

La gestion des RISQUES TECHNIQUES (Sûreté de Fonctionnement) et des RISQUES DE MANAGEMENT

A. Heurtel
CNRS IN2P3/LAL
Version 2.4 11/12/03

Table des matières

TABLE DES MATIERES	2
1 1^{ERE} PARTIE : LA SURETE DE FONCTIONNEMENT (SDF).....	4
1.1 Enjeux	4
1.2 Introduction	4
1.3 Définitions	5
2 LE PHASAGE DES ANALYSES DE RISQUES TECHNIQUES AVEC LE CYCLE DE VIE D'UN PRODUIT	6
2.1 L'identification du risque par la définition et l'analyse préliminaire des risques	6
2.2 La classification hiérarchique des risques suivant leur importance	6
2.3 L'acceptation ou le traitement des risques après analyse de fiabilité	7
2.4 L'Analyse des conséquences pour l'instrument	7
2.5 En pratique	7
3 LA MAITRISE DE LA CONCEPTION.....	8
3.1 Par l'Analyse de la Valeur (<i>Value Analysis</i>)	8
3.1.1 Les caractéristiques du besoin :	8
3.1.2 Les différentes phases de l'Analyse de la Valeur (AV) :	9
3.2 Par des analyses complémentaires en phase de design	11
3.2.1 Marges en conception: analyse des contraintes subies par les composants (derating) :	11
3.2.2 L'analyse Pire Cas (Worst Case Analysis):	11
3.3 Documentation :	12
4 L'ANALYSE PRELIMINAIRE DE RISQUES (APR) (<i>PRELIMINARY RISKS ANALYSIS</i>).	14
4.1 La mesure du risque	14
4.2 La méthodologie de l'analyse	15
4.3 Documentation :	15
5 LA LISTE DES ELEMENTS CRITIQUES (<i>CRITICAL ITEM LIST</i>)	17
5.1 Définition	17
5.2 La méthodologie de l'analyse	17
5.3 Documentation	21
6 LA FIABILITE (<i>RELIABILITY</i>).....	22
6.1 Objectifs, méthodes et conditions.	22
6.2 Modélisation et évaluation des systèmes	22
6.2.1 Principaux concepts:	22
6.3 Les méthodes de modélisation et de traitements	23
6.3.1 Les Blocs Diagrammes de Fiabilité (BDF) :	23
6.3.2 Le graphe de Markov :	26

6.3.3	La détermination de λ :	26
6.3.4	La simulation de Monte-Carlo :	27
6.3.5	Les réseaux de Petri :	27
6.3.6	Les analyses de sécurité par arbres d'événements (ou arbre de causes, arbre de défaillances ou arbre de fautes) :	28
6.4	Les règles de conception :	29
6.5	Bibliographie	29
7	L'ANALYSE DES MODES DE DEFAILLANCE, DE LEURS EFFETS ET CRITICITES (AMDEC OU FMECA).....	30
7.1	Méthodologie	30
7.2	Les rubriques de la feuille d'analyse :	30
7.3	Documents complémentaires pour le domaine spatial :	31
7.3.1	La méthode de Détection, d'Isolément et de Recouvrement des fonctions après Panne (FDIR)	31
7.3.2	L'Analyse des Interactions Software Hardware (HSIA).	31
7.4	Documentation.	31
8	LES OUTILS.....	33
1	2^{EME} PARTIE : LES RISQUES DE MANAGEMENT.....	35
1.1	Les critères de la check-list :	35
1.2	La check-list	35
1.2.1	Risques socio-économiques : Dégradation du climat social	35
1.2.2	Risques économiques : Tout contrat (convention) doit être pesé avant signature	35
1.2.3	Risques politiques et périodes d'instabilité d'un pays	36
1.2.4	Risques géographiques :	36
1.2.5	Risques réglementaires :	36
1.2.6	Risques contractuels :	36
1.2.7	Risques organisationnels :	36
1.2.8	Risques techniques	37
1.3	Remarques générales :	38
1.4	La Méthode des 5M (diagramme d'Ishikawa)	38
1.4.1	Le Milieu ou l'environnement	38
1.4.2	La Matière (en temps que support)	38
1.4.3	La Main d'œuvre (le personnel)	39
1.4.4	Le Matériel et les Moyens :	39
1.4.5	Les Méthodes (d'organisation)	39

1 1^{ERE} PARTIE : LA SURETE DE FONCTIONNEMENT (SDF)

1.1 Enjeux

La découverte tardive d'une erreur de conception peut induire un risque technique lourd de conséquences, et entraîner des surcoûts et des retards parfois importants pour le projet. L'apparition du risque peut aussi conduire à la mise en cause de la sécurité des personnes et des biens, à la dégradation de l'environnement, à la perte de fonctions ou tout simplement à la dégradation de l'image de marque.

Il faut donc **identifier** les risques au plus tôt, dès les revues d'opportunité, dans le cycle de fabrication d'un produit.

Le présent document propose de décrire la démarche qui est mise en œuvre pour *maîtriser* les risques d'un projet. Il montre aussi, à l'aide d'exemples (extraits des documents produits pour l'instrument HFI du satellite Planck, traduits de l'anglais), comment initier puis conduire cette méthodologie en laboratoire.

1.2 Introduction

La **Sûreté de Fonctionnement** est une activité d'Ingénierie qualitative et quantitative. La part qualitative correspond à l'optimisation des études au Bureau d'Etudes; elle représente 70% environ de l'activité totale. Les 30% restants représentent la partie dite quantitative qui est consacrée à la maîtrise des risques avant fabrication à partir des architectures déjà élaborées. C'est donc la phase d'optimisation des architectures des systèmes et de leur mise en œuvre de façon à maximiser, à moindre coût, leur robustesse aux aléas.

La Sûreté de Fonctionnement est donc une action de réduction de risques et, par voie de conséquences, du coût à l'achèvement. Elle s'exerce donc essentiellement pendant les premières phases des projets, jusqu'à la mise en production.

Cette démarche est une partie de la démarche générale qui, depuis quelques années, est mise en œuvre pour contrôler la fabrication d'un produit ou d'un instrument donné, que l'on désigne sous le nom d'Assurance Produit.

1.3 Définitions

Le risque est caractérisé par une grandeur à deux dimensions nommée « *criticité* » (fig. 1.3) :

- en abscisse : la « *sévérité* » des effets et des conséquences (parfois appelée aussi « *gravité* », ce dernier terme ne devant être considéré que comme un terme général).
- en ordonnée : « *la probabilité d'occurrence* », qui peut être quantifiée.

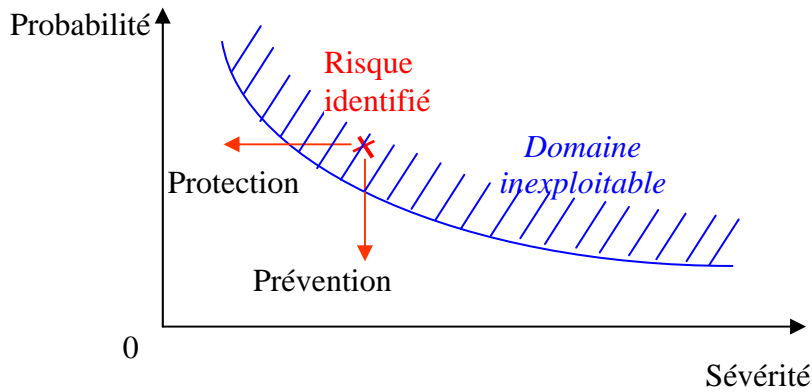


Fig. 1.3

Ainsi, la SdF s'exerce à la fois sur la prévention et la protection.

2 LE PHASAGE DES ANALYSES DE RISQUES TECHNIQUES AVEC LE CYCLE DE VIE D'UN PRODUIT

C'est dès la conception d'un produit que débute la politique de gestion et de maîtrise des risques techniques liés à son utilisation. Le design est vérifié plusieurs fois lors de réunions ou de revues, avant la mise en fabrication.

Quatre étapes majeures pour la maîtrise des risques :

- **L'identification des risques après analyses,**
- **Le classement en fonction de leur importance pour le projet,**
- **L'acceptation ou traitement,**
- **L'analyse des conséquences sur le projet.**

A noter que la maîtrise des risques, si elle accroît les coûts de conception, aura un impact compensateur par la réduction drastique des coûts de production, de mise au point et d'exploitation.

RAPPEL IMPORTANT : L'EXPRESSION DE BESOIN

Le besoin est établi en commun entre les différents partenaires au cours de groupes de travail. Il peut être mis en forme à l'aide de techniques.

Trois techniques couramment utilisées pour identifier et formaliser le besoin :

- L'établissement du Cahier des Charges Fonctionnel (CdCF),
- l'Analyse de la Valeur (AV),
- l'Analyse Fonctionnelle Interne (AFI).

2.1 L'identification du risque par la définition et l'analyse préliminaire des risques

Après l'étape d'expression et de formalisation du besoin, l'Analyse Préliminaire de Risques (APR), est la première étape de la politique de maîtrise des risques mise en œuvre dans un projet. Elle s'appuie sur l'Analyse Fonctionnelle Interne (AFI) (cf. tableau 3.1.4.) des différents sous-systèmes. En pratique, c'est l'établissement de la liste des pannes fonctionnelles possibles et des recommandations formulées pour le design. Cette liste préliminaire est établie en fin de phase A.

