Evolution des études qualitatives de Sûreté de Fonctionnement dans le domaine spatial

Roland Laulheret
Centre National d'Etudes Spatiales (CNES)
Laboratoire de Sûreté de Fonctionnement
18 avenue Edouard Belin
31401 Toulouse Cedex 4
roland.laulheret@cnes.fr
Tél. 05 61 27 47 19
Fax. 05 61 28 22 31

André Cabarbaye
Centre National d'Etudes Spatiales (CNES)
Laboratoire de Sûreté de Fonctionnement
18 avenue Edouard Belin
31401 Toulouse Cedex 4
andre.cabarbaye@cnes.fr
Tél. 05 61 28 27 41
Fax. 05 61 28 22 31

Résumé : La Sûreté de Fonctionnement sur les systèmes spatiaux s'est principalement appuyée sur l'AMDEC (Analyse des Modes de Défaillances, de leurs Effets et Criticités), qui consiste à analyser les effets des pannes de chaque composant élémentaire. Mais cette approche montre aujourd'hui ses limites. En effet, si l'AMDEC donne une impression d'exhaustivité en balayant l'ensemble des composants d'un produit, leurs modes de défaillance deviennent de plus en plus difficiles à caractériser ou ne sont plus déterministes (ASIC, microprocesseur....). De plus l'AMDEC est une analyse tardive, s'appuyant sur une définition détaillée, qui couvre mal les erreurs de conception (anomalies aux interfaces...), de réalisation (erreur de codage, de montage...) et les défaillances à causes multiples. Son coût, lorsqu'elle est généralisée à l'ensemble d'un système aussi complexe qu'un satellite, devient enfin prohibitif.
C'est pourquoi le CNES cherche à promouvoir l'Analyse Préliminaire de Risques (APR) qui, comme son nom l'indique, intervient beaucoup plus tôt en conception. L'APR se caractérise essentiellement par son processus d'identification des risques qui repose sur l'exploitation du retour d'expérience et sur une recherche déductive, descendant du système vers ses composants. Cette recherche s'appuie sur un découpage préalable en fonctions, en phases ou en processus suivant la catégorie de risques auxquels on s'intéresse (fonctionnement, mise en service, fabrication…). Le traitement des risques peut conduire à des actions diverses telles que l'application de règles de conception éliminant a priori les risques techniques (simplicité des architectures, ségrégation, robustesse intrinsèque, standardisation...) ou la réalisation d'AMDEC ciblées, quand les risques de propagation de certaines défaillances sont difficiles à appréhender.
Cependant, l'APR rencontre certaines difficultés qui ne doivent pas être négligées. Mise en œuvre dès le début de la conception elle suppose que des moyens adéquats (humains et matériels) soient disponibles suffisamment tôt dans les projets. Elle conduit parfois à des difficultés contractuelles car il est généralement difficile d'évaluer a priori le volume de l'analyse. Elle se heurte enfin à un frein culturel dans certaines organisations en demandant aux fiabilistes de mener une véritable activité d'ingénierie qui ne se limite plus à une simple vérification a posteriori de la conception faite pour répondre à une demande contractuelle.
Après une brève présentation des limites de l'AMDEC, cette communication présente l'Analyse Préliminaire de Risques en s'appuyant sur des exemples pratiques.

