui constituent un des points des exigences du cahier des charges.
Une norme en la matière traduit et définit le savoir faire de la communauté des développeurs dans un domaine d'application pour respecter notamment des objectifs de sécurité.
La norme est soit tous domaines, soit spécifique à domaine particulier (Aéronautique, Ferroviaire, Automobile…).

Conduite du processus *(comment le met-on en œuvre ?)*

Les deux catégories définies ci avant conduisent à deux conduites de processus bien différents.

{1} La première ne se rattache pas à un projet en particulier. Elle s'inscrit dans la vie de l'entreprise pour en définir, à ses frais, la crédibilité à partir de la date de reconnaissance par un organisme d'accréditation, pour s'éteindre à la date de cession d'activité de l'entreprise, si elle arrive. A un intervalle spécifié par la norme un renouvellement de l'accréditation doit être effectué par l'organisme la délivrant pour en maintenir la pérennité.

{2} La seconde à l'inverse s'attache à un projet particulier dès la phase de faisabilité si l'on est donneur d'ordre, et, se termine lors du retrait de service du produit chez l'exploitant.

Domaine de pertinence

{1} Les normes de qualification d'entreprises s'adressent **plus particulièrement** aux entreprises qui visent de grands contrats auprès d'organismes publics ou privés ou qui souhaitent se démarquer par rapport à la concurrence.

{2} Les normes requises au cahier des charges concernent principalement la sécurité dans les domaines :

1. De l'aéronautique,
2. Du ferroviaire,
3. De l'automobile,
4. ….

Entrées	Sorties
- **{1}** Les procédures mises en œuvre aux différents niveaux et départements de l'entreprise. - **{2}** L'organisation et les moyens tant du spécificateur que de celui qui réalise.	- **{1}** La certification de l'entreprise à un niveau donné. - **{2}** Le dossier destiné à l'organisme chargé de l'autorisation de mise en service. - La spécification du logiciel, le dossier d'analyse, les plans d'organisations projet et de développement, - Les règles de développement, les outils mis en œuvre, - Les résultats documentés de tests et la description circonstanciée des bogues rencontrés.

Avantages	Inconvénients
- **{1}** Permettent de justifier d'un savoir faire, - CMMI constitue un standard de fait. - **{2}** Constituent un référentiel en vue d'autoriser la mise en service.	- **{1}** N'offre aucune garantie pour un projet défini, car si l'entreprise saurait faire, pour un projet déterminé, elle peut réduire, par exemple, ses coûts de production et n'effectuer que partiellement ce qu'elle sait faire, - CMMI se voit parfois reproché un manque de fondement théorique, car fondé sur « *de bonnes pratiques* ». - **{2}** Peuvent dans certains cas empêcher la mise en œuvre de certaines solutions (nouvelles technologies…) non prises en compte dans la norme.

Bibliographie

{1} Capability Maturity Model® Integration (CMMI), SEI(Software Engineering Institute) de l'université Carnegie Mellon.
{2} EN 61-508 : "Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité (E/E/PES)"- 2011.
Normes dérivées :

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

Eurocae **DO-178C/ED-12B**, « Software Considerations in Airborne Systems and Equipment Certification – 11-2011

SdF du logiciel: les moyens, outils et analyses

Objectif *(à quoi ça sert ?)*

L'objectif est de construire la SdF par le choix de moyens, outils et analyses propres à assurer le niveau de SdF souhaité, aux différentes étapes du cycle de vie.

Description *(que produit la méthode et comment ?)*

Ceci conduit à définir :

- La mise en place de l'organisation :
  - La formation des équipes aux techniques, standards requis,
  - Les moyens et l'organisation des équipes tant en personnels, qu'outils pour l'adaptation des ressources aux charges de développement afin de respecter à la fois les délais mais aussi les coûts,
  - Les équipes de test et leurs moyens, leur indépendance ou non vis-à-vis de celles de développement,
  - Les capacités de retour d'expérience pour tracer les défauts identifiés et y remédier.
- Les outils :
  - Outils de spécification,
  - Ateliers de développement,
  - Ateliers de tests.
- Les analyses :
  - En mettant en œuvre :
    - Des méthodes inductives et / ou déductives permettant de définir les conséquences de l'apparition de défauts (AEEL, ADD, Arbre d'évènement,…),
    - Des méthodes basées sur les métriques (ex : prévision de fiabilité) pour en connaître :
      - Les éléments / défauts les plus significatifs et / ou fréquents,
      - Identifier les moyens d'en réduire les conséquences et ou l'occurrence quand nécessaire.
  - Pour identifier les défauts :
    - Leur(s) cause(s),
    - Leur nature,
    - Les conditions d'apparition.
    - Les plus significatifs et / ou fréquents,
    - Leurs conséquences et ou l'occurrence,
  - Pour vérifier la mise en œuvre des règles de développement, de codage par exemple,
  - En vue de :
    - Classer les dysfonctionnements méritant une reprise de conception,
    - Identifier les moyens de réduire ces dysfonctionnements (redondances, barrières de sécurité,…),
    - Evaluer les impacts et conséquences après mise en œuvre des corrections.

Conduite du processus *(comment le met-on en œuvre ?)*

La mise en œuvre est continue tout au long du cycle de vie et doit s'adapter aux charges inhérentes à chacune des phases du projet.
Les méthodes inductives et déductives, d'évaluation, de vérification, sont mises en œuvre de façon itérative au cours de la vie du produit tout en étant mise en œuvre le plus tôt possible pour éviter de coûteux redéveloppement lorsqu'un risque non identifié précédemment est révélé.

Domaine de pertinence	Entrées	Sorties
Tous domaines où les conséquences de l'activation d'un défaut peut entrainer des conséquences importantes / graves sur la disponibilité voire la sécurité liée au produit	Moyens financiers, compétences.	• Des produits conformes au cahier des charges, dans les délais et coûts prévus. • Les défauts critiques du projet, leur identification, leur conséquence, leur occurrence.

Avantages	Inconvénients
• Taux de réussite élevé des projets. • Permet d'identifier les risques de dysfonctionnement, • Hiérarchise les efforts pour remédier aux conséquences.	• Dépend beaucoup de l'expérience des manageurs dans le domaine concerné. • Est largement fonction du degré d'innovation du projet tant en terme de fonctionnalités, de technologie. • Peuvent s'avérer dispendieuses si elles ne sont pas réalisées au bon niveau. • Ne sont pas une garantie d'exhaustivité. • Les évaluations quantitatives sont peu connues et peu reconnues.

Bibliographie

- 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: *What Every Engineer Should Know About Risk Engineering and Management.* London: CRC Press.

La démarche bayésienne en fiabilité

Objectif *(à quoi ça sert ?)*

Améliorer, par l'intégration de connaissances préalables, la précision de l'estimation d'une caractéristique de fiabilité d'un produit lorsque les données de retour d'expérience sont insuffisantes ou biaisées par des modifications de conception, d'exploitation ou de maintenance.
Réduire le volume des essais de fiabilité.

Description *(que produit la méthode et comment ?)*

- La démarche statistique traditionnelle dite « fréquentielle » consiste à estimer les paramètres inconnus des lois de probabilité auxquelles obéissent certains évènements considérés comme aléatoires (ex : nombre de défaillances observés sur un parc de matériel donné) à partir des seules données empiriques.
- A l'inverse, la démarche bayésienne s'appuie à la fois sur ces données empiriques ainsi que sur un a priori basé, selon les cas, sur des données antérieures observées dans un contexte différent du contexte actuel, ou sur le propre jugement « a priori » de l'analyste, ou encore sur des jugements d'experts. Dans cette approche, les paramètres inconnus sont assimilés à des variables aléatoires et les connaissances préalables sont traduites par une distribution de probabilité dite « distribution a priori ». Les données objectives sont ensuite fusionnées avec la « distribution a priori » à l'aide d'une transformation mathématique basée sur le théorème de Bayes qui se traduit par une nouvelle distribution statistique dite «distribution a posteriori ». Celle-ci permet de faire une nouvelle estimation du paramètre à estimer qui reflète à la fois les connaissances a priori et les données objectives. Dans le domaine de la fiabilité, cette estimation se fait le plus souvent sur des taux de défaillance constants et sur des probabilités de bon fonctionnement de mécanismes « mono coup ».
- A l'instar d'autres domaines d'application, la démarche bayésienne en fiabilité est d'autant plus efficace, par rapport à la démarche « fréquentielle », que les données empiriques sont peu nombreuses ou qu'elles sont « polluées » par des modifications de conception ou d'exploitation des matériels suivis, sous réserve que le modèle « a priori » soit pertinent. Outre l'estimation des paramètres inconnus, la démarche bayésienne s'applique aussi, dans le domaine de la fiabilité, à l'élaboration de plans d'essais dits « bayésiens » de validation de la fiabilité ou de contrôle de la fiabilité en production.

Conduite de la méthode

La démarche bayésienne fait appel à des traitements analytiques simples dès lors que la distribution de probabilité « a posteriori » du paramètre à estimer garde une forme stable (i.e. même famille que la distribution « a priori ») après intégration des données empiriques observées. Dans le domaine de la fiabilité, les deux cas suivants satisfont à cette condition :

- Cas de la probabilité de bon fonctionnement des systèmes mono coup : on a affaire à un scénario d'événements bernoulliens à 2 états « le système fonctionne » et « le système ne fonctionne pas ». L'estimation porte dans ce cas sur la probabilité « p » de bon fonctionnement du système. Pour assurer la stabilité de la distribution « a posteriori » de « p », il convient d'adopter pour distribution « a priori » une loi type beta à 2 paramètres (fonction eulérienne de 1ère espèce).
- Cas de la durée de vie d'un système à loi de mortalité exponentielle : dans ce cas, le taux de défaillance « λ » du système est réputé constant et l'estimation porte sur ce paramètre. Pour assurer la stabilité de la distribution « a posteriori » de « λ », il convient d'adopter pour distribution « a priori » de « λ » une loi gamma à 2 paramètres (fonction eulérienne de 2ème espèce).

Dans un cas comme dans l'autre, le bon choix des paramètres de la distribution « a priori » est crucial car il va influer sur la forme de la distribution « a posteriori », et donc sur l'estimation « a posteriori » du paramètre suivi. Pour déterminer les paramètres de la distribution « a priori », deux catégories d'approche peuvent être envisagées selon le contexte :

- Méthode des coefficients de ressemblance : elle est recommandée lorsque l'on dispose au départ de données expérimentales sur des systèmes voisins ou similaires mais ayant été exploités de manière différente. Elle consiste à définir puis à chiffrer des « coefficients de ressemblance » entre le système actuel et le(s) système(s) antérieur(s) pris en référence dans l'a priori. Ces coefficients doivent porter sur des critères techniques considérés comme ayant un impact significatif sur la fiabilité du système. Ils se traduisent alors en terme d'équivalence de données virtuelles « a priori ») qui permettent de régler les paramètres de la distribution « a priori » de la caractéristique de fiabilité.
- Jugement d'experts : il est fait appel au jugement professionnel d'experts qui connaissent bien les caractéristiques du système ainsi que sur le comportement de systèmes similaires. Ce jugement est pris en compte via un questionnaire oral ou écrit. Les réponses collectées sont exploitées et pondérées par l'analyste qui, à l'instar de la méthode des coefficients de vraisemblance, va se traduire en termes de données virtuelles « a priori ».

Dans tous les cas de figure, les paramètres de la loi « a priori » se traduisent par un centrage de la loi autour d'une valeur considérée comme la plus probable et une dispersion d'autant plus élevée que les données « a priori » sont incertaines. Une fois fusionnées avec une première série de données objectives , le traitement analytique conduit à une distribution « a posteriori » dont la dispersion est plus petite que celle de la distribution initiale si les valeurs « a priori » sont réalistes (dans le cas inverse, mieux vaut ne plus passer par les données « a priori » et revenir à l'approche fréquentielle traditionnelle). Une estimation « a posteriori » du paramètre à estimer peut être établie, soit de manière ponctuelle en adoptant par exemple l'espérance mathématique de la distribution, soit par « intervalle de crédibilité » reflétant la plus ou moins grande dispersion de cette distribution. Si l'on dispose, dans un second temps, d'une nouvelle série de données objectives, on réitère ce processus en adoptant pour nouvelle distribution « a priori » la distribution « a posteriori » précédente.