2.2 La classification hiérarchique des risques suivant leur importance

Les risques issus de l'analyse préliminaire sont classés suivant leur importance. Les plus importants pour le projet constituent la Liste des Eléments Critiques. Cette liste, établie en début de phase B, sera réduite au fur et à mesure de la clôture des actions mises en œuvre pour réduire ces risques. La Liste des Eléments Critiques accompagne le projet jusqu'à la mise en service de l'appareillage (voir §5).

2.3 L'acceptation ou le traitement des risques après analyse de fiabilité

Des analyses comparatives de fiabilité sont faites à partir de différentes modélisations du design pour diminuer la probabilité de défaillance. Elle vont conduire à explorer la possibilité de redondances, qui est le doublement des moyens matériels et/ou en logiciels de bord. Ces analyses permettent de décider de les traiter ou de les accepter.

2.4 L'Analyse des conséquences pour l'instrument

En fin de phase B, la caractérisation détaillée des effets de toutes les pannes possibles sur l'instrument et les actions menées pour y remédier ou en diminuer la sévérité est faite. La méthode utilisée est normalisée : c'est l'Analyse des Modes de Défaillances, de leurs Effets et Criticités (AMDEC). Elle est limitée dans un premier temps aux pannes fonctionnelles.

Elle constitue un auto-test de l'instrument avant sa mise en fabrication.

2.5 En pratique

Le niveau d'intervention sur les risques relève d'une décision du Projet en fonction des demandes des commanditaires mais aussi des ressources et des moyens dont il dispose.

Néanmoins le Chef de Projet doit avoir obtenu l'aval du Comité de pilotage sur sa politique de gestion des risques tout au long du projet. Le RAP est alors le garant de la mise en application de ces directives au sein du projet.

3 LA MAITRISE DE LA CONCEPTION

3.1 Par l'Analyse de la Valeur (*Value Analysis*)

L'Analyse de la Valeur (AV) est une méthode qui permet de tendre vers l'optimisation de la conception. Elle est pratiquée au niveau des sous-systèmes. Lui sont parfois associées des analyses complémentaires, telles que l'Analyse des Contraintes et l'étude du Pire Cas (cf. §3.2.2.).

C'est une méthode de travail normalisée par l'AFNOR, qui la définit comme une « *méthode de compétitivité organisée et créative visant les satisfactions des utilisateurs par une démarche de conception à la fois fonctionnelle, économique et pluridisciplinaire* ». Cette démarche est :

- fonctionnelle, car elle impose d'exprimer le besoin en terme de **finalité** et non de solutions,
- économique, car elle permet d'intégrer très tôt les aspects coûts,
- pluridisciplinaire, car elle fait intervenir un groupe de travail destiné à établir un consensus autour des fonctions à développer, de leurs performances, des solutions, des coûts. Elle favorise la créativité et permet un enrichissement mutuel des différentes personnes du groupe de travail.

L'objectif est de rendre « compétitif » un produit ou une réalisation :

- d'un point de vue fonctionnel, en termes de services rendus : c'est ce qui est aussi appelé **fonctions d'usage**.
- d'un point de vue technologique, en termes d'innovation et d'intégration: ce sont les **fonctions de construction**.
- en terme de coût (**fonction coûts**)
- la **fonction "pertinence du besoin"**, qui est la "valeur ajoutée" à la fonction.

3.1.1 *Les caractéristiques du besoin :*

- le besoin doit être connu et justifié (juste nécessaire) et obtenu à la suite d'adéquations et d'itérations,
- seule, sa finalité est exposée avant l'analyse, aucune solution n'étant formulée à ce stade,
- le niveau d'exigences doit pouvoir être modulé, dans une certaine mesure, en favorisant le dialogue avec les sous-traitants.

3.1.2 Les différentes phases de l'Analyse de la Valeur (AV) :

L'AV se déroule suivant 7 phases consécutives, distinctes. Le Tableau 3.1.4 montre l'ordonnement de la démarche.





Phases	Activités de la phase
Phase 1 Orientation de l'action	- Validation de l'action prévue, - Définition des objectifs et des limites de l'action, - Définition des contraintes et des moyens.
Phase 2 Recherche de l'information	Inventaire, mise en commun (et en forme) des besoins et informations dans les domaines: Economique, technique et réglementaire.
Phase 3 a)- Traduction des besoins connus en fonctions (avec prise en compte des coûts) :  Expression Fonctionnelle de Besoin. ----- b)- Recensement des fonctions. Résultats consignés dans le  Cahier des Charges Fonctionnel ----- c)- Travail sur les fonctions	Besoin connu et justifié ----- -Analyse des différentes fonctions * <i>techniques</i> (innovation et intégration (construction), * <i>service rendu</i> (usage) converti en fonctions techniques,, * <i>coût</i> , * <i>pertinence du besoin</i> (valeur de la fonction) - Recherche intuitive de fonctions , analyses des insatisfactions des produits etc.. ----- - Mise en forme des fonctions : formuler avec des verbes à l'infinitif, - Flexibilité, - Classement des fonctions (Hiérarchisation).
Phase 4 Recherche d'idées et de voies de solution (phase créatrice) par :  Analyse Fonctionnelle Interne	- Exploration des solutions possibles (arborescence fonctionnelle), - Hiérarchisation des idées de solutions, - Sélection d'idées par sous-systèmes et conséquences, - Nouveaux besoins, - Identification des risques, - Reconstruction des risques au niveau supérieur.
Phase 5 Etude et évaluation des solutions	Etude technique des solutions retenues (faisabilité, coût, risques).
Phase 6 Bilan prévisionnel, Présentation des solutions, Décisions.	- Elaboration du bilan  Présentation et justification des solutions,
Phase 7 Réalisation, suivi, bilan	Réalisation, suivi de la réalisation.

Tableau 3.1.4

Phase 1 : *L'orientation de l'action* :

C'est la phase de validation de l'action avec la définition des objectifs, des moyens et de leurs limites.

Phase 2 : *La recherche d'informations* :

Pendant cette phase, on effectue l'inventaire, la mise en forme et la mise en commun des informations de nature économique, technique et réglementaire.

Phase 3 : *L'analyse des fonctions et des coûts* :

Cette phase est celle de l'expression du besoin, comme indiqué déjà au §3.1.3 et sa traduction en terme de fonctions. Le passage besoin/fonction se fait par la description des **liens attendus** entre le produit à concevoir ou à modifier, et son environnement.

Actions pratiques :

- recenser les fonctions de service sous forme de verbe à l'infinitif,
- caractériser leur possibilité de flexibilité et de modularité,
- ordonner les fonctions en les classant suivant la logique pourquoi/comment,
- les valoriser et les hiérarchiser selon leur importance,
- valider la liste après justification.

A ce stade du projet, les documents suivants découlent normalement de l'analyse :

- **L'Expression Fonctionnelle de Besoin (EFB)** suivant la norme NF X50-151, Décembre 1991 : Analyse de la valeur, analyse fonctionnelle - Expression fonctionnelle du besoin et cahier des charges fonctionnel
- Le **Cahier des Charges Fonctionnel (CdCF)** pour le sous-système considéré, s'il n'a pas déjà été écrit.

Phase 4 : *Recherche d'idées et de voies de solutions* :

C'est la phase créatrice qui permet d'explorer toutes les solutions potentielles, de les classer et d'en faire une pré-sélection.

Le document résultant de ces séances de travail en groupe, quand il est demandé par le projet, est l'**Analyse Fonctionnelle Interne (AFI)**.

Phase 5: *Etude et évaluation des solutions* :

Cette phase comprend :

- L'évaluation, (effectuée toujours en groupe de travail), et, en retour, de
- La vérification des solutions par l'**identification des risques**.
- La reconstruction des fonctions au niveau supérieur à celui considéré
- La validation des solutions retenues.

Les 3 dernières phases, qui sont liées entre elles par leur démarche, peuvent être conduites lors de la même séance de travail.

Phase 6: *Bilan prévisionnel* :

C'est la présentation et la justification des solutions retenues.

Phase 7 : *Mise en œuvre des solutions techniques retenues et suivi de réalisation* :

Cette phase s'étend jusqu'à la mesure des écarts par rapport à la spécification et comprend la traçabilité des résultats.

3.2 Par des analyses complémentaires en phase de design

Deux analyses complémentaires ayant trait surtout au design électronique peuvent être demandées par les responsables des projets, notamment dans le cas de projets spatiaux pour lesquels des normes spécifiques sont éditées. Ces normes sont les ECSS « European Cooperation for Space Standardisation » applicables aux projets ESA et CNES (cf. §3.3.).

3.2.1 Marges en conception: analyse des contraintes subies par les composants (derating) :

Le taux de charge maximum en fonctionnement permanent de chaque type de composant électronique est imposé par des normes. Les marges demandées sur les caractéristiques intrinsèques des composants doivent être strictement respectées pour tous les composants. Ainsi les grandeurs (la puissance dissipée par ex.), sont-elles mesurées et listées.

La fig. 3.2.1 montre un tableau d'analyse de contraintes appliquées à une résistance. Une contrainte de 0,32W au lieu de 0,25W permis, n'est pas admissible sans demande de dérogation au près de l'autorité de tutelle.

Réf	Type	Description	Paramètre	Contrainte max. de la norme	Taux de contrainte max.	Contrainte maxi applicable	Contrainte appliquée	Comment.
R1	RNC90 10k	Resist.à film métall. 0,02%	Puissance	0,5W	50%	0,25W	0,18W	OK
R1	RNC90 10k	Resist.à film métall. 0,02%	Puissance	0,5W	50%	0,25W	0,32W	Non conforme. Demande de dérogation

Fig. 3.2.1.