Mots-clés : Analyse Préliminaire de Risques - AMDEC - Sûreté de Fonctionnement

1. Introduction

Afin d'identifier les risques sur les systèmes spatiaux, l'activité de Sûreté de Fonctionnement s'est principalement appuyée sur un type d'analyse, l'AMDEC (Analyse des Modes de Défaillances, de leurs Effets et Criticités), qui consiste à analyser les effets des pannes de chaque composant élémentaire.
Cette approche s'est avérée fructueuse dans le passé, comme en témoigne l'excellente fiabilité opérationnelle de certains produits (Spot1, Ariane4,...) mais elle montre aujourd'hui ses limites et nous oblige à choisir une autre démarche.
En effet, si l'AMDEC procure une illusion d'exhaustivité en balayant l'ensemble des composants (matériels) du produit, son efficacité réelle est limitée et a tendance à diminuer aujourd'hui avec l'évolution rapide des technologies qui rend de plus en plus difficile la caractérisation des modes de défaillance. Par ailleurs, l'AMDEC est une analyse relativement tardive, car elle s'appuie sur une définition assez détaillée du produit, et ne peut donc avoir qu'un impact limité sur la conception de celui-ci.
C'est pourquoi le CNES cherche à promouvoir depuis quelques années l'Analyse Préliminaire de Risques (APR) qui intervient beaucoup plus tôt en phases préliminaires de conception.
Après un bref rappel du processus général de maîtrise des risques appliqué sur un projet, cette communication souligne les difficultés et limites de l'AMDEC avant de présenter l'Analyse Préliminaire de Risques de manière approfondie. Elle propose une articulation entre ces diverses analyses en s'appuyant sur un exemple pratique.

2. La maîtrise des risques

La maîtrise des risques recouvre tous les moyens, analyses, procédures, actions… mis en œuvre durant le cycle complet d'un produit pour supprimer ou rendre acceptables les risques liés à sa fabrication, à son utilisation et à sa mise hors service. Celle-ci repose essentiellement sur le processus décrit en figure 1.

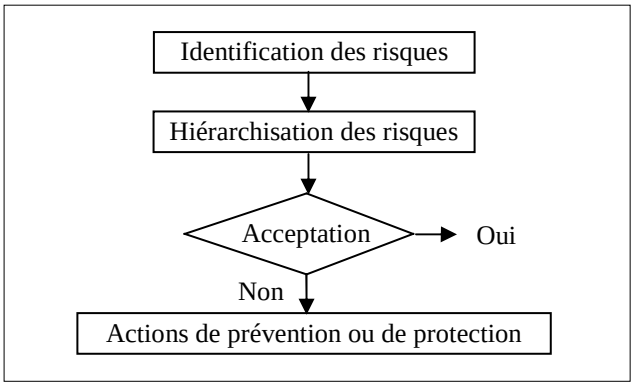

Figure 1 - *Processus de maîtrise des risques*

Ce processus de maîtrise des risques passe par la recherche systématique des risques liés au produit, leur hiérarchisation suivant la gravité de leurs conséquences et leur probabilité d'occurrence, puis leur acceptation éventuelle ou leur traitement. Ce dernier consiste à mettre en oeuvre des actions de prévention, en intervenant sur les causes afin d'éviter que les événements redoutés ne surviennent, ou de protection, pour en diminuer les effets. La définition préalable d'un domaine d'acceptabilité, tel que celui décrit à la figure 2, permet d'accepter ou de rejeter chacun des risques identifiés. Les variables de gravité et de probabilité font généralement l'objet d'une classification pour faciliter ce traitement.