Lorsque les modèles utilisés ne permettent pas d'assurer la stabilité des distributions « a posteriori », la méthode analytique n'est plus possible et l'usage de l'ordinateur s'avère nécessaire. C'est le cas fréquent des systèmes complexes dont les défaillances peuvent être à la fois de nature aléatoires et dues à l'usure.

Dans le domaine du contrôle par échantillonnage de la fiabilité de matériels en production, il existe des plans types d'essais « bayésiens » applicables au cas des matériels mono-coups ou des matériels à taux de défaillance constants. L'usage de ces plans, par comparaison aux plans « classiques », présente l'avantage de réduire le volume des essais à effectuer, en termes de taille d'échantillon et /ou de durées d'essais.

Domaine de pertinence
- Peu de données objectives disponibles sur un nouveau matériel, - Volume significatif de données objectives sur des matériels voisins ou ayant fonctionné dans des conditions d'emploi différentes, - Fortes connaissances d'experts sur le fonctionnement attendu du nouveau matériel ou de matériels similaires.

Entrées	Sorties
- Données a priori (connaissance d'experts, résultats de données biaisées), - Loi de fiabilité du matériel suivi, - Données de retour d'expérience sur le matériel étudié.	- Distribution « a posteriori » de la caractéristique de fiabilité, - Estimation « a posteriori » de la caractéristique de fiabilité (ponctuelle et par intervalle de crédibilité).

Avantages	Inconvénients
- Estimation possible de caractéristiques de fiabilité avec peu de données - Resserrement des intervalles de confiance - Permet d'utiliser les connaissances a priori	- Nécessite un traitement lourd lorsque les lois de fiabilité traitées n'ont pas de conjuguées bayésiennes. - Peut induire un biais significatif sur l'estimation lorsque le jugement a priori n'est pas bon.

Bibliographie

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

Analyse préliminaire des risques (A.P.R.)

Objectif *(à quoi ça sert ?)*

Identifier et estimer / hiérarchiser, dès la phase de définition, les risques courus par un système ou une installation au cours de son profil de vie et définir les mesures à prendre pour les réduire ou supprimer. Les causes de dangers sont associées à la fois aux dysfonctionnements internes du système ou de l'installation, à l'environnement du profil de vie, aux éléments constituant le système, aux scénarios d'emploi et aux erreurs humaines

Description *(que produit la méthode et comment ?)*

L'analyse préliminaire des risques (APR) consiste, dans un premier temps, à recenser les dangers potentiels associés au système étudié. La démarche typique de l'APR consiste à exploiter des listes de risques, fondées essentiellement sur l'expérience, associés aux éléments constitutifs du système et de leurs combinaisons. Ces listes, obligent à s'interroger sur l'existence des dangers connus liés à chaque élément dans chaque phase du profil de vie du système dans ses environnements, aux possibilités de se manifester, aux conséquences prévisibles et aux moyens connus de maîtriser les risques associés. Cette phase initiale peut aussi, dans certains cas, mettre en œuvre des méthodes comme AMDEC, HAZOP, arbres de défaillance, etc. qui sont plus typiques des analyses de risques détaillées.

Dans un deuxième temps, accompagnant l'avancement de la conception, l'APR doit :

- établir et décrire des scénarios d'accident, (ceux qui vont nécessiter des études plus approfondies)
- évaluer des ordres de grandeurs des risques,
- d'identifier des mesures de maîtrise des risques et leur pertinence.

A ce stade l'APR fournit au projet une caractérisation des tâches de sûreté de fonctionnement à accomplir et les éléments pour les organiser.
L'APR se fond alors dans l'ensemble des analyses de risques (systèmes, sous-systèmes, processus, etc.) de l'identification, l'évaluation, la confrontation aux critères d'acceptation jusqu'aux actions de maîtrise des risques tout en constituant une colonne vertébrale et un agenda (à mettre à jour au fur et à mesure de l'avancement du projet) des tâches de SdF.

Conduite de la méthode *(comment la met-on en œuvre ?)*

L'APR est une démarche itérative initiée dès le début de la phase de définition pour pouvoir orienter très tôt les critères de conception. A ce stade, les résultats sont encore incomplets ou imprécis. Elle doit donc être actualisée et affinée au cours de la phase de développement, au fur et à mesure de l'avancement des processus de conception du système et de réduction des risques.

La réalisation de l'APR fait l'objet d'un travail de groupe où chaque membre apporte son expérience sur l'identification des risques potentiels. Ce travail est facilité par l'utilisation de **listes-guides** d'entités dangereuses et de situations dangereuses élaborées pour un domaine précis, ainsi que par l'analyse fonctionnelle réalisée en amont. Il importe, dans un projet innovant pour l'entité qui le conduit, d'associer à ce stade toutes les informations ou compétences possibles externes à l'entité.

La conduite de la méthode consiste à:

- exploiter toutes les connaissances disponibles sur le système (fonctions requises, environnement du profil de vie, composition : matières, énergies, structures, etc.),
- passer en revue ce qui pourrait induire une conséquence indésirable, à la lumière de l'expérience existante (interne ou externe à l'organisation), relative à chacun des constituants du système,
- écarter (en en gardant mémoire) les risques « irréaliste » ou sans importance,
- enrichir l'analyse, pour chacun des risques retenus, jusqu'à identifier ce qui doit être traité et comment le traiter,
- consulter et mettre à jour l'analyse au fur et à mesure de l'avancement du projet et de la vie du système,
- constituer le registre des dangers, le suivi et le bouclage des actions en réduction de risque, la base pour des audits,…

Le tableau de la page suivante illustre une façon courante de présenter les résultats d'une APR. Il est surtout approprié pour un projet technologique conçu de zéro. D'autres présentations peuvent être plus adaptées à un projet de changement dans un système d'exploitation.

Domaine de pertinence

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.

Entrées

- 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

Sorties

Rapport d'APR incluant :

- les tableaux d'analyse,
- des conclusions / recommandations,
- la cartographie des risques,
- le plan de veille, d'audits, de suivi, le registre des dangers.

Avantages

Amélioration de la cohérence de la démarche de maîtrise des risques des différentes phases de la vie du système en posant des fondations aussi larges et complètes que possible.

Inconvénients

Le caractère exhaustif de la démarche dépend beaucoup de l'expérience sur des événements semblables et du soin apporté à l'étude.

Bibliographie

- 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

TABLEAU TYPIQUE DE L'APR

Les résultats d'une APR se présentent en général dans un tableau à 11 ou 12 colonnes qui rappelle celui de l'AMDE(C) :

(1) Système ou fonction,	(2) Phase	(3) Entités dangereuses	(4) Evènements causant une situation dangereuse	(5) Situation dangereuse	(6) Evènement causant un accident potentiel	(7) Accident potentiel	(8) Effets ou conséquences	(9) Classification par gravité	(10) Mesures préventives	(11) Application de ces mesures

Les 11 colonnes du tableau peuvent être explicitées comme suit :

1. Système ou fonction : identification de l'ensemble étudié,
2. Phase : identification des phases ou des modes d'utilisation du système ou de la fonction pendant lesquels certaines entités peuvent générer un danger,
3. Entités dangereuses : identification des entités du système ou de la fonction auxquelles on peut associer un danger intrinsèque,
4. Evénements causant une situation dangereuse : identification des conditions, événements indésirables, pannes ou erreurs qui peuvent transformer une entité dangereuse en situation dangereuse,
5. Situation dangereuse : identification des situations résultant de l'interaction d'une entité dangereuse et de l'ensemble du système à la suite d'un événement décrit précédemment.
6. Evénement causant un accident potentiel : identification des conditions, événements indésirables, pannes ou erreurs qui peuvent transformer une situation dangereuse en accident,
7. Accident potentiel : identification des possibilités d'accidents résultant des situations dangereuses à la suite d'un événement décrit précédemment,
8. Effets ou conséquences : identification des effets ou conséquences des accidents potentiels, lorsqu'ils se produisent, estimation des probabilités d'occurrence effective des accidents,
9. Classification par gravité : appréciation de la gravité des effets ou conséquences suivant une classification du type « mineure », « significative », « critique », « catastrophique »,
10. Mesures préventives : recensement des mesures proposées pour éliminer ou maîtriser les risques ainsi identifiés (situations dangereuses ou accidents potentiels),
11. Application de ces mesures: recueil d'informations relatives aux mesures préventives proposées (ex : est-ce que ces mesures ont été incorporées dans le système ? Se sont-elles révélées efficaces ? etc.).

Notes :

- une 12ème colonne dédiée à l'estimation des probabilités d'occurrence des accidents peut être ajoutée.
- l'APR peut être étendue à une étude de scenarios d'accidents en adjoignant des colonnes criticité et rapport coût /risque

Analyse des Modes de Défaillance et de leurs Effets (A.M.D.E.)

Termes liés : A.M.D.E.C.: Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
F.M.E.A.:Failure Modes and Effects Analysis
F.M.E.C.A.: Failure Modes, Effects and Criticality Analysis

Objectif *(à quoi ça sert ?)*

L'AMDEC est une méthode d'analyse inductive et rigoureuse ayant pour buts d'identifier les défaillances dont les conséquences peuvent affecter le fonctionnement d'un système, de les hiérarchiser selon leur niveau de criticité afin de les maîtriser.

Description *(que produit la méthode et comment ?)*

Dans un premier temps, la méthode vise donc à recenser les faiblesses potentielles d'un système (produit en conception, processus de fabrication, moyen de production…) en recherchant, pour chaque composant du système, les modes vraisemblables de défaillance, les causes possibles, les effets sur le fonctionnement du système, selon la phase de mission et du cycle de vie.
Chaque défaillance est ensuite évaluée en terme de criticité au regard de l'objectif fixé de sûreté de fonctionnement. Deux ou trois critères sont exploités: l'occurrence (fréquence ou probabilité d'apparition) du mode de défaillance, la gravité des effets, la probabilité de détection de la défaillance.
Des grilles (barèmes) de cotation sont utilisées pour réaliser cette évaluation. La criticité résultante est souvent obtenue par le produit des notes obtenues pour chaque critère. Elle permet de hiérarchiser les risques de défaillance et de définir les points critiques éventuels.
Enfin, pour les défaillances jugées critiques ou inacceptables, des actions préventives et/ou correctives sont recherchées dans le but de réduire la criticité. Elles peuvent concerner toutes les étapes du cycle de vie du système.

Conduite de la méthode *(comment la met-on en œuvre ?)*

L'AMDEC offre une méthodologie simple et systématique d'analyse des risques de défaillance.
Elle nécessite une étape d'analyse fonctionnelle préliminaire du système. Elle permet de décrire la mission du système à analyser, ses modes de fonctionnement nominaux, les diverses fonctions de service qu'il doit assurer, enfin ses fonctions techniques.
L'AMDEC se pratique en groupe de travail. Les participants sont choisis en fonction de leur connaissance du système ou de systèmes analogues. La présence d'un animateur est indispensable. Le groupe s'appuie sur les informations disponibles au moment de l'étude : plans, documentations, historiques des pannes déjà rencontrées sur des systèmes équivalents…

A la suite de l'analyse, une synthèse des résultats (sous la forme de listes de pannes, de symptômes) doit être réalisée par le pilote et/ou l'animateur. En particulier, un plan d'actions est décidé avec désignation des responsables et fixation des délais à respecter.
Une fois les actions mises en œuvre, des remises à jour de l'analyse doivent être effectuées après validation des résultats obtenus.

Domaine de pertinence
- L'AMDEC est d'un usage très large et concerne tous les secteurs d'activité, - L'AMDEC est essentiellement destinée aux systèmes matériels : mécanique, hydraulique, électrique, électronique… Dans le cas des logiciels, on utilise un équivalent appelé A.E.E.L.

Entrées	Sorties
- Dossier de conception du nouveau système, - Historique des pannes du système existant, - Description fonctionnelle et structurelle du système, issue de l'analyse fonctionnelle, - Connaissance de l'environnement du système, de ses conditions d'utilisation, - APR, HAZOP.	- Identification des dysfonctionnements potentiels et de leur criticité, - Plan d'actions préventives ou correctives, d'amélioration.