3.2.2 L'analyse Pire Cas (Worst Case Analysis):

Cette analyse est l'évaluation des performances du produit par rapport au besoin. Elle prend en compte les dérives des paramètres des constituants dues au vieillissement pendant la durée de vie. Les causes sont les jeux mécaniques, les radiations, l'effet de la température, les variations extrêmes des signaux d'entrée et des charges de sortie sur les composants etc.

Beaucoup de ces dérives sont maintenant données par les constructeurs des composants. A charge aux concepteurs de calculer, à partir des données précédentes, les contraintes maximales attendues en fin de vie et de les comparer avec celles données dans les normes.

Ceci permet de valider les marges du produit par rapport au besoin.

Trois méthodes peuvent être utilisées :

- l'étude analytique de la fonction de transfert du produit (ex: Calcul des dérivées partielles au point de fonctionnement nominal ou détermination du domaine de variation),
- la simulation de la fonction de transfert du produit quand elle est plus complexe à traiter d'un point de vue analytique,
- les essais, parfois destructifs, et l'analyse de leurs résultats.

A noter que ces analyses sont très lourdes et très coûteuses. Elles nécessitent d'être donc ciblées au plus juste.

La fig. 3.2.2 ci-dessous donne un exemple d'Analyse Pire Cas pour des résistances. La table donne les conditions maximales acceptables et le ΔR à prendre en compte pour d'une condition d'utilisation donnée.

Type de résistances	Caractéristiques imposées par la norme				Résultats de l'Analyse Pire Cas : Dérive calculée de la résistance (ΔR) à tenir compte dans le design.
	Contrainte maxi . sur la tension	Contrainte maxi . sur la puissance	Température max. pour la puissance nominale	Température max. admissible à puissance nulle	
Carbone	80%	50%	+70°C	+100°C	Dérive de $\pm 15\%$
Film métallique (RNC)	80%	50%	+125°C	+150°C	Dérive de $\pm 2\%$
Films de haute précision (RNC90)	80%	50%	+70°C	+125°C	Dérive de $\pm 0.1\%$

Fig.3.2.2. Résultats du calcul de l'Analyse Pire Cas pour 3 résistances de même valeur initiale (10k Ω), en fonction de leur nature et de leur précision. Le résultat, combiné en terme de dérive, est indiqué dans la dernière colonne. Il reflète les effets des coefficients de variation thermique différents et le fait que les taux de vieillissement sont différents selon les résistances.

3.3 Documentation :

- AFAV (Association Française pour l'Analyse de la Valeur)
<http://www.afav.asso.fr/>
- Ouvrage général : de l'Analyse de la valeur au management par la valeur Editions AFNOR 1998.
- Nombreuses normes AFNOR dont NF EN 12973 : Management par la valeur. Juin 2000

- Sur le site de l'ESA :

<http://www.ecss.nl/>

après demande d'autorisation de téléchargement en ligne. Les normes ECSS-E-10-05A : pour l'Analyse Fonctionnelle, ECSS-Q-60-11 et PSS-01-301 pour le "derating", et ECSS-Q-30-01 pour l'Analyse Pire Cas.

4 **L'ANALYSE PRELIMINAIRE DE RISQUES (APR) (*PRELIMINARY RISKS ANALYSIS*).**

L'Analyse Préliminaire de Risques est la première étape de la politique de gestion de risques, l'Analyse de la Valeur étant considérée comme une phase d'étude et non d'analyse de risques.

C'est une analyse **déductive** dont les objectifs sont :

1. de forcer le projet à pratiquer une décomposition fonctionnelle de base, de tout le concept de l'instrument, y compris les softs, pendant la phase de design,
2. l'identification des erreurs et des non-conformités de design en comparaison aux spécifications d'origine,
3. l'identification très tôt dans le déroulement du projet, des modes de pannes possibles et en particulier des pannes à effet catastrophique sur le système, ces dernières sont traitées en priorité,
4. l'apport de modifications pour réduire le nombre d'éléments critiques et, plus généralement, pour réduire les risques de pannes.

Les résultats attendus de l'APR :

1. une visibilité sur l'adéquation des spécifications déjà établies permettant la tolérance aux pannes,
2. une première idée sur la nécessité ou pas de redonder des sous-systèmes,
3. une première idée du fonctionnement en mode dégradé après une panne ou après une mise en sécurité pour danger.
4. une visibilité sur les dangers entraînés par les pannes,
5. une première justification des analyses de détail qui sont lourdes et coûteuses,
6. la mémorisation de la raison des choix techniques.

4.1 **La mesure du risque**

Le risque est évalué par l'analyste (la fonction analyste peut être partagée entre le chef de projet, l'ingénieur système et le RAP) qui estime sa « *sévérité* » en fonction des conséquences de la défaillance de la fonction considérée, tant pour le système que pour l'expérience. Elle s'exprime par un nombre allant de 1 et 5 :

1. « *catastrophique* » quand il y a perte de l'instrument,
2. « *grave* » quand la conséquence est la perte du dispositif,
3. « *majeur* » lorsqu'il y a perte d'un sous-système,
4. « *significatif* », pour la d'une fonction,
5. « *négligeable* » lorsque la défaillance n'entraîne pas de conséquences.

Nota :

- dans certaines normes de l'ESA, on constate que les risques 2 et 3 sont confondus et appelés « *critiques* ».
- dans l'APR, lorsque l'on détecte qu'une panne peut se produire, on ne prend en compte que sa « sévérité » et non sa probabilité d'occurrence. Cette dernière sera éventuellement évaluée par l'AMDEC. L'AMDEC peut entreprendre une analyse technique du composant, en tenant compte des conditions de sa fabrication et les probabilités de pannes qui y sont associées.

4.2 La méthodologie de l'analyse

La décomposition fonctionnelle, déjà réalisée (*lors de l'Analyse de la Valeur ou bien est-ce distinct ?*), de l'Arbre Produit, en considérant les phases opérationnelles. Elle est formalisée par un tableau dont les colonnes sont : (*cf. tableau 4.2.*)

1. N° issu de l'Arbre Produit,
2. les événements redoutés,
3. la sévérité des pannes prévisibles,
4. l'unité concernée,
5. les symptômes observables,
6. les actions de réduction de risques prévues en conséquences.

Cette étude est faite par le responsable Qualité (ou Assurance Produit) du projet en liaison avec le Chef de projet, l'Ingénieur Système et les responsables techniques des sous-systèmes et les responsables qualités (ou Assurance Produit) des sous-systèmes le cas échéant. Le document résultant est diffusé à l'ensemble du Projet.

L'APR n'est pas formalisée par des normes. Il en résulte que les résultats obtenus sont très dépendants de l'analyste, d'où l'importance de l'action collective évoquée ci-dessus.

Cette liste n'est pas réactualisée pendant le déroulement du Projet. Elle sert de base pour constituer la liste des éléments critiques.

La fig. 4.2, montre la première page de d'APR de l'instrument HFI du satellite Planck. On peut remarquer que l'une des pannes : rupture des tubes en fibre de carbone chargée de fibre de verre qui supportent l'instrument sur sa plate-forme, est effectivement catastrophique car elle entraîne la perte de l'instrument. Elle a la sévérité 1. Elle est dite « *Point de Panne Unique* ».

4.3 Documentation :

- Sécurité de Fonctionnement des systèmes industriels A. Villemeur Edition Eyrolles Paris 1987,
- Sur le site de l'ESA : l'ECSS-Q-30B « Dependability »

Arborescence fonctionnelle	Evènements redoutés	Sévérité	Unité concernée	Moyens d'observation	Actions de réduction de risques
1. SIGNAL SCIENTIFIQUE FROID 1.1. Répétitivité du signal	1- <u>Echantillonnage du ciel imparfaitement réalisé</u>	2	HFI-S/C		- Modélisation du télescope. Conditions de contrôle du pointage.
	2- <u>Dépointage</u>	3	HFI		- Contrôle du design, simulations. Tests de qualification spécifiques à prévoir.
	- <i>Forme du foyer du télescope non correctement optimisée</i>	3	HFI		- Plan de montage et de mise en place. Plan d'étalonnage. Assurance du positionnement correct avec LFI
	- <i>Erreur de positionnement par rapport à LFI</i>	3	HFI		- Plan d'alignement particulier et Plan d'étalonnage.
	- <i>Mauvais alignement des cornets avec le télescope</i>	3	HFI		
	- <i>Distorsions dues au dessin du télescope</i>	3	HFI-S/C		- Modélisation du télescope. Plan de test du télescope.
	- <i>Mauvais alignement des le long de la direction de scanning du ciel</i>	3	HFI		- Design, fabrication, simulations au sol pendant la phase d'étalonnage. Tests de qualification.
	- <i>Incertitudes sur les mesures de polarisation (fuites, polarisation croisée)</i>	3	HFI		- Design et fabrication des cornets. Plan de Développement à écrire. Tests de qualification.
	- <i>Non-similarité des faisceaux des voies d'observation</i>	3	HFI	TM	- Analyse de la chaîne électronique. Phase d'étalonnage et de contrôle en vol à prévoir. Tests spécifiques de qualification.
	- <i>Centre focal des cornets en dehors de l'axe focal de Planck</i>	3	LFI/HFI HFI		- Modélisation, étalonnage, Plan d'alignement.
3- <u>Dérèglements du Plan Focal dus au lancement</u>	3			- Assurance de la rigidité du positionnement de la liaison HFI/LFI	
4- <u>Rupture des tubes de liaison entre HFI et LFI qui le supporte</u>	1			- POINT DE PANNE UNIQUE : PERTE DE L'INSTRUMENT (Plan d'Assurance du collage des tubes)	
1.2- Signal scientifique/ disposition des cornets	1- Recouvrement et/ou mauvaise réponse spectrale	2	HFI	TM	- Contrôle du design, Application du Plan de Tests au sol
	2- Voies de détection non-similaires en sensibilité	3	HFI	TM	- Tests de qualité, compensation en vol
	3- Perte de fiabilité intrinsèque /temps	3	HFI	TM	- Tests de qualité, compensation en vol
	4- Mauvaise fréquence de modulation	3	HFI-S/C		- Application et vérification du Plan de Fréquences

Nota: S/C = spacecraft

FPU =Unité de Plan Focal

TM = envoi de télémesures

LFI = Autre instrument du satellite Planck

Fig. 4.2.