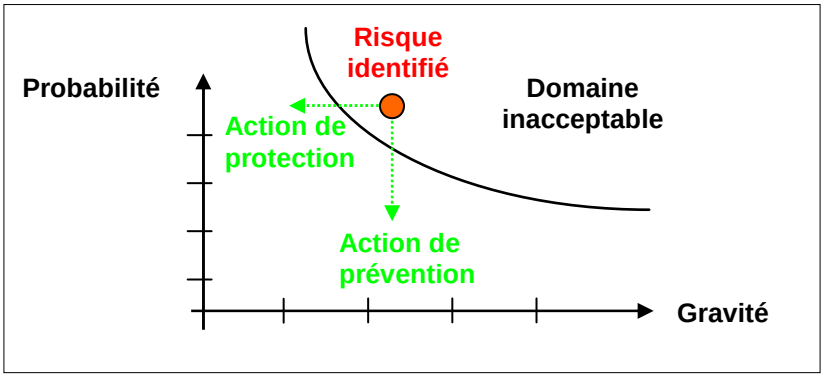

Figure 2 - *Domaine d'acceptabilité des risques*

L'identification des risques s'appuie essentiellement sur trois types de démarche (figure 3) :
- la démarche déductive descendante qui consiste à imaginer les causes possibles d'un événement redouté tel que la perte de tout ou partie du service rendu par le produit ou des dommages occasionnés par celui-ci à des personnes, à l'environnement et aux biens,
- la démarche inductive montante qui consiste à analyser les effets au niveau du produit ou de son environnement des défaillances de ses constituants,
- l'exploitation du retour d'expérience qui peut recouvrir des formes multiples telles que des listes de risques génériques (utilisée notamment en sécurité) ou des règles de conception (normes, marges de dimensionnement, recommandations après incidents…).

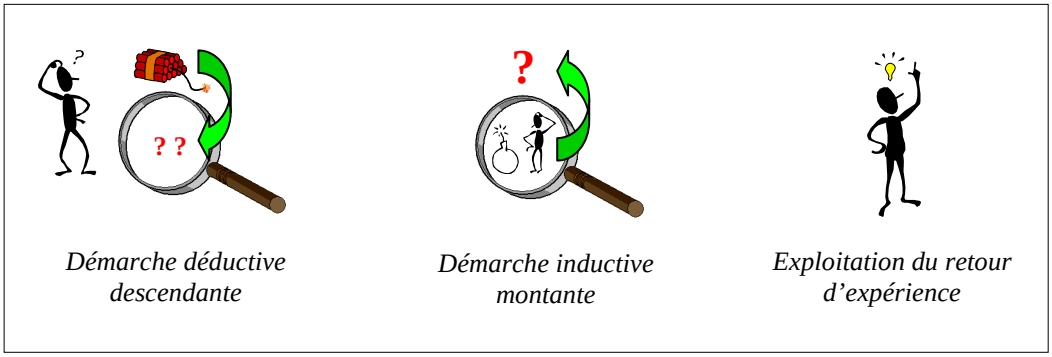

Figure 3 – *Démarches d'identification des risques*

3. L'AMDEC et ses limites

L'AMDEC fait l'objet de normes internationales reconnues (X 60-510, CEI 812 et MIL-STD-1629A) qui la définissent précisément comme une analyse inductive montante, partant du niveau le plus bas pour lequel on dispose d'information sur de possibles défaillances (composants, sous-ensemble…) pour en analyser les effets au niveau le plus haut (produit); Les modes de défaillances considérés étant soit issus du retour d'expérience, sous forme de base de données de défaillance de composants, soit identifiés par une analyse déductive au niveau élémentaire. L'AMDEC se présente sous forme de tables (Figure 4). Sur de gros systèmes tels que des satellites, celles-ci s'enrichissent progressivement par les différents intervenants durant le développement du produit (de l'équipementier au maître d'oeuvre).

PROJET : *SATELLITE* S-SYSTEME : *Propulsion*

Identif. Comp.	**Fonctions Etats**	**Mode de défaillance**	**Causes**	**Effets**	**Gravité**	**Proba.**	**Détection**	**Actions Recommandations**
Vanne N_2H_4 Repère V01	Vanne monostable Etat de repos : fermée	1. bloquée ouverte	Défaut mécanique clapet interne Commande électrique permanente	Modification d'orbite . Risque de perte mission	**3** (maxi)	5.10^{-8} panne/h	Orbite erronée ou pas de réception du satellite, lors de la visibilité sol suivante	Effectuer le contrôle d'orbite en phase de visibilité sol. Si panne, stopper la propulsion par la vanne "arm" Prévoir une limitation temporelle sur la commande de la vanne