Avantages	Inconvénients
- L'AMDEC est une méthode relativement simple et facilement accessible, - C'est un outil très puissant, au domaine d'application très large, qui peut être mis en œuvre aussi bien en conception qu'en exploitation, - En tant que méthode inductive, elle offre une analyse systématique et un maximum de garantie d'exhaustivité, - Enfin, le tableau d'analyse assure une bonne traçabilité des réflexions et une aide à la décision pour les actions d'amélioration à entreprendre.	- La méthode souffre d'une certaine lourdeur en volume et temps passé, - Il est difficile de prendre en compte les phénomènes combinatoires ou dynamiques, les pannes multiples. Dans ce cas on peut utiliser d'autres méthodes mieux adaptées (Arbre de défaillance), - L'AMDEC ne prend pas en compte les défaillances dites de « mode commun », - L'AMDEC est mieux adaptée aux systèmes mécaniques et analogiques qu'aux systèmes numériques, - On ne dispose pas à l'heure actuelle de banque de données de défaillances d'organes, causes, effets…

Bibliographie

1. **MIL STD-1629-A** : "Procedures for performing a failure modes and effects analysis", notice 1 – 1983,
2. **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.) ",
3. **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,
4. CETIM, "Guide de l'AMDEC machine" – 1994,
5. ISdF, condensé pédagogique n° 4, " AMDEC ".

Graphe d'état

Objectif *(à quoi ça sert ?)*

Evaluer les principales caractéristiques de sûreté de fonctionnement[*1] d'un système réparable.

Description *(que produit la méthode et comment ?)*

Les états possibles d'un système (état nominal, état de fonctionnement dégradé, état de panne totale…) sont modélisés à l'aide de cercles reliés entre eux par des flèches indiquant les transitions possibles entre ces états. Ces transitions sont conditionnées, selon les cas, par des processus de défaillance ou par des remises en état des entités en panne dont l'intensité (taux de défaillance ou taux de réparation) est indiquée. Mathématiquement, le diagramme d'état donne lieu à un système d'équations différentielles qualifié de "markovien" lorsque les taux de transition sont constants. La résolution de ce système différentiel permet de calculer les probabilités associées aux différents états identifiés et les principales caractéristiques de SdF du système.

Conduite de la méthode *(comment la met-on en œuvre ?)*

L'analyse des caractéristiques de SdF par graphe d'état passe par 4 étapes principales :

1. Recensement et classement de tous les états fonctionnels possibles du système (nominal, dégradés, en panne). Si chaque élément du système peut être caractérisé par 2 états possibles (fonctionnement ou en panne), le nombre maximum d'états est 2^n.
2. Recensement et identification de toutes les transitions possibles entre les différents états identifiés du système. Ces transitions sont conditionnées par des processus de défaillance ou par des remises en service (après réparation) d'éléments en panne.
3. Réalisation d'un graphe d'état, constitué de cercles et de flèches reliant ces cercles, ayant pour objet de schématiser tous les états du système identifiés à l'étape 2 ainsi que les liaisons (et les intensités associées) entre ces états.
4. Etablissement et résolution du système d'équations différentielles linéaires associé au graphe d'état. Cette résolution conduit à l'obtention, selon les cas, de la disponibilité instantanée (fonction du temps), de la disponibilité asymptotique (en régime établi), ou des principales caractéristiques de SdF telles que : le MTTF, la MTBF, le MTTR, la fréquence moyenne de pannes du système…

Domaine de pertinence

- Optimisation sous l'angle coût/disponibilité de l'architecture de systèmes réparables à taux de défaillance et taux de réparation constants dont les états ne sont pas influencés par des événements extérieurs se produisant à des instants prédéterminés.

Entrées	Sorties
- Etats du système, - Taux de transition, - Objectifs SdF.	- Disponibilité (instantanée et/ou asymptotique), - Caractéristiques SdF : MTTF, MTBF, MTTR, fréquence de panne…

Avantages	Inconvénients
- Intérêt de la visualisation graphique, - Traitement possible de systèmes à éléments dépendants (ex : redondance passive), - Prise en compte possible de lois non exponentielles dans les durées de réparation (méthode des états fictifs).	- Limité aux dispositifs sans usure, - Impossibilité de prendre en compte des événements déterministes dont la date est fixée de l'extérieur, - Croissance exponentielle du nombre d'états du graphe avec le nombre d'éléments du système, - L'usage d'un programme informatique spécialisé est nécessaire dès que le nombre d'états devient important.

Bibliographie

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

NE CONFONDONS PAS !

Ces méthodes qu'on peut croire semblables ou variantes d'une même démarche n'ont, en fait, pas grand' chose en commun. L'arbre de défaillances (Fault Tree Analysis) et l'arbre d'événement (Event Tree) sont des **démarches d'analyse prévisionnelle** alors que l'arbre des causes est **une description a posteriori** d'un accident.

L'arbre des défaillances se construit de la conséquence vers les causes, c'est-à-dire l'ensemble des combinaisons de défaillances, et éventuellement de circonstances, capables de provoquer l'événement redouté étudié.

L'arbre d'événement se construit, à l'inverse, de la cause – l'événement – vers les conséquences possibles en prenant en compte toutes les alternatives qui peuvent modifier ces conséquences.

L'arbre des causes part de l'accident qui s'est produit et décrit les enchaînements de causes (défaillances, circonstances, actions, fonctionnements normaux…) qui se sont combinés ce jour-là pour créer l'accident ; c'est une méthode particulièrement utilisée dans l'analyse des accidents du travail.

La confusion entre les termes, des traductions littérales de l'anglais, des écarts historiques diffusés par les ouvrages de référence ont créé force quiproquos et malentendus sur ces termes. **Il est très important de ne pas confondre ces trois méthodes dont les démarches sont différentes, ce ne sont pas des variantes de la même démarche !** Peu importe si vous utilisez des appellations différentes de celles-ci, à condition d'être conscient du risque de confusion. Lisez attentivement les fiches et identifiez clairement la démarche qui vous concerne !

Bonne lecture.

Analyse par Arbre de Défaillances (A.A.D.)

Terme lié : Fault Tree Analysis (F.T.A.)

Objectif *(à quoi ça sert ?)*
La méthode des arbres de défaillances permet une analyse « déductive » des causes techniques ou opérationnelles pouvant provoquer des situations contraires à un objectif spécifié, en particulier, de sécurité (situation redoutée) ou de disponibilité (événement indésirable). On dit que la méthode est déductive car elle permet d'identifier les causes à une situation.

Description *(que produit la méthode et comment ?)*

Il s'agit d'une méthode logique de type booléen :

- (a) " Cette situation pourrait bien arriver **si** cette opération était exécutée **et si** ce défaut survenait de manière accidentelle ",
- (b) " Cet événement pourrait tout à fait survenir si ce contrôle n'était pas réalisé en temps utile ou si cette défaillance du système n'était pas réparée suffisamment vite ".

Cette analyse déductive est de nature " Top-Down". C'est à dire qu'en partant de l'événement redouté, on recherche pas à pas les événements qui peuvent en être la cause, de l'événement le plus général pour aller aux événements élémentaires.
Ces événements sont la conséquence d'événements internes ou externes au produit. Parmi ceux-ci figurent les défauts du produit.

Conduite de la méthode *(comment la met-on en œuvre ?)*

La méthode peut se mettre en œuvre en suivant les étapes principales suivantes :

- Définition de la/des situation(s) indésirable(s) à étudier,
- Définition des combinaisons qui conduisent à cette situation,
- Construction de l'arbre en utilisant les opérateurs logiques (portes « ET », « OU »…),
- Recherche de la/des coupe(s) minimale(s) (chemin(s) le(s) plus court(s) conduisant dans l'arbre à la situation indésirable).

Domaine de pertinence	Entrées	Sorties
- La méthode est plus particulièrement bien adaptée aux événements combinatoires. Elle devient cependant délicate à mettre en œuvre quand il s'agit d'événements séquentiels.	- La liste des états indésirables du produit. Une telle liste peut être établie dès la phase amont de la conception, être le résultat de l'expérience de l'entreprise ou de son client ou de la réflexion libre d'un groupe de travail. Souvent, il s'agit de considérer les aspects réglementaires du système en situation ou les risques inacceptables à faire courir aux utilisateurs (cas des études de sécurité).	- Document contenant : ➢ Les arbres de défaillances correspondant aux évènements redoutés étudiés, ➢ Analyse des coupes minimales.

Avantages	Inconvénients
- La méthode permet de connaître combien il est nécessaire d'avoir d'évènements intermédiaires pour conduire à l'événement redouté (coupe(s) minimales(s)).	- La qualité des résultats dépend beaucoup de l'expérience et de « l'imagination » de celui qui effectue l'analyse, - La méthode nécessite un programme informatique, lorsque le nombre de combinaisons d'évènements dépasse quelques dizaines d'unités, pour calculer l'occurrence de l'événement indésirable étudié et rechercher les coupes minimales.

Bibliographie

1. **DEF STAN 00-56** : "Safety Management Requirements for Defence Systems",
2. **CEI 61025 Ed. 2.0** : "Analyse par arbre de défaillance",
3. RAC : "Application Guide",
4. Ian S. Sutton : "Process Reliability and Risk Management", Van Nostrand Reinhold – 1992.

Analyse par Arbre d'Evénement (A.A.E.)

Terme lié : Event Tree Analysis (E.T.A.)

Objectif *(à quoi ça sert ?)*
Identifier et évaluer les conséquences possibles d'un événement initiateur selon les circonstances ou disfonctionnements avec lesquels il se combine.

Description *(que produit la méthode et comment ?)*
Basée sur une logique binaire (l'évènement se produit ou non, le composant ou le système est défaillant ou non), cette méthode permet de déterminer les conséquences possibles d'un évènement initiateur en étudiant les chemins possibles qui y conduisent. Ces chemins sont affectés d'une probabilité d'occurrence permettant de calculer les probabilités des conséquences. Un scénario ou un système (par exemple de sécurité) est formé de plusieurs éléments qui se combinent pour prévenir les conséquences graves. A partir de l'événement étudié, on envisage deux branches selon que le premier élément joue son rôle ou non ; dans chaque branche on envisage une alternative selon que le deuxième élément joue son rôle ou non et ainsi de suite jusqu'à la conséquence finale. On peut associer à chaque branche d'alternative la probabilité de succès et ainsi calculer *in fine* la probabilité de chacune des conséquences trouvées.

Conduite de la méthode *(comment la met-on en œuvre ?)*
1) Identifier l'évènement initiateur : ce peut être la défaillance d'un système, sous-système, composant… ou un évènement extérieur. On détermine ensuite la fréquence d'apparition de cet évènement (qui peut résulter d'un arbre de défaillances ou des conséquences d'un autre arbre d 'évènements), 2) Identifier les mécanismes de prévention : systèmes automatiques de sécurité, alarmes opérateurs, actions de l'opérateur, barrières de sécurité… Leur efficacité s'évalue au travers d'une probabilité de succès/échec, 3) Construction de l'arbre, de la gauche (avènement initiateur), vers la droite (conséquences) en enchaînant les mécanismes de prévention représentés par des branches : branche supérieure pour le succès, branche inférieure pour l'échec, 4) Estimer les probabilités de chaque branche (à l'aide d'un arbre de défaillances pour l'échec, par exemple), 5) Estimer les probabilités de chaque conséquence par combinaison des probabilités des branches, 6) Hiérarchiser les conséquences par probabilités.

Domaine de pertinence
- Affecter une gravité moyenne à un événement difficile à éviter (agression, panne…). - Comparer l'efficacité de différentes mesures (de prévention ou de protection) dédiées à la réduction de l'impact d'un événement initial, - Outil de modélisation très utile pour l'étude et l'estimation des risques d'accidents et l'enchaînement des aggravations successives conduisant à une liste de conséquences pour le système étudié, son personnel, les « riverains », l'environnement,

Entrées	**Sorties**
- Les éléments du système et de son environnement qui influent sur le cheminement des effets de l'événement étudié. Pour une approche quantitative, les probabilités des événements et conditions qui influent sur ces cheminements.	- Liste des conséquences possibles de l'événement, probabilités de chacune d'entre elles, liste pour chacune de ces conséquences des combinaisons d'éléments qui peuvent la causer, donc identification des possibilités de prévention de ces conséquences.