5 LA LISTE DES ELEMENTS CRITIQUES (*CRITICAL ITEM LIST*)

Cette liste n'est pas effectuée suivant une norme définie. Elle peut être exigée par les commanditaires du Projet. C'est la deuxième étape de la politique de gestion des risques entreprise tout le long d'un projet.

5.1 Définition

Au §4.1, la classification des risques a été donnée suivant les défaillances possibles lors du fonctionnement de l'appareillage :

Une autre manière d'aborder le traitement de risques est de spécifier les risques liés aux **éléments** en tant quels tels. C'est le but de cette liste.

Un élément est dit « *critique* » quand le risque qu'il entraîne est compris entre « *catastrophique* » et « *significatif* ».

De surcroît, un élément est « *critique* » quand il s'applique aux pièces :

1. non encore développées,
2. dont les propriétés ne peuvent être contrôlées directement sans dégradation,
3. localisées aux interfaces,
4. produites par des instituts non encore expérimentés dans les domaines concernés.

Il est aussi défini par deux critères :

1. la « *catégorie critique* » qui concerne :
 - A : la sécurité ou la probabilité de panne dans le temps,
 - B : la possibilité pour l'élément de se fracturer,
 - C : un élément dont la durée de vie est limitée.
2. sa « *criticalité* », répartie selon 2 groupes : Majeure (M) ou mineure (m), suivant la sévérité de la panne résultant du non fonctionnement de l'élément.

5.2 La méthodologie de l'analyse

La liste est faite sous forme de colonnes dont le format est le suivant :

1. numéro de ligne,
2. code produit (arbre produit),
3. catégorie critique,
4. criticalité,
5. identification précis de la pièce en question,
6. risques encourus,
7. activités prévues pour rendre la pièce, si possible, non critique (plans de contrôle etc.),
8. état : Ouvert ou Fermé

9. référence du document attestant la clôture du risque et sa date de parution.

Chaque groupe est responsable de ses propres actions de réduction de risques. La liste finale est le recueil de toutes les listes des sous-systèmes, remises au même format par le responsable de l'Assurance Qualité (ou de l'Assurance Produit) du projet. Il sollicite périodiquement les responsables des sous-systèmes pour sa mise à jour. La diffusion de cette liste est étendue à tout le projet.

La fig. 5.1, page suivante, montre, à titre d'exemple, la première page de la liste des éléments critiques de l'instrument HFI. Ce document a été validé par l'Agence Spatiale Européenne, après correction. Les documents indiqués en dernière colonne sont des documents existants, qui appartiennent à la base de donnée du satellite.

N°	Arbre produit	Catégorie critique	Criticalité	Élément	Risque	Activité de réduction prévue	Etat	Référence du document
REFROIDISSEUR A DILUTION (température de 0,1K) Actions à prendre en compte par l'Institut d'Astronomie Spatiale (IAS)								
1	PHAA	A	m	Alliage HoY	A qualifier pour une utilisation spatiale	Programme d'évaluation et de qualification à écrire	Fermé	ESA. TOS-QMC rapport 00/8
2	PHAA	A	M	Pièce en forme de "Té" recevant le refroidisseur à 18K	Pièce redondée. Mauvais contact thermique entre le réservoir LR1 et le refroidisseur à 18K	Programme d'évaluation et de qualification à écrire pour l'assurance de contact thermique et mécanique correct. <i>(Cyclage thermique dans N2 liquide, validation du fonctionnement, vibration à basse et température ambiante, re-test à 18K). A qualifier. Rapport à écrire.</i>	Ouvert	Dessin préliminaire réalisé
3	PHAABM	A SPF	M	Dispositif de maintien des étages à 0,1 et 4K pendant le lancement	Non ouverture en vol des 3 doigts de blocage	Un programme d'évaluation et de qualification a été écrit par le sous-traitant. <i>Tests début 2003</i>	Ouvert	Documents sous-traitant: /PRET/PN/SG/02.45 (0) DTA/PRET///SG/01.114(1) DTA/PRET/GA/SG/02.136
4	PHAABM	A	m	Vis sur les platines refroidies	Risque de desserrage à très basse température suivant les matériaux, la nature des vis et les couples de serrages appliqués.	Un programme doit être proposé pour calculer les couples et faire des essais.	Fermé	1- Action IAS: HFI_INST 000037 2- Procédure : Sap-GERES FM-0283-97 3-Procédure STD-91-01-IAS
5	PHAAAm	A	M	Entretoises en fibre de carbone chargée de résine polyester reliant HFI/LFI	- Mauvaise attaché dans les capuchons - Sensibilité aux vibrations à la diffusion thermique et incertitudes sur le comportement mécanique.	Programme d'évaluation et de qualification à écrire. Tests en cours	Ouvert	- Design: Note relatant le procédé de collage: AN-PHAAB-1000046IAS et PR-PHAAB-100005-IAS - Plan Test à écrire - Plan de Qualification à écrire
6	PHABC	A	m	Platine supportant les bolomètres	Mauvais centrage par rapport au Plan Focal	Design. Programme d'évaluation et de qualification à écrire pour le centrage par une méthode optique.	Fermé	1- Document d'interface fournir par l'équipe en charge 2- Directive sous-traitant A DTA/SYSO/PN/TN/02.105 3- Matrice de vérification DTA/SYSO//CA/TN/02.104
7	PHAC	A	m	"PID" sur la plaque des	Assemblage non correct dans	Programme d'évaluation et de qualification à écrire pour	Ouvert	

N°	Arbre produit	Catégorie critique	Criticalité	Élément	Risque	Activité de réduction prévue	Etat	Référence du document
				bolomètres (ou sous la plaque de dilution)	le temps (Décollage ou dévissage intempestifs)	vérifier l'assemblage des PID. <i>Plan de validation dans le cadre du programme de tests de l'instrument</i>		
8	PHAD	A	m	Isolation électrique du plan focal	Mauvaise optimisation de la cage de Faraday	Design. Programme d'évaluation et de qualification à écrire pour l'assemblage de la cage. <i>Analyse réalisée. Vérification du design. Plan de développement à écrire</i>	Ouvert	AN-PH215-200173-IAS PL-PH251-200168-IAS
9	PHEF	B	m	Refroidisseur par dilution	Fluctuations de température.	Assurance du fonctionnement correct de la dilution: Programme d'évaluation à écrire. <i>Tests prévus sur une maquette (02-2002)</i>	Ouvert	SP-PHACO-100044-IAS SP-PHAC212-200017-IAS PL-PHAC410-200013-IAS

Fig. 5.1

5.3 Documentation

Documents de l'Agence Spatiale Européenne (ESA) : ECSS-Q-20A « Quality Assurance », ECSS-Q-60A « Electrical, Electronic and Electrochemical Components », ECSS-Q-70A « Materials, Mechanical Parts and Processes ».

6 LA FIABILITE (*RELIABILITY*)

Les études de fiabilité constituent le moyen de quantifier les risques définis par l'APR et par la liste des éléments critiques. **La détermination de la probabilité d'occurrence des risques concernés va permettre de statuer sur l'opportunité de les traiter ou de les accepter.** C'est la 3^{ème} étape de la gestion de risques d'un projet.

6.1 Objectifs, méthodes et conditions.

L'objectif est d'évaluer différentes architectures possibles en comparant leurs performances au moyen de données statistiques. Pour ce faire, la méthode employée doit être suffisamment riche pour décrire le fonctionnement du produit, mais, cependant, la plus simple possible pour que le projet puisse contrôler l'évaluation qui est faite.

La méthode générique universelle pour faire ces études n'existe pas. Les limites sont d'une part l'utilisation abusive d'analyses quantitatives complexes pour justifier les risques qui sont difficiles à mesurer, et d'autre part, la tendance à rejeter toute quantification qui peut conduire à des architectures incohérentes. Cela reste un outil très utile d'évaluation relative des différentes solutions techniques.

6.2 Modélisation et évaluation des systèmes

6.2.1 Principaux concepts:

- La fiabilité **R** : (*Reliability*).

C'est l'aptitude d'un produit à accomplir une fonction requise pendant un intervalle de temps donné. C'est la probabilité que le produit ne soit pas défaillant sur l'intervalle (0,t). Elle est définie à partir du **taux de défaillance** λ qui varie avec le temps comme indiqué sur la courbe suivante de la fig. 6.2.1 (Courbe dite « en baignoire »).