Figure 4 – *Exemple d'AMDEC*

Bien que l'AMDEC balaye l'ensemble des composants d'un produit, sa valeur ne dépend que de la pertinence des défaillances élémentaires considérées.
Ainsi les modes de panne "circuit ouvert" et "court-circuit" des composants électroniques sont généralement pris en compte dans les analyses, mais rarement les dérives de paramètre qui peuvent avoir des effets critiques comme, par exemple, une dissipation thermique venant "stresser" des éléments à proximité (fonctionnement linéaire d'un transistor de commutation par exemple).
Les composants discrets (résistances, condensateurs, transistors...) disparaissent au profit de circuits très intégrés (ASIC, microprocesseur…) pour lesquels les défaillances se manifestent par des effets qui ne sont plus déterministes et qui dépendent notamment de l'instant de leur occurrence. Effectuer une AMDEC à l'intérieur d'une puce n'a pas vraiment de sens car les phénomènes de propagation de panne interne ne sont pas maîtrisables en raison des proximités.
De plus, l'AMDEC couvre mal les erreurs de conception (problèmes de spécification, anomalies aux interfaces...), de réalisation (erreur de codage, de montage...) et les défaillances à causes multiples. Ainsi sur les divers mécanismes utilisés en orbite (générateur solaire, systèmes de gerbage, gyroscopes…), les

dysfonctionnements rencontrés concernent essentiellement des problèmes d'interface, de compatibilité entre matériaux, de pollution ou de montage mais très rarement des défaillances de composants. De même l'AMDEC n'est pas applicable aux logiciels et aux humains (malgré certaines tentatives infructueuses), dont les comportements anormaux apparaissent le plus souvent irrationnels.
Par ailleurs, l'AMDEC est une analyse tardive qui s'appuie sur une définition suffisamment détaillée du matériel pour appréhender des modes de défaillance crédibles, si possibles issus de l'expérience. Enfin le coût d'une AMDEC généralisée à l'ensemble d'un système aussi complexe qu'un satellite devient prohibitif en regard des contraintes budgétaires. Ces contraintes ont déjà conduit dans le passé à certains relâchements des exigences, comme la rédaction des AMDEC au niveau des blocs fonctionnels (quelques composants assurant une fonction) et non plus des composants élémentaires. Mais les modes de défaillances considérés sont-ils alors toujours crédibles ? Quelques PPU (Points de Panne Unique : panne simple entraînant un événement redouté majeur) découverts très tardivement sur certains programmes peuvent nous en faire douter.

4. L'Analyse Préliminaire de Risques

L'APR est une analyse déductive descendante dont l'objet est d'identifier très tôt les événements redoutés et les causes possibles de défaillance. Ces dernières peuvent être d'origine matérielles, logicielles ou humaines. Elle permet une optimisation de la conception en proposant des recommandations ou actions en réduction du risque en phase avec le cycle de développement du produit. L'effort en terme de sûreté de fonctionnement est donc essentiellement porté dans les phases amont du développement, compte tenu des conséquences industrielles de la découverte tardive d'une erreur (impacts sur les coûts et le planning lorsque le traitement de l'erreur est encore possible). Il est à noter qu'une démarche similaire est couramment utilisée dans le domaine aéronautique civil (pour ne citer que lui), pour s'assurer que l'avion conçu satisfait aux objectifs de la réglementation (FAR/JAR 25) et aux attentes des compagnies en terme de réussite mission (taux de disponibilité élevé).

4.1 Démarche

L'analyse de risques suit le processus de maîtrise des risques décrit précédemment, enrichi de la manière suivante (figure 5) :

- identification des risques,
- hiérarchisation,
- détermination de la criticité des différentes fonctions du système,
- identification des matériels, logiciels et opérations critiques car supportant ces fonctions critiques,
- définition des besoins en analyses ciblées plus poussées (AMDEC, analyse de pire cas), en essais supplémentaires (durée de vie, tenue à l'environnement), en observables (télémesures, …), et proposition de modifications d'architectures, de procédures particulières, ...