Avantages	**Inconvénients**
- Démarche naturelle très facile à s'approprier. Quelques recommandations importantes faciles à assimiler. Un animateur bien formé (1 ou 2 jours) est recommandé mais la méthode ne requiert pas de compétences longues ou difficiles à acquérir. La qualité des conclusions dépend de la qualité et l'exhaustivité de la liste des éléments pris en compte. Le chiffrage dépend de la disponibilité et de la précision des probabilités des alternatives élémentaires, - Permet d'estimer l'influence d'un facteur en faisant varier sa probabilité de réalisation, - Permet de suivre le déroulement d'un scénario accidentel et d'évaluer l'influence des parades sur la fréquence des conséquences, - Associée aux arbres de défaillances permet de connaître combien il est nécessaire d'avoir d'évènements intermédiaires pour conduire à l'événement redouté (coupe(s) minimales(s)).	- Les facteurs d'aggravation peuvent se confondre avec des défaillances, - La détermination des facteurs d'aggravation est fortement tributaire de la compétence de l'analyste, - La méthode nécessite un programme informatique, lorsque les événements résultent d'arbres de défaillances qui dépassent quelques dizaines d'unités, pour calculer l'occurrence de chaque conséquence étudiée et rechercher les coupes minimales.

Bibliographie

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

Analyse par Arbre de Causes

Objectif *(à quoi ça sert ?)*
Réunir dans une représentation synthétique et logique tous les éléments ayant contribué à un incident avéré.

Description *(que produit la méthode et comment ?)*
A partir de l'incident survenu, on relie les événements ou conditions dont la combinaison a directement provoqué l'incident. Puis, on reprend la décomposition pour chaque événement jusqu'à avoir intégré tous les événements et conditions élémentaires cités comme ayant contribué à l'incident.

Conduite de la méthode *(comment la met-on en œuvre ?)*
D'abord réunir librement tous les éléments : les faits, les circonstances, les étapes du scénario. Ensuite, les classer selon qu'ils sont « normaux » ou « anormaux » ou bien « internes » ou « externes ». Selon les référentiels, on classe ces éléments selon plusieurs critères plus ou moins nombreux. Puis établir les liens logiques ou chronologiques (C est la conséquence de A + B…). Représenter les événements par des symboles correspondants à leur classement (ronds, carrés…), les liens logiques par des traits. Il en résulte un schéma de forme arborescente où l'événement étudié est l'unique point final et les faits ou circonstances ayant contribué se déploient en amont à une place qui représente leur rôle dans le scénario.

Domaine de pertinence
- Analyse a posteriori des incidents et accidents. Elle est d'autant plus pertinente qu'on dispose de bonnes informations sur l'incident. Elle conduit à poser des questions adéquates pour approfondir l'enquête. Elle doit éviter de se focaliser sur une cause, un coupable et négliger des éléments plus discrets ou perdre des enseignements secondaires mais profitables.

Entrées	**Sorties**
- Connaissances de l'incident et des fonctionnements réellement possibles du système.	- Explication ouverte de l'incident, (articulant tous les éléments contributeurs et ne limitant pas à l'identification d'une « cause » ou d'une combinaison minimale de « causes »).

Avantages	**Inconvénients**
- Favoriser le travail en groupe, la synthèse de points de vue divers, - Méthode très répandue, - L'animation doit être rigoureuse et maîtrisée pour que le résultat ne soit pas réducteur et rassurant à bon compte.	- Elle prend bien en compte des logiques d'enchaînements temporels mais est très limitée pour représenter des données continues comme la durée.

Bibliographie
Publications INRS: 1. **ED 833**, « Face aux accidents : analyser, agir », 2. **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.

Arbres de Maintenance et d'Aptitude à la Maintenance

Objectif *(à quoi ça sert ?)*

L'arbre de maintenance ou d'aptitude à la maintenance (maintenabilité) fournit aux utilisateurs le moyen de définir, d'optimiser et d'actualiser la politique de maintenance de leurs outils de production : fournir aussi un moyen d'adaptation en fonction de l'évolution qualitative et quantitative de l'ensemble des biens durables constituant le patrimoine technique de leur entreprise.

Description *(que produit la méthode et comment ?)*

Chaque constituant de l'ensemble des biens durables sera bénéficiaire d'un niveau de maintenabilité opérationnel pondéré d'un facteur d'hétérogénéité dont les données seront déterminées :

1) par le niveau de qualité des documentations techniques de maintenance de chaque type de bien durable,
2) par un coefficient de dispersion de chaque type extrait de l'inventaire des biens durables de l'entreprise.

Conduite de la méthode *(comment la met-on en œuvre ?)*

1) Disposer au préalable d'un système et d'une doctrine de gestion des configurations et des arborescences de la nomenclature des types d'articles concernés,
2) Disposer au préalable d'un système de gestion de l'inventaire et du suivi technique des investissements matériels et logiciels de l'entrepris,
3) Définir des critères de non-maintenabilité des biens durables en fonction des moyens de logistique de maintenance disponible dans l'entreprise,
4) Etablir la cartographie de la maintenabilité des outils de production de l'entreprise,
5) Définir les parts des configurations susceptibles d'être traitées par des opérations préventives et correctives en entreprise et hors entreprise.

Domaine de pertinence

- La méthode s'applique avec efficacité uniquement pour la maintenance d'un parc de biens durables hétérogènes sur le plan des origines des fabricants, des technologies utilisées et des années de mise en service,
- Son application se situe sur le traitement des critères de choix des politiques de maintenance,
- Le type de problème à traiter par la méthode relève du domaine des activités de l'après-achat :
  - Service de maintenance interne de l'entreprise,
  - Entreprises prestataires de services de maintenance multi marques.
- La méthode s'applique à tous les patrimoines techniques des entreprises, qu'elles produisent des biens ou des services (Grands Comptes et PME/PMI),
- La méthode est particulièrement pertinente pour les entreprises situées dans des pays en voie de développement ou pour les entreprises qui désirent trouver des solutions aux problèmes posés par l'arrêt d'activité ou la disparition des fabricants de leurs biens durables.

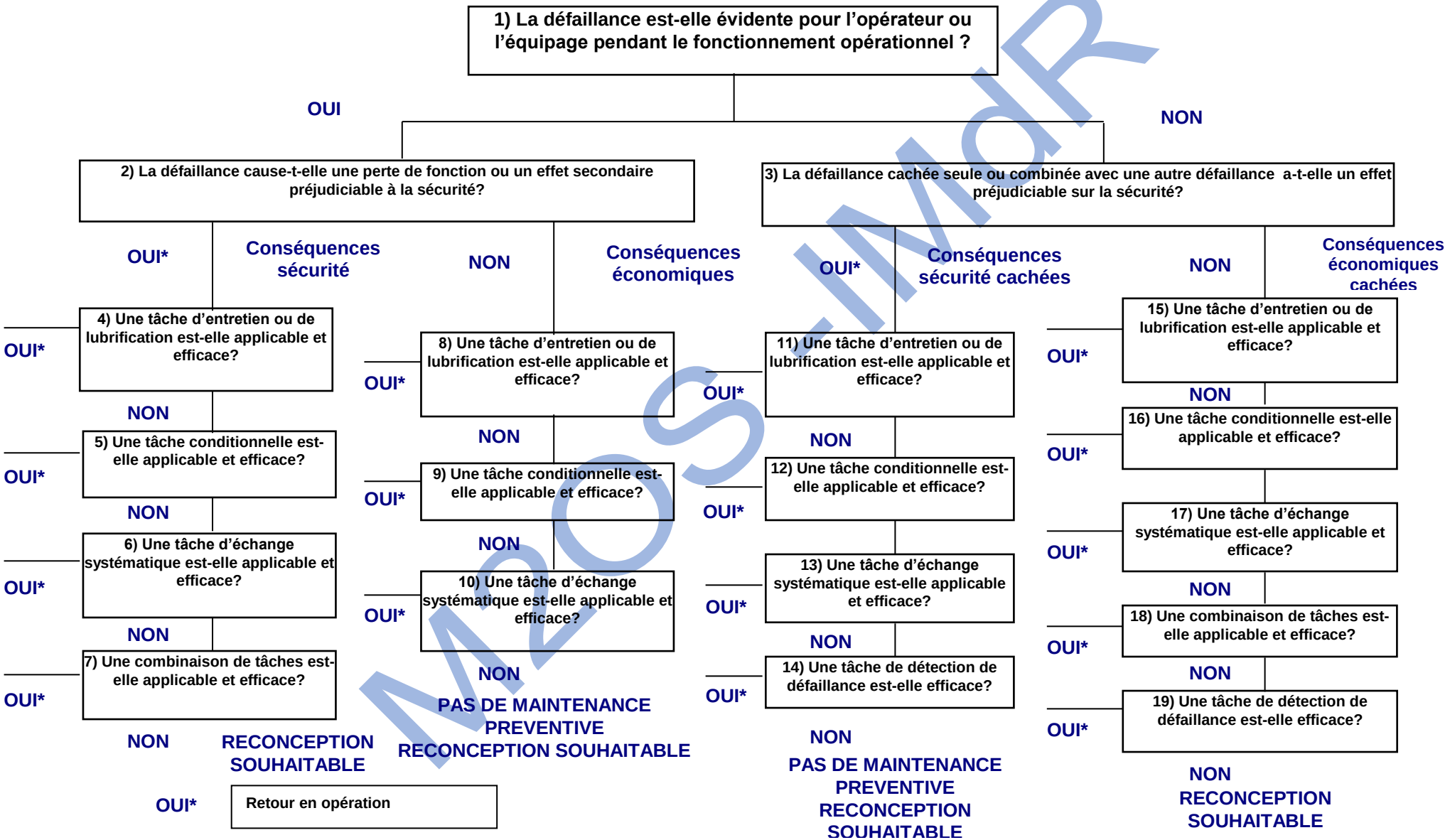
Entrées	Sorties
- L'inventaire des matériels et des logiciels identifiés, - La nomenclature et le prix des articles composés et composants, - L'arborescence des objets de la nomenclature et identifiés dans l'inventaire, - Les seuils de non-maintenabilité et les niveaux d'adéquation du soutient logistique de maintenance interne.	- L'évolution de la cartographie de la maintenabilité du patrimoine technique de l'entreprise, - Les éléments de décision en matière de gestion des rechanges et de politique maintenance, - Les traitements statistiques d'aide à la décision.

Avantages	Inconvénients
- L'arbre de maintenance et d'aptitude à la maintenance, permet aux utilisateurs de maîtriser une politique de maintenance dynamique et adaptable aux évolutions du profil de mission de chaque élément de l'ensemble du patrimoine technique de l'entreprise, - Pour les utilisateurs de matériels importés la méthode permet d'acquérir progressivement le savoir et le pouvoir faire une maintenance locale moins captive de monopoles ou d'obsolescences d'article de rechange, - Elle permet de mettre en place un soutien logistique de maintenance pertinent et adapté aux possibilités d'appropriation technico-économique nécessaires à la gestion de la durabilité opérationnelle, - La décision d'extérioriser une partie ou la totalité des opérations de maintenance est prise en connaissance de cause sur des critères économiques et techniques parfaitement et continuellement identifiés.	- Obligation éventuelle de disposer de logiciels capables de nourrir et de traiter des bases de données en vérifiant la cohérence des informations sur les évolutions de structure des configurations et sur les informations du retour d'expérience de la maintenance, - Obligation éventuelle de mettre en place en interne une nomenclature identifiant les articles de maintenance d'une façon univoque en filtrant les risques de doublons de références de fabricants / assembleurs différents, - Recours à la Maintenologie (étude du soutien logistique, de la maintenabilité durable, de la pertinence d'opérations de maintenance et de la typologie des défaillances probables).

Bibliographie

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

Illustration de la méthode : Alternatives de maintenance



Etude de danger et d'exploitabilité

Terme lié: HAZard and OPerational Study (HAZOP)

Objectif *(à quoi ça sert ?)*

Examen détaillé des composants d'un système pour déterminer ce qui se produirait si ce composant devait fonctionner en dehors de son mode normal d'utilisation.

Description *(que produit la méthode et comment ?)*

Chaque composant est affecté d'un ou plusieurs paramètres (pression, débit, puissance électrique…). L'Hazop regarde chaque paramètre alternativement et emploie des mots-guides pour énumérer le comportement anormal possible tel que « plus », « moins », « supérieur », « inférieur », « pas de »… . Les effets d'un tel comportement sont alors évalués.