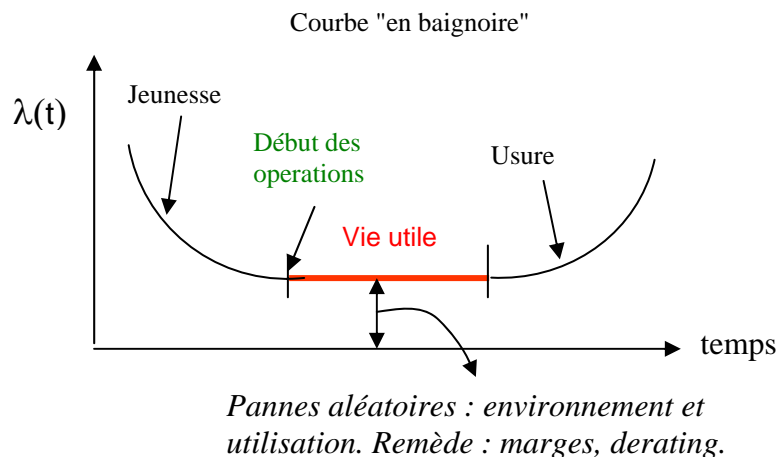


Fig. 6.2.1

On montre que pour un système, dont ce taux de défaillance est constant dans le temps, c'est-à-dire pendant la période de vie utile :

$$R=e^{-\lambda t}$$

- **La maintenabilité : (*Maintainability*).**

C'est l'aptitude d'un produit à être maintenu ou réparé. C'est la probabilité que la maintenance soit achevée à l'instant t, sachant que le produit est défaillant à l'instant initial.

- **La disponibilité : (*Availability*).**

C'est l'aptitude à accomplir une fonction requise à un instant donné, caractérisée par la probabilité que le produit ne soit pas défaillant à l'instant t.

- **La sécurité (*Safety*)**

C'est l'aptitude d'un produit à ne pas entraîner de dommages graves aux personnes, à l'environnement ou aux biens. Caractérisé par sa probabilité.

Remarque : Les 4 concepts que sont la **Fiabilité**, la **Maintenabilité**, la **Disponibilité**, et la **Sécurité**) sont des analyses qui sont souvent groupées, notamment dans les logiciels, sous le terme de **FDMS ou RAMS**.

- **Le fonctionnement se caractérise par les paramètres suivants :**

- **le MTTF (*Mean Time To Failure*)** : durée de bon fonctionnement avant la première défaillance ,
- **le MUT (*Mean Up Time*)** : durée moyenne de bon fonctionnement ,
- **le MDT (*Mean Down Time*)** : durée moyenne d'indisponibilité,
- **le MTTR (*Mean Time To Repair*)** : durée moyenne de réparation,
- **le MTBF (*Mean Time Between Failure*)** : durée moyenne entre 2 défaillances consécutives.

6.3 Les méthodes de modélisation et de traitements

L'évaluation repose sur l'emploi d'une méthode de modélisation couplée à une méthode de traitement.

6.3.1 Les Blocs Diagrammes de Fiabilité (BDF) :

Le BDF est une représentation des éléments qui participent à la réalisation des diverses fonctions d'un produit, sous la forme de blocs rectangulaires, en série ou parallèle, liés entre eux. Le fonctionnement est assuré tant que la chaîne n'est pas rompue par la défaillance de certains blocs. La fiabilité de la chaîne est calculée et différentes redondances sont simulées pour augmenter sa fiabilité.

Les types de redondances sont :

- la redondance active M parmi N : les N éléments en redondance fonctionnent simultanément, sachant que seulement M éléments sont nécessaires pour assurer le service attendu.
- la redondance passive M parmi N : M-N éléments sont des éléments de rechange.

- les redondances chaude/froide : Elles caractérisent l'état énergétique d'un système.
- le cross-strapping : qui partage les circuits en éléments redondés individuellement. Simple en apparence, en fait, il introduit le ralentissement des informations et des risques de non-fonctionnement qui sont liés à l'activation du commutateur.

Limite de la méthode : La BDF est une méthode simple, dont la symbolique s'est récemment enrichie pour tenir compte des taux de réparation après panne, des taux d'utilisation pour les éléments actifs, de ressources supplémentaires quand la redondance est activée. La modélisation doit se faire avec soin pour tenir compte à la fois des pannes dites « *Avant* » qui sont des fonctionnements intempestifs et des pannes « *Retard* » ou absence de fonctionnement.

La Fig. 6.2.3 ci-après montre un exemple de calcul de la fiabilité du circuit numérique du « Data Processing Unit » (DPU) ou Unité de traitement de données avant l'envoi des informations à terre du satellite Planck.

La représentation du DPU avec ses 4 interfaces (I/F) et le convertisseur DC/DC par la méthode des blocs diagrammes de fiabilité est montrée sur cette figure. Chaque bloc diagramme rectangulaire correspond à un ensemble de fonctions du sous-système et est traité en tant que tel. Les valeurs de λ sont données dans la littérature. La fiabilité du DPU ainsi calculée est 0,9538 pour 2 années de fonctionnement.

Dans la Fig. 6.2.4., on a considéré toute la chaîne électronique du satellite hormis la partie analogique de détection. Chaque ensemble de fonctions, auquel correspond physiquement un boîtier électronique, est représenté par un bloc diagramme, le DPU précédent, constituant un des sous-systèmes. La chaîne ainsi constituée est présentée sur la Fig.6.2.4. Deux versions sont présentées:

- L'une sans aucun élément en redondance. La fiabilité de la chaîne est 0,8676,
- L'autre avec 2 sous-systèmes en redondance (lecture des signaux de détecteurs d'une part et, d'autre part, traitement et acquisition numérique de la carte des signaux dans les conditions où il n'y a pas de cross-strapping). La fiabilité atteint maintenant 0,94043.

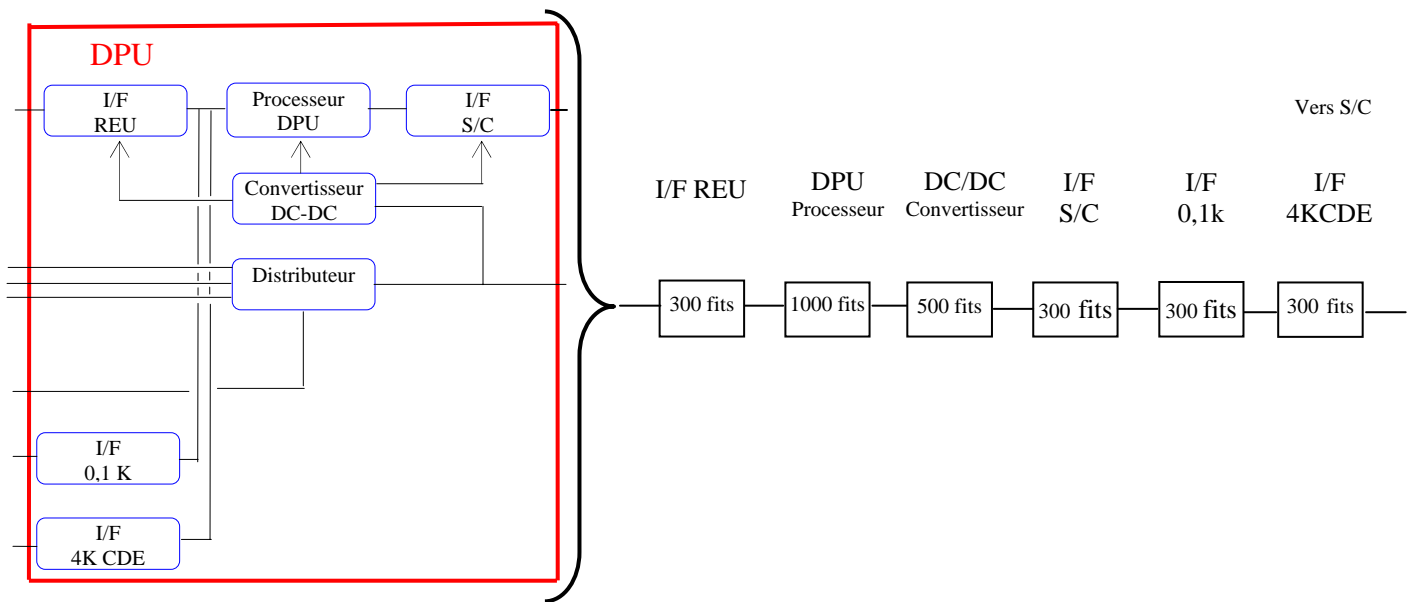


Fig. 6.2.3 Exemple de représentation d'un sous-système électronique par la méthode des blocs diagrammes. Le cadre carré de gauche appelé DPU (Unité de traitement de données) est représenté à droite par l'ensemble des petits rectangles reliés entre eux. Comme tous les éléments fonctionnent simultanément, ils sont donc représentés en série sur le schéma. Nota : Les valeurs de λ sont exprimées en fits (1 fit égal 10^{-9} pannes/h).

(Pour information, les autres acronymes des différents modules utilisés ici sont I/F : interface, REU : Unité de lecture électronique, 4KCDE : Commande d'électronique de refroidisseur à 4K, 0.1K : refroidisseur à dilution à 0,1K, DC/DC : Convertisseur à courant continu).