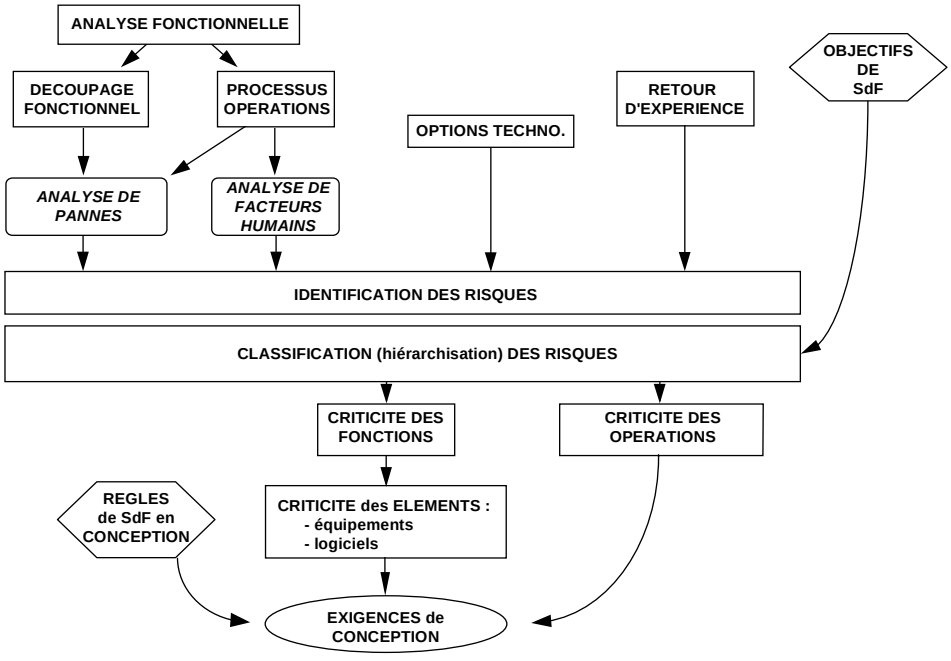

Figure 5 - *Synoptique de la démarche d'analyse de risques*

4.2 Identification des risques

L'identification des risques repose dans un premier temps sur l'exploitation du retour d'expérience. Hors, l'expérience est souvent mal formalisée. Elle apparaît au détour de certaines spécifications de réalisation de programmes antérieurs, de recommandations émises lors de revues, ou de rapports d'incident. Mais elle est souvent difficilement consultable surtout quand elle ne réside que dans le savoir faire de quelques spécialistes.
Cette exploitation du retour d'expérience doit être complétée par une analyse plus systématique qui est menée à partir d'un découpage du produit à un niveau suffisamment fin pour bien appréhender les risques :

- en fonctions (issues d'une analyse fonctionnelle). On analyse les effets sur le produit et son environnement de la perte, de la dégradation ou de l'apparition intempestive de chacune des fonctions.
- temporel ou en phases de fonctionnement (mise à poste d'un satellite, par exemple). Elle a alors pour objet d'identifier les risques induits par un mauvais enchaînement des différents événements élémentaires (mauvais séquencement, perte du synchronisme, fonctionnement intempestif ou tardif).
- en processus, afin d'identifier les risques liés à une activité d'intégration ou de production. La démarche est alors similaire à celle évoquée ci-dessus.

Remarque : hormis pour les aspects liés à la sécurité des personnes, les analyses sont menées en ne considérant pas de combinaisons de pannes.

4.3 Hiérarchisation des risques

Cette classification des risques est définie pour un projet donné et lui est spécifique. Elle consiste à classer les risques identifiés suivant leurs conséquences et permet de faire porter l'effort sur les fonctions (et les moyens de les réaliser: matériels, logiciels, humains) impliquées dans les risques ayant les conséquences les plus néfastes.
A titre d'exemple le tableau 6, illustre notre propos.