Conduite de la méthode *(comment la met-on en œuvre ?)*

L'HAZOP passe par les étapes suivantes :

1) Définition du domaine d'étude et des objectifs,
2) Mise en place d'un groupe de travail,
3) Recherche des informations de conception, présentation du système à étudier par le concepteur,
4) Identification des éléments et de leurs caractéristiques, performances…
5) Choix des mots-guides et affectation des déviations (en cas de doute, ne pas écarter un risque),
6) Exploration de la façon dont elles pourraient se produire, recherche de causes et des conséquences,
7) Proposition de recommandations, recherche des mécanismes de protection ou d'alarme existants ou prévus, étude de leur efficacité (réduction de la probabilité ou de la conséquence du risque),
8) Impact sur la conception.

Mots-guides :

- NON : aucune donnée ou signal ne passe,
- PLUS : hausse quantitative,
- MOINS : baisse quantitative,
- AUSSI BIEN QUE : action réalisée correctement mais avec des résultats supplémentaires,
- UNE PARTIE DE : seulement une partie de la fonction est réalisée,
- INVERSE : inversion de la fonction,
- AUTRE QUE : le résultat obtenu est différent de celui attendu,
- TOT/AVANT : quelque chose se produit plus tôt que prévu,
- TARD/ENSUITE : quelque chose se produit plus tard que prévu.

Domaine de pertinence

- Le but est d'identifier les causes des risques et d'y trouver des remèdes,
- Une HAZOP ne doit pas être utilisée comme une étude de conception. Si la conception est incorrecte ou incomplète, la pertinence de l'étude sera compromise.

Entrées	Sorties
- Dossier de conception, - Analyse fonctionnelle, - Description de l'environnement, - APR, AMDEC, arbres de défaillances.	- Identification des risques, - Action de réduction des risques, - Hazard Log, - AMDEC, arbres de défaillances.

Avantages	Inconvénients
- Travail pluridisciplinaire en équipe, - Analyse systématique et détaillée, - Prise en compte de tous les points de vue (concepteur, utilisateur, maintenance, fournisseurs…), - Possibilité de travailler avec des « boîtes noires », - Possibilité de travailler sur les interactions entre composants si les modes de défaillances ne sont pas connus ou très complexes, - Audit de la conception.	- Si le périmètre d'étude est trop vaste, risque de non-exhaustivité, - Approche parfois lourde à mettre en place, - Attention au choix des mots-guides. Si on en réduit la liste ou s'il est trop limité, il abaisse la pertinence de l'analyse, - Adapter les mots-guides au domaine d'analyse.

Bibliographie

1. **DEF STAN 00-56** : "Safety Management Requirements for Defence Systems",
2. **DEF STAN 00-58** : "HAZOPS Studies on Systems Containing Programmable Electronics".

Analyse des Risques, Points Critiques pour leur Maîtrise (A.R.P.I.C.–M.)

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

Objectif *(à quoi ça sert ?)*

Le système ARPIC–M est un moyen de garantir la salubrité des aliments. Il repose sur la prévision et la prévention des dangers biologiques, chimiques et physiques.
Il a pour objectif de fournir une approche systématique d'identification, de localisation, d'évaluation et de maîtrise des risques potentiels de dégradation de la salubrité des denrées dans la chaîne alimentaire.
La directive européenne 93/43 sur l'hygiène des denrées alimentaires a instauré l'application du système ARPIC–M pour l'ensemble des filières agroalimentaires.

Description *(que produit la méthode et comment ?)*

La mise en place d'un système ARPIC–M correspond à une démarche rationnelle composée d'étapes successives. Celles-ci peuvent se regrouper en 6 grandes familles :

1) Définition du produit et du procédé de fabrication,
2) Identification des dangers à chaque étape de fabrication,
3) Etablissement des points critiques pour le contrôle (CCP),
4) Etablir un système de surveillance des points critiques,
5) Enregistrer et garder ces enregistrements,
6) Vérification de l'efficacité du système.

Conduite de la méthode *(comment la met-on en œuvre ?)*

La mise en œuvre du système ARPIC–M nécessite la constitution d'un groupe de travail.
Un arbre de décision est constitué pour qualifier une étape de fabrication.
Une analyse de cet arbre conduit à identifier les points critiques.
La gestion de ces points critiques permet d'en assurer la maîtrise.
Ce système peut être intégré dans des systèmes de management de la qualité des entreprises agroalimentaires.

Domaine de pertinence

- Le système ARPIC–M est un outil de gestion de la sécurité alimentaire,
- La méthode peut être appliquée à l'ensemble des secteurs de la transformation d'aliments ou de boissons, la distribution, la vente, la restauration.

Entrées	Sorties
- Données relatives au produit, - Synoptique des opérations de fabrication.	- Système de surveillance du procédé, - Plan d'actions correctives, - Enregistrements.

Avantages	Inconvénients
- Le système ARPIC–M fournit une méthodologie claire pour développer un plan d'assurance qualité : ➢ Les principes sont internationalement reconnus, ➢ Exhaustivité de l'analyse des dangers.	- Difficulté à identifier les Risques et Points Critiques (RPC), - Difficulté à évaluer la gravité des dangers et la probabilité de leur occurrence.

Bibliographie

1. 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,
2. C.Wallace, S.Mortimore : HACCP : Guide pratique – Polytechnica, 1998.

Analyse de zone

Objectif *(à quoi ça sert ?)*

Mettre en évidence les problèmes résultant des interactions physiques entre éléments voisins ou de flux perturbateurs générés par des sources externes.

Description *(que produit la méthode et comment ?)*

L'analyse de zone consiste à identifier et analyser, grâce à une investigation systématique réalisée sur maquettes, les problèmes résultant d'interactions physiques (émissions thermiques, bruit acoustique, nœuds de vibration, EMC…) entre différentes « zones » d'un produit ou entre certaines « zones » et le milieu extérieur. Ces problèmes ne peuvent pas être identifiés, en principe, à partir de la seule documentation technique et nécessitent donc une investigation spécifique sur des ensembles maquettés faisant eux-mêmes l'objet d'une partition en « zones ».

Conduite de la méthode *(comment la met-on en œuvre ?)*

La démarche suivie consiste à identifier successivement, à l'examen des maquettes disponibles :

- les zones géographiques d'appartenance des différents éléments matériels,
- les flux de toute nature pouvant être émis par chaque élément d'une même zone, que cet élément soit en fonctionnement normal ou non (ex : émission thermique, dégazage, épanchement d'électrolyte)…),
- les flux émis par les sources externes à chacune des zones (ex : EMC, vibrations, erreurs humaines…),
- l'effet de ces différents flux (internes et externes) sur les performances de chaque élément d'une même zone puis sur celles des fonctions de service et/ou des fonctions techniques du produit.

Les conséquences des effets d'interactions sont ensuite classées selon deux catégories :

- les conséquences mineures, qui sont en principe classées sans suite,
- les conséquences significatives qui donnent lieu à des propositions de modifications ou à des recommandations. Par exemple :
  - ajout de dispositifs d'isolation,
  - amélioration des interfaces homme/machine,
  - amélioration des dispositifs d'évacuation (par exemple sur le plan thermique),
  - recommandations sur les procédures de maintenance,
  - recommandations sur les procédures d'exploitation…

L'analyse de zone, appliquée de manière successive sur des maquettes de plus en plus représentatives du produit final, peut enfin conduire à la définition d'essais à entreprendre (ex : essais de compatibilité) et à la préparation d'études spécifiques (ex : analyses de risques particuliers : feu, explosions, contamination…).

Domaine de pertinence
- Tout système dans lequel des interactions physiques, non appréhensives par les analyses classiques (AMDEC, AAD…) entre « zones » distinctes risquent de nuire à son bon fonctionnement, - Tout système dans lequel des défaillances de cause commune sont à prévoir, - Interfaces homme/machine.

Entrées	Sorties
- Ensembles maquettés, - Dossiers techniques.	- Effets des flux perturbateurs sur les différentes zones du produit ou sur le milieu extérieur, - Défaillances de causes communes, - Actions correctives ou essais à entreprendre.

Avantages	Inconvénients
- Mise en évidence de problèmes non détectables par les analyses papier.	- Nécessité de disposer de maquettes de plus en plus représentatives des exemplaires définitifs.

Bibliographie

1. C. Lievens – "Sécurité des systèmes", Edition Cepadues,
2. A. Villemeur – "Sûreté de fonctionnement des systèmes industriels", Eyrolles, 1988.

Maintenance Basée sur la Fiabilité (MBF)

Terme lié: Reliability Centered Maintenance (RCM)

Objectif *(à quoi ça sert ?)*
Méthodologie visant à optimiser la maintenance tout en maîtrisant la sécurité, la disponibilité et la durée de vie d'un équipement.

Description *(que produit la méthode et comment ?)*
Il s'agit d'une méthode qui définit le programme de maintenance préventive optimale vis à vis des enjeux liés aux conséquences des défaillances des systèmes et des équipements. Le dimensionnement de la maintenance doit s'effectuer en fonction des conséquences des défaillances sur les fonctions (approche système) plutôt qu'en fonction des défaillances sur les composants (approche objet). Cette méthode peut influencer la définition de l'équipement lui-même.

Conduite de la méthode *(comment la met-on en œuvre ?)*

La méthode MBF – Voir aussi sous le nom d'OMF (Optimisation de la Maintenance par la Fiabilité) – passe par les étapes suivantes :

1) Elaboration d'un plan MBF (objectifs, méthodes, planification et organisation),
2) Détermination des données initiales (critères de sélection des candidats MBF, caractéristiques de conception, définition fonctionnelle, données de Sûreté de Fonctionnement, de Coût et d'Environnement),
3) Analyse RCM proprement dite :
   - Analyse des conséquences des défaillances (conséquences sécuritaires, économiques…),
   - Analyse structurale,
   - Définition des tâches de maintenance améliorant le niveau de fiabilité ou de sécurité du candidat,
   - Identification des alternatives de maintenance,
   - Analyse et hiérarchisation des tâches de maintenance suivant les paramètres de sûreté de fonctionnement[*1] à optimiser,
   - Analyse système construite en arbre logique,
   - Détermination des seuils et intervalles de maintenance en cohérence avec les paramètres de l'analyse.
4) Exploitation des retours d'expériences internes et externes à la suite de la phase d'exploitation de systèmes comparables.

Domaine de pertinence
- La méthode MBF s'inscrit conjointement aux processus des études de Sûreté de Fonctionnement et des Analyses du soutien Logistique de façon à orienter l'organisation de la maintenance pour une sécurité et une disponibilité optimale à moindre coût. Cette méthode concerne donc les systèmes complexes, coûteux et à longue durée de vie.

Entrées	**Sorties**
- Plan de maintenance d'un système similaire, - Etudes FMDS, AMDEC, - Décomposition logistique du système et concept de maintenance associé.	- Plan de maintenance optimisé, - Périodicités des tâches homogénéisées.

Avantages	**Inconvénients**
- Justification organisée et structurée des types de tâches à effectuer et de leur périodicité, - Prise en compte de l'impact de la fonction sur la sécurité et la disponibilité et du profil de vie, - Visualisation de la mission réalisée par le système, - Optimisation en fonction : ➢ de l'exploitation du produit, du sous-ensemble, de la fonction, ➢ de la criticité des fonctions en termes de : • Sécurité, • Disponibilité, • Coût.	- Approche parfois lourde à mettre en place, - La méthode s'appuie sur une AMDE(C).

Bibliographie

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

Intégration Conception et Soutien (ICS)

Objectif *(à quoi ça sert ?)*

Aide à la décision pour la sélection d'une solution préférentielle pour la conception d'un matériel durable et réparable, compte tenu de critères de COUT, de DISPONIBILITE et d'EFFICACITE.

Description *(que produit la méthode et comment ?)*

Le processus « ICS » fournit un classement des conceptions envisageables, selon:

- les divers paramètres entrant dans la définition des facteurs de base « COUT GLOBAL », « DISPONIBILITE », « EFFICACITE » ainsi que les méthodes de calcul associées (ces paramètres doivent être renseignés dans une base de données appropriée),
- la réalisation de simulations liées à la recherche du compromis optimum et les critères de sélection de la solution préférentielle retenue a priori pour la conception du matériel considéré.

Conduite de la méthode *(comment la met-on en œuvre ?)*

Initialisation du processus « ICS », incluant :

- la présentation d' « ICS » au Donneur d'ordres,
- la prise en compte du cahier des charges,
- l'introduction d' « ICS » chez les éventuels sous-traitants.