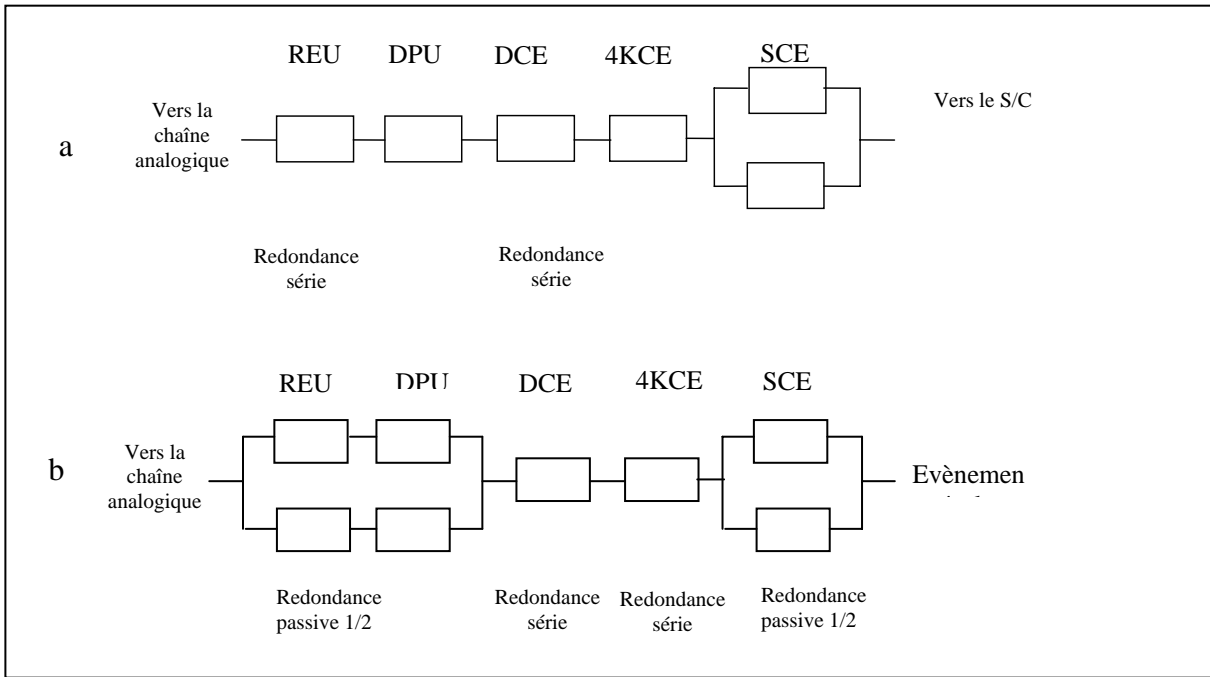


Fig. 6.2.4 Exemple de simulation de fiabilité: (a) sans et (b) avec redondance sans cross-strapping de la partie électronique d'un instrument. Chacun des modules est traité de la même façon que pour la figure 6.2.3. La fiabilité à 2ans passe de 0,8676 à 0,94043 en redonnant le couple de sous-systèmes REU/DPU. Cette configuration est celle qui a été réalisée.

6.3.2 Le graphe de Markov :

Le traitement du graphe consiste à calculer le **vecteur probabilité de trouver les différents états du système à t**. Il est utilisé pour décrire le comportement dynamique d'un produit par la représentation matricielle des états du système.

Cette méthode est maintenant combinée avec la précédente dans des logiciels de simulation. Cependant dans ce cas, il faut que les taux de transition entre états soient constants, ce qui exclut le fonctionnement quand le taux de pannes varie avec le temps (jeunesse des dispositifs ou fin de vie avec usure).

6.3.3 La détermination de λ :

Les résultats des calculs de fiabilité dépendent des valeurs des taux de fiabilité λ qui sont prises pour les calculs. Ces valeurs sont souvent tabulées. Cependant, elles n'existent pas toujours, notamment, dans le domaine de la mécanique. Ces tables indiquent parfois des valeurs différentes pour les mêmes composants électroniques, bien que les modèles prévisionnels soient maintenant recalés les uns par rapport aux autres. Un vaste champ de recherche s'est créé sous l'impulsion des industriels et est relayé par le monde universitaire et les écoles d'ingénieurs, sous forme de réseaux,

afin d'optimiser les méthodes de détermination de λ . Les facteurs pris en compte sont :

- le retour d'expérience et le traitement statistique qui lui est associé,
- les essais de fiabilité (tests de vie, cyclage thermiques, essais de fatigue) sous contrainte accélérée, suivant des modèles et des lois pré-établies,
- la physique des défaillances dans laquelle le mécanisme de défaillance est modélisé par une loi physique analytique,
- les avis d'experts,
- la prise en compte de paramètres empiriques ou prévisionnels etc.

D'une façon générale, les méthodes bayésiennes font intervenir des combinaisons de données statistiques basées sur la probabilité totale des différentes causes de nature diverses. Elles sont de plus en plus employées en simulation et diagnostic.

Deux autres méthodes sont en développement :

- Les algorithmes génétiques,
- Les réseaux de neurones.

6.3.4 La simulation de Monte-Carlo :

Elle est utilisée en SdF quand un système s'avère trop complexe pour pouvoir être traité par les 2 méthodes précédentes combinées. Son principe consiste à simuler un grand nombre de fois le comportement dynamique des composants d'un système afin d'évaluer ses caractéristiques de fonctionnement, en reconstituant l'état total.

Les inconvénients :

- la précision est liée au nombre de simulations effectuées,
- le traitement est long et peut difficilement s'appliquer aux événements rares
- la méthode peut faire l'objet de développements logiciels spécifiques contrairement aux méthodes précédentes qui utilisent des logiciels du commerce.

6.3.5 Les réseaux de Petri :

Un réseau de Petri est constitué de places, transitions et arcs, qui vont représenter successivement les propriétés du système à modéliser lors de ses changements d'état, à travers les relations place/transition.

Couplés à la simulation de Monte Carlo, ils permettent d'évaluer la fiabilité/disponibilité de systèmes divers et notamment dans le domaine de l'automatique et de la productique en considérant des transitions déterministes ou aléatoires.

Le pouvoir de modélisation de cette méthode est très riche, mais demande en contrepartie une grande maîtrise du processus de modélisation de la part de l'analyste qui doit en être expert.

6.3.6 Les analyses de sécurité par arbres d'événements (ou arbre de causes, arbre de défaillances ou arbre de fautes) :

Le but est de représenter graphiquement les combinaisons d'événements de base qui entraînent la réalisation d'un événement (risque) indésirable.

Ces événements de base peuvent être des pannes, des erreurs humaines, des conditions extérieures pour lesquelles des données probabilistes sont ou ne sont pas disponibles. Elles ont pour ordre le nombre d'événements qui les constitue. La représentation des événements et des portes logiques s'effectue par l'intermédiaire d'une symbolique synthétique. Le traitement mathématique permet de calculer la probabilité de l'arbre sommet lorsque des données probabilistes sont disponibles. Néanmoins, en pratique, cette méthode est délicate à appliquer pour des systèmes complexes.

La fig. 6.2.5 ci-dessous montre un exemple d'arbre d'événements conduisant à la perte d'un système. Les éléments sont représentés par des symboles (cercles, losanges, triangles, maison) auxquels sont associées des portes logiques : "et", "ou", "non-ou". On recherche la plus petite combinaison possible d'événements de base conduisant à l'événement au sommet. Dans le cas de cette figure, les événements de niveau immédiatement supérieur apparaissent si "d et non(g) et non(h)" se produisent ou de la même façon "e et non(g) et non(h)" et également "f et non(g) et non(h)" se produisent. 3 éléments sont à chaque fois mis en cause, la coupe est alors dite d'ordre 3. Nota: Pour un Point de Panne Unique, l'ordre est 1.

Dans le cas général, toutes les coupes minimales sont déterminées lors de l'analyse. Elles peuvent être ensuite classées par ordre d'importance et par probabilité.

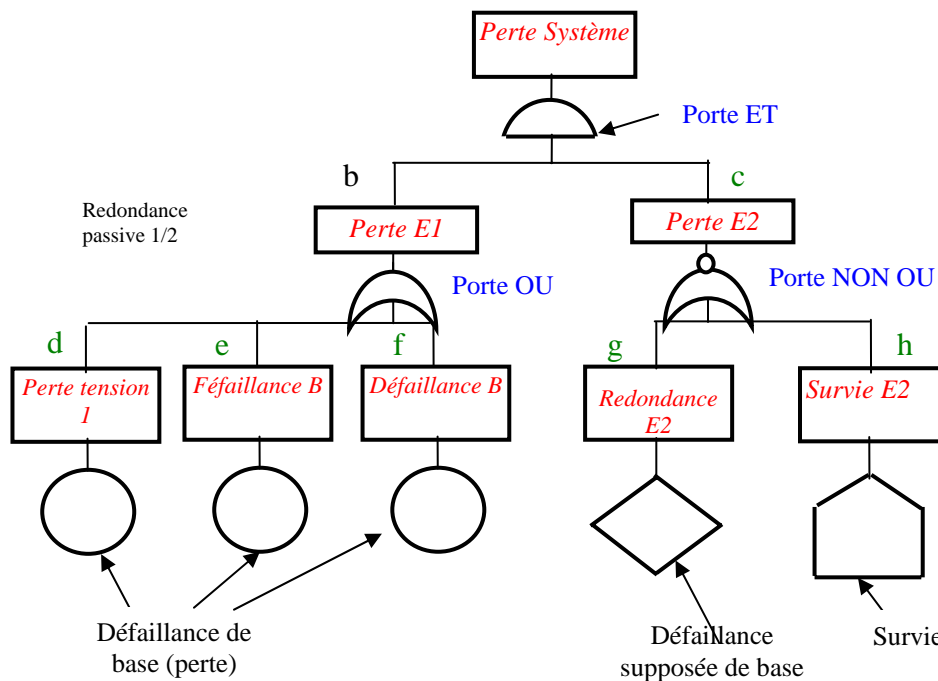


Fig. 6.2.5 Exemple de symboliques

6.4 Les règles de conception :

Les fonctions nominales et redondantes si elles doivent être implantées sur une même carte, doivent être séparées physiquement (éloignement sur la carte, séparation mécanique, drain thermique etc.), à moins que l'absence de risque de propagation de panne entre partie nominale et partie redondante ne soit démontré.

Les mécanismes de détection des pannes ou de protection doivent être indépendants des fonctions surveillées ou protégées.

6.5 Bibliographie

1- Ouvrages généraux :

- Fiabilité des systèmes : A. Pagès et M. Gougran Edition Eyrolles Paris 1980,
- Sûreté de Fonctionnement des systèmes industriels : A. Villemeur Edition Eyrolles Paris 1987
- Cours de Technologie Spatiale Vol1 Editions Cépadues Toulouse 1998
- Handbook of Reliability Engineering Editions Springer
- Les réseaux bayésiens : P. Naim et A. Becker Editions Eyrolles

2- Recueils de données pour la détermination de λ et modèles de fiabilité :

- MIL HDBK 217F du Department of Defense pour les composants militaires,
- RDF 99 du CNET (UTE 80810) pour les composants électroniques commerciaux,
- Lambdathèque du STPA-SOPEMEA GIFAS,
- Données du Reliability Analysis Centre (RAC),
- CABTREE: Saisie d'arbres de fautes

<http://perso.wanadoo.fr/andre.cabarbaye/fr/cabtree2.htm>

7 L'ANALYSE DES MODES DE DEFAILLANCE, DE LEURS EFFETS ET CRITICITES (AMDEC OU FMECA)

Cette analyse constitue la 4^{ème} étape de l'action en réduction de risques. C'est l'analyse **inductive** de recherche des **effets** des pannes des composants **sur les sous-systèmes et le système**.

La "*criticité*" qui est la probabilité d'occurrence des pannes, n'est pas calculée lorsque l'analyse s'effectue au niveau fonctionnel, ce qui est généralement le cas, sauf demande expresse du Projet (pannes intrinsèques des composants). Comme pour les autres étapes de la politique de gestion des risques techniques, les pannes sont donc caractérisées par leur composante « *sévérité* ». On parle alors d'AMDE. En fait, le sigle AMDEC est généralement usité, même lorsque la probabilité d'occurrence n'est pas calculée. *L'AMDEC dite composant, qui est l'étude de la probabilité de défaillance d'un composant suivant sa technologie n'est pas exposée ici.*

7.1 Méthodologie

L'AMDEC se pratique, comme l'Analyse de la Valeur, en groupe de travail dirigé par un animateur.

La méthode comprend 4 étapes que l'on va retrouver dans le formalisme :

- 1- une revue aussi détaillée que possible, à partir de l'APR, des possibilités de pannes (dégradation dans le temps ou rupture brutale) pour chaque fonction de l'équipement et des interfaces,
- 2- pour chaque panne identifiée, détermination des **causes** et des **effets** (dommages et interférences) sur les autres sous-systèmes en terme de « *sévérité* » (voir § 4.1),
- 3- la détermination des moyens de détection et de recouvrement de la fonction en question,
- 4- des propositions d'action pour supprimer la panne.

Particularités :

- pour les interfaces : l'analyse est détaillée jusqu'au niveau composant,
- l'AMDEC s'applique également aux logiciels et aux interfaces logiciels/matériel dès le début de l'écriture des logiciels et constitue une analyse spécifique complémentaire,
- les recommandations sont éditées sous forme de liste d'actions,
- les recommandations proposées peuvent être rejetées après étude et d'autres propositions faites en retour.

7.2 Les rubriques de la feuille d'analyse :

- 1- Le numéro d'ordre pour le sous-système considéré suivant l'arbre produit,
- 2- La fonction considérée,
- 3- Le mode de panne supposé (souvent plusieurs possibles par fonction),
- 4- La cause la plus probable de chaque panne,

- 5- Les symptômes observables : effet local,
- 6- Les symptômes observables : effet amont,
- 7- Les symptômes observables : effet final,
- 8- Les méthode de détection de la panne au niveau considéré,
- 9- La sévérité suivant §4.1
- 10- La méthode employée pour isoler la panne,
- 11- La méthode utilisée pour recouvrer la fonction en fonctionnement normal,
- 12- Les remarques et recommandations aux concepteurs.

A l'analyse est joint un tableau rassemblant les principaux modes de pannes et leurs conséquences. Il est souvent croisé avec la Liste des Eléments Critiques, qui est réactualisée en conséquences.

La fig. 7.2, montre une page de l'analyse AMDEC réalisée pour l'Unité de Traitement des Données (DPU) du satellite Planck. Cet exemple complète l'étude faite pour la redondance (Fig. 6.2.3 et 6.2.4). On voit, en particulier, que pour une même fonction de la RAM programme, qui concerne le stockage du programme d'application, 3 pannes systèmes ont été analysées (n°5, 6, 7). On constate que la sévérité de ces pannes varie fortement (de 1 à 4), avec pour 1, la nécessité de passer en redondance.

7.3 Documents complémentaires pour le domaine spatial :

7.3.1 *La méthode de Détection, d'Isolément et de Recouvrement des fonctions après Panne (FDIR)*

Les agences spatiales demandent que les méthodes de détection, d'isolement et de recouvrement des fonctions après pannes soient formalisées dans un document de synthèse. Cette analyse est déduite de l'AMDEC. Elle fait apparaître la logique de gestion des pannes.

7.3.2 *L'Analyse des Interactions Software Hardware (HSIA).*

Elle caractérise les risques dus à l'utilisation de logiciels avec le matériel, à chaque étage et pour chaque système. C'est aussi une analyse complémentaire, en grande partie déduite de l'AMDEC, dont il reprend le formalisme.

7.4 Documentation.

- Normes NFX60-510, CEI 812,
- ESA ECSS-030-02A FMECA,
- Juran's Quality Handbook, Ed Mac GrawHill (ISBN-0-07-0340023-X)
- Méthodes et outils de gestion qualité WEKA (ISBN-2-7337-0139-8)
- MIL-STD-1629A Military Standard Procedures for performing a failure mode, effects and critically analysis,

Nu m.	Élément	Fonction	Mode de panne supposé	Cause la plus probable	Effets locaux	Effet au niveau suivant	Effets finaux	Méthode de détection des pannes	Sévérité/Redondance	Méthode d'isolation	Méthode de recouvrement en vol	Remarques/Recommandations
1	PROM de boot	Stockage du programme de boot	Défaillance permanente mot/bit		Lecture erronée d'une instruction	Crash du programme de boot ou mauvaise exécution	Unité de traitement de données hors d'usage	Absence de communication - watchdog	1	Non	Redondance	Faible probabilité d'occurrence
2	PROM de boot	Stockage du code du programme de boot	Défaillance permanente d'un bloc/composant		Lecture erronée d'une instruction	Crash du programme de boot ou mauvaise exécution	Unité de traitement de données hors d'usage	Absence de communication - Watchdog.	1	Non	Redondance	Faible probabilité d'occurrence
3	EEPROM	Stockage de la version par défaut et de la nouvelle version du programme d'application (code et constantes)	Défaillance permanente mot/bit		Perte de l'intégrité du soft de bord			Checksum d'erreur	4	Non	Correction d'erreur	
4	EEPROM	Stockage de la version par défaut et de la nouvelle version du programme d'application (code et constantes)	Défaillance permanente d'un bloc/composant		Non stockage de version(s) du soft de bord	Cas 1 : pas d'exécution du programme d'application après reset	Fonctionnement de l'instrument en mode dégradé	Checksum d'erreur	3	Non	Envoi d'un patch du programme d'application en RAM après chaque reset	Pas d'espace pour le programme d'application
5	RAM programme	Stockage du programme d'application	Basculement temporaire d'un bit	Upset d'un évènement simple (SEU) (<i>ion lourd</i>)	Lecture erronée d'une instruction	Mauvaise exécution ou crash du programme d'application		Watchdog – Test du programme de boot	4	Non	Reset du watchdog RAM et processeur	
6	RAM programme	Stockage du programme d'application	Défaillance permanente d'un bloc étroit		Lecture erronée d'une instruction	Mauvaise exécution ou crash du programme d'application		Watchdog – Test du programme de boot	4	Non	Rechargement du programme d'application	
7	RAM programme	Stockage du programme d'application	Défaillance permanente d'un bloc étendu		Lecture erronée d'une instruction	Mauvaise exécution ou crash du programme d'application	Unité de traitement de données hors d'usage	Watchdog – Test du programme de boot	1	Non	Redondance	Le programme de boot ne peut envoyer que des paquets de diagnostic
8	RAM de données	Stockage de variables et de constantes	Basculement temporaire d'un bit	Upset d'un évènement simple (SEU)	Mauvaise lecture de données			Contrôle de parité	4	Marquage des données corrompues	Reset du processeur et de la RAM si besoin	
9	RAM de données	Stockage de variables et de constantes	Défaillance permanente d'un bloc étroit		Mauvaise lecture de données			Contrôle de parité	4	Non	Rechargement des données	Interdiction d'accès au bloc concerné

Fig. 7.2

8 LES OUTILS

Un certain nombre de logiciels du domaine de la SdF et de la qualité en général, y compris pour le contrôle et l'amélioration des processus de fabrication, sont notés ci-dessous à titre indicatif. Leur ergonomie est très variable et tous ne possèdent pas des bibliothèques de données, ce qui rend leur utilisation difficile sans la présence du concepteur. Des informations peuvent être obtenues sur les sites suivants (06-2003) :

<http://www.gfi.fr>

- ARALIA WorkShop(Sim-Tree, Hévéa) Arbres de défaillances et d'évènements.
- MOCA-RP, SCARABEE Boites de Pétri
- CECILIA WorkShop OCAS (ARBOR) Conception et Analyse Système (par Arbres de Défaillances)

<http://www.sofreten.fr>

SOFIA Analyse fonctionnelle et dysfonctionnements, AMDEC, arbre de fautes

<http://www.minitab.com>

MINITAB : statistiques en qualité : maîtrise statistique des procédés, analyse de fiabilité.