Définition des solutions envisageables à la conception, incluant :

- les tâches techniques et technologiques dédiées au bureau d'études,
- la prise en compte de la « SdF » (les rubriques « FMDS »),
- la prise en compte de l'ASL (Analyse du Soutien Logistique), compte tenu de la logistique « UTILISATEUR »,
- la collecte des données de coût et de technico-logistique associées.

Calcul des facteurs de base « ICS » : « COUT GLOBAL », « DISPONIBILITE », « EFFICACITE » (ces dernières étant liées à la notion d'ESSENTIALITE).

Sélection de la solution préférentielle, incluant :

- le calcul de l'indicateur de base (FACTEUR DE MERITE),
- le calcul d'indicateurs auxiliaires d'aide à la décision,
- le « rebouclage » sur la conception,
- la décision finale (validation).

Domaine de pertinence

- Le processus « ICS », axé sur le compromis « COUT/DISPONIBILITE-EFFICACITE », se veut simple et résolument opérationnel pour tous ceux qui ont en charge la conception d'équipements et/ou de systèmes.
- « ICS » a une vocation « SYSTEMIQUE », un caractère « PLURIDISCI-PLINAIRE » et est donc destiné tant aux administrations clientes et aux grands groupes industriels qu'aux PME/PMI, sociétés-conseils et universitaires qui se spécialisent dans l'ingénierie logistique.
- « ICS » constitue à cet effet un outil permettant d'améliorer la compétitivité des produits conçus et de conforter ainsi l'image de marque des fournisseurs.

Entrées	Sorties
- Cahier des charges + données « COUT » et « TECHNICO-LOGISTIQUES ».	- Valeurs des facteurs de base et des indicateurs, - Classement des solutions envisageables, - Sélection de la solution préférentielle.

Avantages	Inconvénients
- Mise en œuvre d'une démarche pragmatique de SLI, incluant : ➢ Rapidité d'exécution des tâches, ➢ Utilisation aisée avec des moyens simples, ➢ Prise en compte simultanée du couple « COUT/PERFORMANCES », ➢ Introduction d'un facteur de mérite et d'autres indicateurs spécifiques d'aide à la décision. - Adaptation du processus aux règles propres à l'entreprise sans surcoût notable hormis des frais limités de formation.	- Nécessité de réaliser des « AMDEC » évoluées. - Possibles difficultés pour l'estimation des facteurs d' «ESSENTIALITE».

Bibliographie

GTR – ICS / IMdR, Ouvrage « ICS », version n°3, 01/01/2006.

Plans d'expériences

Objectif *(à quoi ça sert ?)*

Permettre aux concepteurs de maîtriser les paramètres de conception, à l'aide d'un nombre minimal d'essais. Le réglage de ces paramètres permet d'optimiser les performances du produit ou des procédés et/ou de réduire leur sensibilité aux différentes sources de variabilité.

Description *(que produit la méthode et comment ?)*

Un plan d'expériences est une méthode d'expérimentations basée sur un protocole d'essais structuré. On y fait varier simultanément les valeurs (ou les niveaux) de plusieurs facteurs d'entrée d'un essai à un autre. On observe alors l'impact de ces variations sur une ou plusieurs performances (variable de sortie) d'un produit ou d'un procédé. De ce fait, il est en opposition avec le schéma expérimental « classique » dans lequel la recherche de l'effet de facteurs d'entrée contrôlés sur une performance consiste à ne faire varier qu'un seul facteur à la fois d'une expérience à une autre. La structuration de cette expérimentation ainsi que le traitement des résultats obtenus s'appuient sur l'application des tests statistiques faisant appel à l'analyse de la variance (ANAVAR).

Conduite de la méthode *(comment la met-on en œuvre ?)*

La faisabilité d'un plan d'expériences est sous-tendue par le respect de plusieurs conditions :

- Nombre d'exemplaires de l'entité testée (produit ou procédé) compatible avec le schéma expérimental requis,
- Planning suffisant pour la réalisation complète des essais,
- Budget compatible avec le protocole expérimental retenu,
- Existence d'une équipe multidisciplinaire devant mener à bien la réalisation du plan d'expériences et constituée au minimum :
  - D'un expert en plan d'expériences (ex : un statisticien, un expert en fiabilité…) dont le rôle essentiel est de mettre au point le protocole expérimental, de le valider et d'exploiter les résultats,
  - D'ingénieurs et/ou de techniciens ayant une connaissance approfondie du produit (ou du procédé) et de son profil d'utilisation,
  - D'experts technologiques dans les domaines liés à la raison d'être du plan d'expériences (ex : Technologies électriques, technologies mécaniques, expertise de l'environnement…),
  - D'expérimentateurs ayant la charge de réaliser les essais conformément au protocole retenu et d'effectuer les mesures nécessaires avec la précision requise.

Lorsque ces conditions sont réalisées, le plan d'expériences peut être mis en œuvre et passe par les étapes suivantes :

- Le choix d'une méthode d'expérimentation : facteurs retenus, nature de ces facteurs, choix des modalités ou des niveaux sur les facteurs, interactions envisagées (d'ordre 2 ou plus), nature du plan d'expériences (complet, fractionnaire, simple ou croisé, définition de la matrice d'essais du plan retenu, ordre des essais).
- La conduite de l'expérimentation proprement dite : elle consiste à mettre en œuvre la séquence d'essais conformément au protocole retenu à l'étape précédente. La valeur des résultats obtenus en final dépend beaucoup des soins apportés à la qualité de réalisation des expériences et à la précision des mesures.
- L'analyse des résultats se complète d'une série de vérifications de la part du « pilote » de l'expérimentation :
  - Vérification de la cohérence des résultats et l'examen des valeurs suspectes,
  - Recherche des effets significatifs (analyse de la variance) et modélisation de la réponse à l'aide du modèle linéaire (utilisation préconisée d'un logiciel spécifique),
  - Recherche des ambiguïtés au niveau des « effets » (ex : mélange possible des « contrastes » et des effets dans l'utilisation des plans fractionnaires),
  - Contrôle a posteriori du domaine d'intérêt des résultats (i.e. : envisager éventuellement la poursuite de l'expérimentation dans une nouvelle région),
  - Analyse des « alias » entre effets principaux et effets d'interactions (intérêt possible d'un plan complémentaire),
  - Examen de la validité du modèle du 1er degré (intérêt possible de plans complémentaires pour envisager un modèle quadratique par exemple).

Une reprise de l'expérimentation doit donc être envisagée si nécessaire. Selon les cas, cette reprise peut conduire à :

- Lever les ambiguïtés (alias, mesures incertaines, biais…),
- Intégrer dans le modèle de nouveaux facteurs d'entrée non pris en compte dans le plan initial,
- Utiliser un modèle non linéaire (ex : modèle quadratique),
- Mettre en évidence l'optimum recherché,
- Rechercher une solution « robuste » (i.e. : insensible aux fluctuations des facteurs non contrôlés),
- …

Domaine de pertinence
- Recherche de l'optimisation des performances d'un produit nouveau, par la mise en évidence des valeurs ou des modalités des paramètres de conception du produit, - Construction de la robustesse d'un produit nouveau, par la fixation des paramètres de conception en vue de réduire la sensibilité de ses performances aux différentes sources de variabilité.

Entrées	Sorties
- Identification des performances du produit, - Identification des paramètres de conception (quantitatifs ou qualitatifs) pouvant avoir un effet significatif sur les performances du produit.	- Identification des paramètres de conception ayant un effet significatif sur les performances du produit, - Valeurs ou modalités des paramètres de conception permettant d'optimiser les performances et/ou de réduire leur sensibilité aux sources de variabilité.

Avantages	Inconvénients
- Réduction du nombre d'expériences à effectuer, - Identification des effets unitaires et des effets d'interaction des paramètres de conception sur les performances du produit, - Optimisation des performances du produit, - Aide à la conception de la robustesse d'un produit nouveau.	- Peut nécessiter un protocole expérimental difficile à mettre en œuvre, - Nécessite souvent l'usage d'un logiciel spécifique pour déterminer le protocole expérimental, pour traiter les résultats (analyse de la variance).

Bibliographie

1. **NF X 06.080 :** « Plan d'expériences : vocabulaire et indications générales »,
2. M. Vigier – « Pratique des plans d'expériences – Méthodologie Taguchi », Les Editions d'organisation,
3. J. Goupy – « La méthode des plans d'expériences » Ed. Dunod,
4. J. Demonsant – « Comprendre et mener des plans d'expériences, AFNOR »,
5. WG Cochran & G. Cox – « Experimental Design » Ed. John Wiley & Sons,
6. ASTE – « Le rôle des essais dans la maîtrise de la fiabilité »,
7. RAC Blueprints for Product Reliability.

Essais accélérés de durée de vie

Objectif *(à quoi ça sert ?)*

Prédire, de manière économique et sur un laps de temps réduit, l'évolution dans le temps d'une (ou plusieurs) performance(s) fonctionnelle(s) ainsi que la durée de vie d'une entité matérielle utilisée dans ses conditions normales d'emploi, à partir d'essais réalisés sous des valeurs de contraintes supérieures aux niveaux spécifiés en utilisation normale.

Description *(que produit la méthode et comment ?)*

Les essais accélérés consistent à soumettre une ou plusieurs entités matérielles (composant, carte, sous-ensemble, ensemble complet) à une ou plusieurs contraintes simultanées, sous des niveaux supérieurs aux niveaux spécifiés en utilisation normale, jusqu'à obtention de leur fin de vie. Les résultats obtenus seront ensuite extrapolés dans les conditions normales du produit à l'aide de modèles analytiques validés par l'expérience. En général, l'entité considérée correspond à un composant, à un assemblage de matériaux ou à des structures simples.

Conduite de la méthode *(comment la met-on en œuvre ?)*

La réalisation d'un essai accéléré passe par les étapes suivantes :

- **Planification de l'essai :** Elle est fondamentale pour obtenir les résultats espérés. Il s'agit avant tout d'identifier les performances et/ou caractéristiques de l'entité à mesurer, d'évaluer les mécanismes de défaillances déterminants et d'identifier la nature de la contrainte (ou des contraintes) accélérant de manière prépondérante ces mécanismes. Le niveau (amplifié) de chaque contrainte appliquée au cours de l'essai est ensuite à déterminer. Afin de faciliter cette planification de l'essai, les recommandations suivantes sont à prendre en compte :
  - Les exemplaires testés de l'entité considérée doivent être représentatifs du produit final,
  - Seules les contraintes ayant une action prépondérante sur les mécanismes de défaillance déterminants sont à amplifier, les autres contraintes devant rester « normales » ou inexistantes (ex : absence de vibrations),
  - Les niveaux de contraintes amplifiés ne doivent pas excéder les limites imposées par les technologies de l'entité. De plus, les niveaux retenus doivent être tels que les modes de défaillance qu'ils génèrent soient représentatifs des modes de défaillance pouvant être observés dans les conditions d'utilisation normale de l'entité.

- **Réalisation de l'essai :** l'essai accéléré est réalisé sur tous les exemplaires identifiés à l'étape de planification, en faisant appel aux moyens d'essais permettant de générer l'environnement spécifié. Pour pouvoir extrapoler la durée de vie de l'entité dans les conditions normales d'utilisation, il est indispensable de poursuivre l'essai jusqu'à défaillance de chaque exemplaire testé. Lorsque le modèle analytique retenu donnant l'accélération de la probabilité de défaillance au niveau de contrainte appliqué n'apparaît suffisamment validé par l'expérience, il est recommandé de compléter l'essai de base par des essais complémentaires consistant à appliquer à d'autres exemplaires les contraintes de même nature mais sous des niveaux différents. Les durées de vie observées sous ces différents niveaux permettent alors de s'assurer que le modèle analytique initialement retenu pour l'extrapolation des résultats dans les conditions normales est valide et, le cas échéant, de faire appel à un autre modèle.