<http://www.sigmaplus.fr>

Logiciels de statistiques (MODDE, STATGRAPHICS, SIMCA, MULTISIMPLEX, SYNERGY 2000)

<http://www.gpc-system.com>

Détection des anomalies

<http://www.cabinnovation.fr>

SUPERCAB, CABTREE, SIMCAB RAMS

<http://www.itemuk.com>

ITEM TOOL KIT dont MIL STRESS RAMS

<http://www.relexsoftware.com>

RELEX RAMS

<http://www.ligeron.com> RAMS

<http://rac.alionscience.com>

SELECT RAMS

<http://www.calce.umd.edu>

CADMP II RAMS électronique

<http://www.norsys.com>

Netica Réseaux bayésiens

<http://rdsoft.edf.fr/>

fig.Seq

KB3

MTTF, Fiabilité, indisponibilité

Dépendabilité

1 2^{EME} PARTIE : LES RISQUES DE MANAGEMENT

Les risques de management doivent être pris en compte au même titre que les risques techniques avant la mise en route du système. Ces risques sont ceux liés au fait que les performances, les coûts et les délais ne sont pas tenus pour des raisons autres que les raisons purement techniques. Par opposition à ces derniers risques techniques, ils sont aussi appelés risques « généraux » du projet.

Dès le début d'un projet, les risques généraux sont évalués au moyen d'une check-list. Le résultat attendu est la prise de décision à l'aide de procédures.

1.1 Les critères de la check-list :

Les critères sont les suivants :

- la taille (en termes de coûts, ressources humaines, nombre de laboratoires, nombre d'interfaces...) du projet par rapport à ceux déjà menés,
- la difficulté technique (l'innovation, les compétences à trouver) et le domaine technique abordé (un projet terrestre est moins formel qu'un projet spatial, etc.) liés à la complexité du projet,
- le degré d'intégration du projet,
- la configuration organisationnelle,
- la stabilité et la compétence des membres du projet.

1.2 La check-list

Cette méthode **intuitive** permet d'examiner, catégorie par catégorie, le type de risque de management et les procédures appropriées :

1.2.1 *Risques socio-économiques : Dégradation du climat social*

Parade : *Etude de marché préalable, associer les utilisateurs au développement.*

1.2.2 *Risques économiques : Tout contrat (convention) doit être pesé avant signature*

- Evolution des barrières douanières
- Inflation : *La prévoir au budget.*
- Taux de change : *Choisir une unité monétaire appropriée.*
- Contraintes économiques liées au protocole d'accord ou par la convention ou le contrat : *Négocier pour limiter les risques.*
- Protocole d'accord ou MOU mal établi : *Etablir un comité de lecture avant approbation.*
- Hausse des prix : *Tenter une prévision de leur évolution.*

1.2.3 Risques politiques et périodes d'instabilité d'un pays

1.2.4 Risques géographiques :

- Législation sur l'environnement : *En prendre connaissance.*
- Climat : *Evaluer au préalable ses conséquences à partir des données antérieures.*
- Catastrophe naturelle : *S'informer au préalable de cette possibilité.*

1.2.5 Risques réglementaires :

- Non connaissance des codes et règlements à appliquer et de leur conséquence (durée et coût) : *S'informer auprès d'experts.*
- Evolution de la réglementation en vigueur : *Se tenir informé de la réglementation.*

1.2.6 Risques contractuels :

- Protocole d'accord ou convention ambigu : limite des prestations non définies :
Formaliser le Plan de Management et le Plan des Tâches (WBS).
- Interventions intempestives : *Plan de Management.*
- Manque de clarté des clauses de résiliation et d'arbitrage :
Les faire expliciter avant signature.
- Nature et durée des engagements pris : *Peser l'étendue des prestations.*
- Défection des sous-traitants : *Vérifier leur certification et les auditer avant contrat (cf. santé financière de la société).*

1.2.7 Risques organisationnels :

- Incohérence des procédures de gestion de projet :
Plan de Management.
- Manque de coordination dans le projet : ***Revoir l'organisation du projet et le Plan de Management.***
- Dilution importante des responsabilités : *Plan de Management concis (un seul responsable par tâche ou lot de travaux).*

- Faiblesse des structures en place et de la prise de décision :
Revoir le Plan de Management.
- Communication interne insuffisante : *Créer au besoin un Plan de Communication et de Gestion de Documentation (s'il n'a pas été rédigé).*
- Importance excessive des procédures de concertation :
Revoir le Plan de Management.
- Réunions projet inadéquates : *Différencier les Réunions d'Avancement des Réunions techniques.*
- Prédominance excessive d'un acteur du Projet :
Marquer la définition des fonctions (Revoir au besoin le Plan de Management).
- Mobilisation difficile des ressources : *Le faire ressortir dès que possible dans le planning.*

1.2.8 Risques techniques

- Evolution ou fluctuation du besoin : ***Le besoin doit être figé en phase B.***
- Manque de décisions entre choix techniques possibles :
Affirmation par responsables en phase B.
- Absence de coordination aux interfaces : *Dossiers d'interfaces avec responsables désignés.*
- Manque d'expérience antérieure dans une technologie :
Trouver les spécialistes ou les former.
- Technologies trop innovantes : ***Maquetter ou prototyper et valider les processus.***
- Technologie en obsolescence : *Analyser les inconvénients.*
- Transferts de technologies non étudiées sérieusement :
Etudier complètement les conséquences des transferts au besoin au moyen d'un modèle.
- Combinaison de procédés non maîtrisés : ***Revue de Procédés.***
- Evolutions du projet non maîtrisées : *Gérer la configuration selon le Plan*

- Non-conformités non maîtrisées : *Mettre en place les procédures prévues pour leur traitement.*
- Conception trop complexe : *Revue de conception.*
- Fabrication impossible : *Revue dédiée avant la CDR (Critical Design Review).*
- Reproductibilité en fabrication difficile : *Idem.*
- Procédures de suivi de fabrication non adaptées au produit : *Plan de suivi de fabrication.*

1.3 Remarques générales :

- 1 Le découpage du projet en **tâches** et l'identification des interfaces autorise des revues ponctuelles. Celles-ci réduisent les risques techniques de conception et de fabrication.
- 2 La division du projet en **phases** qui se closent par des revues génère un développement progressif du produit : en effet, les décisions sont prises en considérant les risques que les revues font ressortir.
- 3 La **gestion de configuration et de documentation** assurent la cohérence entre conception et réalisation et interdisent des évolutions non maîtrisées.
- 4 Le suivi au jour le jour du **budget et du planning** au niveau de la direction du projet détectent très rapidement toute déviation et évalue les conséquences.

1.4 La Méthode des 5M (diagramme d'Ishikawa)

C'est une autre méthode plus **analytique** qui permet de rechercher parmi le **Milieu**, la **Matière**, la **Main d'œuvre**, les **Moyens**, les **Méthodes**, les causes possibles d'un risque potentiel.

1.4.1 *Le Milieu ou l'environnement*

Les paramètres qui vont influencer sur l'environnement sont :

- l'espace, l'implantation, les distances, la proximité,
- la température et le bruit,
- la propreté et le nettoyage,
- l'encombrement et l'espace.

1.4.2 *La Matière (en temps que support)*

- l'énergie,
- les consommables,
- les composants,
- les pièces avec leur traçabilité (documents, formulaires, imprimés),
- les conditions d'approvisionnement,

- les conditions de fabrication et de transport (normes, pureté, tolérances, conditionnement, conditions de transport).

1.4.3 La Main d'œuvre (le personnel)

- les opérateurs : leur aptitude, leur formation, leur motivation, leurs attitudes au travail,
- les comportements individuels et en groupe,
- les relations entre travailleurs et la communication interne,
- le soutien de l'encadrement.

1.4.4 Le Matériel et les Moyens :

- l'état des machines outils et des outillages,
- la technologie des outils,
- les équipements, leur accessibilité, leur taux d'utilisation et leurs modes opératoires,
- le magasinage, l'emballage et la distribution des divers équipements fabriqués.

1.4.5 Les Méthodes (d'organisation)

- les procédures internes et les circuits de diffusion de l'information,
- les consignes et les instructions,
- les procédés de fabrication,
- la documentation disponible,
- les exigences, les standards à appliquer et la concision des directives à appliquer.

http://qualite.in2p3.fr/telechargement/telechargement/pdf/recommandation/Sdf_risques%20111203_SaP-AH.doc