- **Analyses et prédiction :** les analyses effectuées à partir des durées de vie observées à l'issue de l'essai accéléré en vue de la prédiction de durée de vie dans les conditions normales d'utilisation s'appuient sur le modèle analytique retenu. De plus, les techniques de lissage sur des échelles fonctionnelles appropriées peuvent s'avèrent nécessaires pour valider ce modèle. Parmi les modèles les plus fréquemment utilisés, on peut citer :
  - le modèle d'Arrhenius : surtout applicable aux composants électroniques, il traduit l'évolution du taux de défaillance avec la température sous la forme d'une loi exponentielle.
  - le modèle d'Eyring : généralisant le modèle d'Arrhenius, il traduit l'évolution du taux de défaillance sous la forme d'une loi exponentielle faisant intervenir à la fois la température et l'humidité.
  - la loi en puissance inverse du type : N x Sb = K, où S correspond à un niveau de contrainte donné et N le nombre de cycles d'application de cette contrainte jusqu'à défaillance de l'entité. Cette loi s'applique particulièrement au cas des structures mécaniques soumises à sollicitations répétitives (loi de Basquin).

Domaine de pertinence

- En principe sur certains ensembles a priori critiques des prototypes disponibles en phase de faisabilité, afin de pouvoir envisager les actions correctives nécessaires avant que la conception ne soit figée. Lorsqu'ils sont réalisés en **phase de conception**, les essais accélérés ont plutôt pour vocation d'aider à résoudre certains problèmes technologiques déjà identifiés.

Entrées	Sorties
- Profil de vie du produit, - Niveaux normaux des contraintes, - Éléments a priori critiques. - Contraintes les plus critiques, - Modèles d'accélération.	- Durée de vie dans les conditions de l'essai, - Durées de vie extrapolées dans les conditions normales d'utilisation, - Faiblesses potentielles du produit.

Avantages	Inconvénients
- Réduire de manière significative les délais nécessaires qui seraient entraînés par la mise en œuvre d'essais réalisés sous des contraintes « normales », pour pouvoir prédire la durée de vie et l'évolution des caractéristiques dans le temps d'une entité matérielle dans ses conditions d'utilisation spécifiées, - Permettre d'identifier des faiblesses de conception (produit et procédés) vis-à-vis de certaines contraintes.	- Difficulté de pouvoir appliquer simultanément au cours de l'essai toutes les contraintes présentes dans le profil d'utilisation, - Incertitudes sur la nature des modèles mathématiques d'accélération ou sur la valeur de leurs paramètres (ex : énergie d'activation dans le modèle d'Arrhenius).

Bibliographie

1. ASTE « Le rôle des essais dans la maîtrise de la fiabilité »,
2. RAC Reliability Toolkit – Commercial practices edition,
3. Wayne Nelson « Accelerated Testing » – Éd. John Wiley,
4. Revue Phoebus n°13 « Les essais accélérés », – Ed. Préventique,
5. Annales journées SIA de mai 2000 « Les essais accélérés »,
6. Revue IEEE Transaction of Reliability.

Essais aggravés

Objectif *(à quoi ça sert ?)*

Explorer les marges de fonctionnement d'un produit en développement et déceler au plus tôt, pour pouvoir les corriger, les défauts inhérents à la conception (produit et procédés) qui réduisent ces marges à des valeurs jugées insuffisantes.

Description *(que produit la méthode et comment ?)*

Les essais aggravés consistent à soumettre une entité matérielle de conception nouvelle (pièce, composant, assemblage…) à des contraintes d'environnement et/ou de fonctionnement sous des niveaux croissants en vue d'atteindre les limites de résistance des technologies utilisées. Par principe même, ces contraintes sont portées à des niveaux supérieurs aux valeurs spécifiées. Une fois les limites de résistance atteintes, les essais sont interrompus avant de statuer sur les suites à donner : marges jugées suffisantes, reprise de conception, corrections ponctuelles…

Conduite de la méthode *(comment la met-on en œuvre ?)*

Pour connaître les limites de fonctionnement de l'entité soumise à essai et déceler au plus tôt les causes assignables de défaillance (i.e. : causes non liées aux limites technologiques et en principe corrigibles), le principe retenu consiste à appliquer à l'entité les contraintes sélectionnées de manière échelonnée en partant d'un niveau au moins égal au niveau spécifié en utilisation et en augmentant ce niveau par échelons successifs.

Si, en l'absence de défaillance (selon les critères préalablement définis), on atteint un niveau de contrainte tel que la dispersion maximale prévisible des sources de variabilité (ex : procédés de fabrication, caractéristiques internes des matériaux, environnement,..) reste sans effet sur la conformité des performances par rapport à la spécification, la marge de fonctionnement est considérée comme suffisante et l'essai peut être arrêté.

En cas d'apparition d'une défaillance (selon les critères retenus) sous un niveau donné de la contrainte appliquée, il est nécessaire de procéder à une analyse technologique approfondie afin d'en déterminer la cause première. Deux situations peuvent alors se présenter :

- La cause de défaillance est une cause « assignable » (ex : tolérance insuffisante, composant mal calibré, problème de fabrication…), une action corrective visant à supprimer cette cause ou à en atténuer les effets (opération dite de « contournement ») est alors engagée. Cette action corrective étant incorporée, le processus itératif de l'essai aggravé est repris à partir du niveau de contrainte sous lequel la défaillance s'était manifestée,
- La cause de défaillance est inhérente aux technologies utilisées, à la nature même du concept du produit ou des procédés de fabrication. On considère alors que l'on a atteint la limite technologique du produit, qui peut apparaître suffisante au regard de la spécification, ou au contraire insuffisante, ce qui doit entraîner, selon les cas :
  - Soit un retour sur la spécification,
  - Soit une remise en cause de la conception de l'entité.

Quelle que soit la décision retenue, l'essai aggravé faisant intervenir la contrainte considérée est arrêté.

La démonstration de l'efficacité des essais aggravés peut se mesurer de manière naturelle en termes de rentabilité économique. La méthode permettant d'évaluer cette rentabilité consiste à comparer :

- Le surcoût généré par la mise en œuvre des essais aggravés (moyens d'essais, destruction éventuelle de prototypes, heures opérateurs…),
- Les gains (en termes économiques) résultant de la mise en évidence précoce des défauts et de leur correction.

Domaine de pertinence

- En priorité, éléments du produit ou des procédés qui présentent un caractère critique de par leur fonction ou de par certains caractères de nouveautés : conception et technologies nouvelles, nouveau profil d'utilisation, procédés encore non matures…

Entrées

- Profil de vie du produit,
- Valeurs spécifiées des contraintes,
- Eléments a priori critiques (sorties AMDEC),
- Contraintes jugées efficaces.

Sorties

- Marges de fonctionnement,
- Faiblesses potentielles du produit.

Avantages

- Détermination des marges de fonctionnement,
- Identification des défauts de conception (causes assignables de défaillances) du produit,
- Construction de la robustesse du produit.

Inconvénients

- Nécessité de pouvoir disposer de moyens d'essais spécifiques (ex : vibrateurs 6 axes),
- Impossibilité de prédire la fiabilité du produit,
- Destruction des exemplaires soumis à essais (en général).

Bibliographie

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

Epreuves de déverminage

Objectif *(à quoi ça sert ?)*
Faire apparaître les défauts de jeunesse d'un produit afin de les corriger avant livraison.

Description *(que produit la méthode et comment ?)*

Les épreuves de déverminage consistent à soumettre les exemplaires (ou certains de leurs sous-ensembles) d'un matériel en sortie de production à des cycles de contraintes adaptées (électriques, mécaniques, thermiques…) visant à précipiter les défauts latents (présents dans le produit) en défauts patents (observables). Le niveau des contraintes appliquées peut être, selon les cas, inférieur ou égal aux valeurs de spécification d'emploi (***déverminage classique***) ou supérieur à ces valeurs (***déverminage aggravé***). **Dans tous les cas de figure, le principe de base est de stimuler plutôt que simuler, mais ne pas détruire.**

Conduite de la méthode *(comment la met-on en œuvre ?)*

La décision et la planification d'épreuves de déverminage doivent être établies en amont de la phase de production, sur la base de critères économiques et de faisabilité technique… L'opération de déverminage est la résultante d'un **processus récurrent** qui doit se décliner de la façon suivante :

- Dès la phase de conception, planification initiale des épreuves de déverminage :
  - Intérêt économique du déverminage,
  - Partie(s) du système soumise(s) à déverminage (i.e. : cartes, équipements, sous-systèmes…),
  - Profil de déverminage envisagé : nature des contraintes, valeurs retenues, durées d'application…
- En fin de phase de conception : expérimentation (par exemple sous la forme d'un plan d'expériences) du profil de déverminage planifié initialement sur quelques exemplaires ayant une configuration proche de la configuration finale. En fonction des résultats obtenus, le profil d'environnement initial peut être modifié pour rendre le déverminage plus efficace.
- Au cours de la phase de production, les épreuves de déverminage doivent continuer à être pilotées, sur la base d'analyses statistiques portant sur les défauts révélés par ces épreuves et sur les données de retour d'expérience des produits en exploitation. En fonction des résultats de ces analyses, les décisions suivantes peuvent être envisagées :
  - Poursuite du déverminage en l'état : si les taux de chute en déverminage restent significatifs, si les procédés apparaissent encore immatures et si les défaillances en exploitation sont peu nombreuses,
  - Modification du profil d'environnement du déverminage : si les défaillances en exploitation sont trop nombreuses (i.e. : le déverminage dans sa forme actuelle n'est pas suffisamment efficace),
  - Arrêt du déverminage : dès que les procédés deviennent matures et que les taux de chute révélés en déverminage ainsi que les défaillances observées en exploitation deviennent très faibles. On peut être amené aussi à ne pas supprimer complètement le déverminage, mais à l'appliquer seulement sur des échantillons prélevés périodiquement afin de s'assurer qu'il n'y a pas de dérives importantes dans les procédés de fabrication ou dans la qualité des produits approvisionnés.

L'efficacité du déverminage dépend essentiellement du profil d'environnement retenu à chaque niveau d'application (cartes, équipements…). Afin de choisir la nature des contraintes applicables, il est recommandé d'analyser préalablement le profil de vie complet du produit et de caractériser les contraintes d'environnement associées aux différentes situations de ce profil. Le profil de déverminage retenu initialement devrait ainsi être conçu de manière à stimuler, dans le respect des marges de fonctionnement de l'entité considérée, les défauts latents dont la manifestation au cours du profil de vie risque d'être corrélée avec les contraintes d'environnement et d'utilisation identifiées. Les profils de déverminage les plus efficaces et les plus pratiqués sont constitués de séquences répétitives de **cycles thermiques** et de **cycles de vibrations aléatoires**, avec adjonction de stimulis et de séquences « arrêt-marche » dans le cas des matériels électroniques.

Dans le cas du déverminage « aggravé », les niveaux de contraintes appliquées sont au-delà des valeurs spécifiées. Cela impose d'avoir réalisé en amont des essais aggravés assurant la robustesse du produit et permettant de connaître ses **limites de fonctionnement** (i.e. : limites du domaine dans lequel les performances restent nominales) et ses **limites de destruction** (i.e. : limites du domaine dans lequel les performances sont dégradées mais réversibles). Les niveaux appliqués dans ce type de déverminage sont en général compris entre ces deux limites de manière à obtenir le maximum d'efficacité sans pour autant entamer trop sensiblement la durée de vie potentielle du produit. Des essais de validation du profil de déverminage retenu devront dans ce cas être effectués avant transfert à la production de manière à vérifier d'une part l'**innocuité**, et d'autre part l'**efficacité** de ce profil.

Domaine de pertinence
- Matériels (assemblages complets, sous-ensembles, cartes, composants) de nature électrique ou électronique. A un niveau fin de d'assemblage du système (ex : cartes) les contraintes appliquées peuvent être plus facilement personnalisées au besoin recherché et peuvent donc s'avérer plus efficaces, - Matériels faisant appel à des technologies innovantes et/ou dont les procédés de fabrication sont innovants ou mal maîtrisés, défauts générés dans les opérations d'assemblage (ex : soudures, connexions, tolérances non respectées…), - Sous-ensembles critiques (ex : spatial, domaine médical…), - Soumis à un environnement opérationnel très sévère.

Entrées	Sorties
- Nature du produit, - Procédés de fabrication, - Flux de production, - Limites de fonctionnement et de destruction (déverminage aggravé), - Profil de vie du produit), - REX sur des produits similaires, - Moyens d'essais disponibles.	- Mise en évidence des défauts latents, - Correction et/ou remplacement des entités défectueuses avant livraison.

Avantages	Inconvénients
- Réduction du nombre de reprises après livraison aux clients, - Satisfaction des clients, - Amélioration de l'image de marque.	- Coût et délais associés à l'opération de déverminage (disponibilité de moyens d'essais spécifiques, énergie consommée, main d'œuvre).

Bibliographie

1. ASTE « Guide pour le déverminage des matériels électroniques » – 1987
2. ASTE « Guide pour le déverminage des matériels électroniques : apport de la démarche aggravée » – 2006
3. **BNAe RG Aéro 000 29**:« Guide pour la définition et la conduite d'essais aggravés »
4. **CEI 61.163-1** : « Déverminage sous contraintes Partie 1 : Assemblages réparables fabriqués en lots » – 2008
5. G.K. Hobbs « Accelerated Reliability Engineering « John Wiley & Sons » – 2000
6. Harry W. McLean « HALT, HASS & HASA explained: Accelerated Reliability Techniques » – ASQ Quality Press – Milwaukee – Wisconsin.

Logique de traitement des incidents et actions correctives (LTI-AC)

Terme lié: Failure report and corrective Action System (FRACAS)

Objectif

Fournir toutes les informations requises pour identifier les causes de dysfonctionnements d'un produit manifestés au cours de son développement ou de son utilisation en vue d'apporter, en temps et en heures, les actions correctives appropriées. Fournir des indicateurs permettant d'évaluer la croissance de fiabilité du produit en phase de développement ou en phase d'utilisation.

Description

La logique de traitement des incidents et des actions correctives (LTI–AC**)** consiste à établir, tant chez le fournisseur en phase de conception du produit que chez l'exploitant en phase d'utilisation, une boucle de réaction visant à enregistrer, documenter et analyser tous les incidents survenant au cours du cycle de vie du produit. Cette boucle de réaction s'appuie sur une organisation appropriée de l'équipe de développement (chez le fournisseur) et de l'équipe de suivi opérationnel ou de maintenance (chez l'utilisateur).

Conduite de la méthode

La LTI–AC est articulée essentiellement sur :

- la formalisation de règles de fonctionnement structurées faisant appel, au sein de l'organisation interne à l'industriel ou à l'exploitant, à différentes compétences dans le cadre du programme ou du projet concerné,
- l'existence d'une documentation appropriée,
- la mise en œuvre d'outils de gestion des incidents et de banques de données,
- la réalisation d'expertises approfondies pour analyser les incidents et en déterminer les causes.

Les incidents étant enregistrés au fur et à mesure de leur apparition dans la base de données, un objectif majeur de la LTI–AC est de déterminer ceux qui laissent présager un caractère reproductible afin d'en rechercher les causes et de pouvoir y remédier. Il convient à cet effet de :

- favoriser le degré d'investigation sur les causes de tous les incidents, même s'ils ne sont pas critiques pour le programme (ou la qualité de service),
- classer chaque cause d'incident selon deux types de critères,
- cause assignable (incident a priori reproductible),
- cause non assignable (incident fortuit),
- décider des incidents sur lesquels les investigations doivent être plus approfondies,
- décider des incidents pour lesquelles des actions correctives devront être engagées,
- élaborer en temps utile les actions correctives appropriées,
- vérifier l'efficacité de ces actions correctives (après un délai suffisant de temps opératoire après leur incorporation).

Une clé de l'efficacité de la LTI–AC réside dans la structure même de la base de données et dans la nature des informations saisies. Ces informations sont saisies dans la base de données avant d'être complétées par les investigations ultérieures.
Des analyses de défaillance peuvent être menées à différents niveaux et nécessitent parfois la participation d'un fournisseur de composant ou d'un module spécifique acheté en l'état. Les analyses de défaillance sont en principe demandées dans le cas des incidents les plus critiques (ex : incidents de nature récurrente, incidents difficiles à réparer, incidents mettant en jeu la sécurité…).

La base de données, cœur de la LTI–AC, permet l'émission de documents de synthèse périodiques nécessaires au système de gestion des incidents :

- historique des incidents enregistrés sur une période donnée,
- livret des points critiques,
- indicateurs de croissance de fiabilité,
- les histogrammes et diagrammes de Pareto…

Domaine de pertinence

- Mise en œuvre chez le fournisseur sur toute la phase de conception dès que les premières maquettes ou prototypes du produit sont disponibles, et en phase de production,
- Mise en œuvre chez l'exploitant en phase d'exploitation et de retrait de service, sous la responsabilité de l'exploitant qui est en mesure de l'alimenter, via le retour d'expérience, à partir des incidents générés au cours de ces phases.

Entrées	Sorties
- Données sur les défaillances observées (via les fiches d'incidents), - Résultats d'expertise.	- Actions correctives envisagées, - Indicateurs de croissance de fiabilité, histogrammes, - Evolution des procédures de maintenance, - Livret des points critiques.

Avantages	Inconvénients
- Identifier et corriger les causes de dysfonctionnement avant la mise en production, - Elément-clé de la croissance de croissance de fiabilité.	- Nécessite une organisation de projet structurée, - En phase d'utilisation du produit, difficulté de connaître les durées d'utilisation.

Bibliographie

1. **RE Aéro 703 0**6 : « Guide pour le pilotage de la croissance de fiabilité »,
2. **RG Aéro 000 33** : « Logique de traitement des incidents dans le cadre d'un programme »,
3. **MIL STD 2155**: « Failure Reporting, Analysis & Corrective Action System (FRACAS) »,
4. **DGA/AQ 6008** : « Guide pour le pilotage de la croissance de fiabilité »,
5. RAC Reliability Toolkit (commercial practices edition).

Coût de Cycle de Vie (CCV), Coût global de possession (CGP)

Terme lié : Life Cycle Cost (LCC)

Objectif *(à quoi ça sert ?)*

L'analyse du Coût de Cycle de Vie (CCV) vise l'optimisation prévisionnelle et la maîtrise du coût global de possession d'un produit, d'une machine ou d'une installation. C'est une donnée économique destinée à faciliter les choix stratégiques de conception et de développement du produit ainsi que le contrôle de sa gestion.
La conception à coût global objectif constitue un outil méthodologique essentiel dans cette approche.
Cette analyse permet d'orienter les études de sûreté de fonctionnement, les études de maintenance et de soutien logistique intégré.

Description *(que produit la méthode et comment ?)*

L'analyse de CCV est une démarche qui vise à guider les prises de décision des concepteurs et des acheteurs par une vision aussi large que possible des coûts induits par l'équipement en question depuis son acquisition jusqu'à son démantèlement. Elle permet de mettre en évidence les centres de coût les plus importants.
La démarche peut être structurée en 4 étapes :

- Plan d'analyse du CCV : domaine d'application, objectif, résultats attendus,
- Développement du modèle de CCV : niveau d'analyse, phases du cycle de vie, arborescence des coûts, catégories de coûts,
- Analyse du modèle de CCV : collecte des informations,
- Gestion de l'analyse du CCV : documentation, analyse des résultats, mise à jour.

Conduite du processus *(comment le met-on en œuvre ?)*

L'analyse du CCV consiste à chiffrer de manière prévisionnelle les coûts liés aux diverses phases du cycle de vie du produit :

- Expression du besoin,
- Conception préliminaire,
- Conception détaillée et qualification,
- Industrialisation,
- Production,
- Utilisation,
- Retrait de service.

Chacune de ces phases est génératrice de coûts. La maîtrise du CCV concerne l'ensemble de ces phases. L'analyse doit être conduite dès les phases amont car celles-ci induisent des coûts sur les phases de développement, de production et d'utilisation.
Le CCV se calcule à une date donnée et pour une période de référence définie. On doit raisonner en termes de coûts actualisés du fait que les durées prises en compte sont assez importantes (durée de vie du produit).

Domaine de pertinence

- En conception, la démarche permet de faire des choix de conception par l'identification des facteurs influents,
- En cours d'exploitation, la démarche permet d'orienter les décisions de gestion de l'installation à partir de l'évolution des coûts énergétiques, l'augmentation de la charge de maintenance, tout comme la baisse de performance de l'installation.

Entrées	Sorties
- Phases du cycle de vie, - Catégories de coûts (main d'œuvre, matière, énergie…), - Collecte des éléments de coût, - Performances de sûreté de fonctionnement, - Durée de référence concernée…	- Evolution des coûts d'exploitation, - Coût moyen sur une période de référence donnée, - Centres de coûts les plus importants…

Avantages	Inconvénients
- L'analyse CCV permet la mise en évidence des principaux inducteurs de coût (énergie, fiabilité, maintenance…), - Elle apporte une vision globale et permet une prise de décision justifiée.	- Le réalisme de l'analyse CCV dépend de la pertinence des prévisions de fiabilité, d'évolution des prix, d'impact des défaillances…

Bibliographie

1. **XP X 50.155** : Management par la valeur – Coût global – Décembre 1997
2. **CEI 60-300-3-3** : Dependability management – Application guide – Life cycle costing – Juillet 2007

Glossaire

Acronyme français	Définition	English acronym	Definition
A.A.D.	Analyse par Arbre de Défaillances	**F.T.A.**	Fault Tree Analysis
A.A.E.	Analyse par Arbre d'Evénements	**E.T.A.**	Event Tree Analysis
A.E.E.L.	Analyse de l'Effet des Erreurs du Logiciel	**S.E.E.A**	Software Effect Error Analysis
A.F.E. / A.F.I.	Analyse Fonctionnelle Externe / Analyse Fonctionnelle Interne	**F.A.**	Functional Analysis
A.M.D.E.	Analyse des Modes de Défaillances et de leurs Effets	**F.M.E.A.**	Failure Mode and Effects Analysis
AMDEC	Analyse des Modes de Défaillances de leurs Effets et de leur Criticité	**F.M.E.C.A.**	Failure Modes, Effects and Criticallity Analysis
A.P.R.	Analyse Préliminaire de Risques	**P.H.A.**	Preliminary Hazard Analysis
A.R.P.I.C.–M.	Analyse des Risques, Points Critiques pour leur Maîtrise	**H.A.C.C.P.**	Hazard Analysis Critical Control Point
A.S.L.	Analyse du Soutien Logistic		
B.D.F.	Blocs Diagrammes de Fiabilité	**R.B.D.**	Reliability Block Diagram
C.C.V.	Coût de Cycle de Vie	**L.C.C.**	Life Cycle Cost
CdCF	Cahier des Charges Fonctionnel		
C.G.P.	Coût Global de Possession	**G.C.O.**	Global Cost of Ownership
		C.M.M.I.	Capability Maturity Model® Integrated
COTS	Composant sur étagère		Component Of The Shelf
FARADA			FAilure RAte DAta bank
F.M.D.S.	Fiabilité, Maintenabilité, Disponibilité, Sécurité	**R.A.M.S.**	Reliability, Availability, Maintainability, Safety
		F.O.R.M. / S.O.R.M.	First Order Reliability Methods / Second Order Reliability Methods
HAZOP	Etude de danger et d'opérabilité	**HAZOP**	Hazard and Operability study
I.C.S.	Intégration Conception et Soutien		
		I.E.E.E.	Institute of Electrical and Electronics Enginners
ISdF	Institut de Sûreté de Fonctionnement		
L.T.I.–A.C.	Logique de Traitement des Incidents et Actions Correctives	**F.R.A.C.A.S.**	Failure Report And Corrective Action System
M.A.C.Q.	Méthodes de l'Arbre des Conséquences et Qualité		
M.B.F.	Maintenance Basée sur la Fiabilité	**R.C.M.**	Reliability Centered Maintenance
M2OS	Management, Méthodes Outils, Standards		

Acronyme français	Définition	English acronym	Definition
M.T.B.F.	Temps moyen entre défaillance	**M.T.B.F.**	Mean Time Between Failure
M.T.T.F.	Temps moyen avant première défaillance	**M.T.T.F.**	Mean Time To Failure
M.T.T.R.	Temps moyen de réparation	**M.T.T.R.**	Mean Time To Repair
O.M.F.	Optimisation de la Maintenance par la Fiabilité	**R.C.M.**	Reliability Centered Maintenance
		R.A.D.C.	Rome Air Development Center
		S.E.I.	Software Enginnering Institute
		S.I.L.	Safety Integrated Level
S.L.I.	Soutien Logistique Intégré	**I.L.S.**	Integrated Logistic Support
		S.P.I.C.E.	Software Process Improvement Capability dEtermination
		S.R.C.	System Reliability Center

Page volontairement blanche