CLASSE	EFFETS
CATASTROPHIQUE	Perte de vie humaine. Destruction d'infrastructures (lanceur, pas de tir, ...) et / ou de biens.
GRAVE	Risque qui ne permet plus d'assurer la mission. Pour la partie sol : Perte définitive de l'accès au satellite par ses moyens propres. Report de lancement.
MAJEURE	Risque qui réduit sensiblement les capacités du bord ou du sol mais qui : - permet d'assurer une mission dégradée ou écourtée, - entraîne des contraintes opérationnelles importantes, - ne permet pas de respecter les durées maximales d'indisponibilité spécifiées.
SIGNIFICATIVE	Situation qui permet d'assurer la mission mais qui entraîne des contraintes opérationnelles acceptables telles que le passage d'une chaîne nominale à une chaîne redondante.
MINEURE	Risque qui entraîne : - une diminution acceptable des performances du bord ou du sol, - des contraintes opérationnelles supplémentaires acceptables, - une indisponibilité compatible avec les exigences spécifiées.

Tableau 6 - *Exemple de classification des risques*

4.3 Recommandations issues de l'APR

L'analyse conduit à des recommandations telles que celles indiquées ci-dessous :

- exigences à respecter concernant les fonctions, opérations, matériels, logiciels, (tolérance à une ou plusieurs pannes, robustesse vis-à-vis de l'environnement, ...)
- modifications de design telle que la mise en place d'une protection spécifique, d'une redondance locale, d'un observable particulier, ...
- hypothèses de travail à confirmer,
- besoins d'études complémentaires telles que des analyses de validation (AMDEC, analyse de pire cas),
- besoins d'essais ou de simulation,
- répercussions à évaluer,
- etc...

Ces recommandations constituent la sortie essentielle de l'analyse de risque qui garantit la sûreté de fonctionnement du produit.

4.4 Exemple d'une fiche d'analyse de risque :

Segment Sol	**Référence**	**Titre**
Fonction	F1.4.4	Archiver la télémesure enregistrée en station
Scénario	1	Perte de l'archivage
Phase de mission ou mode de fonctionnement		Toutes phases
Répercussion		Perte de l'archivage de la télémesure au niveau du centre de contrôle / commande depuis la dernière sauvegarde
Moyen de détection **(Temps de détection)**		Immédiat par l'opérateur
Moyens de reconfiguration / Action opérateur **Etat du système après la reconfiguration** **(Temps de reconfiguration)**		• Réparation (voir R18) • Récupération des données à partir de la dernière sauvegarde au centre de contrôle / commande et de la sauvegarde en station
Recommandations / Actions		R13 : Vérifier la cohérence de la capacité de stockage de la télémesure enregistrée en station, vis-à-vis des 72 heures de réparation du centre de contrôle / commande R14 : Sauvegarder l'archive sur une mémoire de masse (CD, ...), avec une fréquence inférieure à 72 heures, sachant que les dernières 72 heures sont sauvegardées à la station (antenne) R18 : Exigence de réparation en moins de 72 heures, et une disponibilité > à 0.99, après les 24 premières heures suivant l'injection en orbite par le lanceur

Evénement Redouté		
Référence	**Libellé**	**Classification**
E.R. 108	Perte de l'archive en ligne	MAJEUR

Fonction analysée

Mode de défaillance :
- Perte,
- Dégradation,
- Fonctionnement intempestif

Effets sur les différentes composantes du système

Intégration, lancement, recette, Mode opérationnel, Mode survie, ...

Observables et délais de réaction

Moyens initialement prévus pour isoler la défaillance et reconfigurer le système

Sorties principales de l'analyse

Echelle de classement établie avec le projet

Figure 7 - *Exemple d'une fiche d'analyse de risques*

4.5 Articulation des analyses

L'articulation entre l'APR et les autres analyses de sûreté de fonctionnement peut être illustrée par l'exemple de la figure 8.

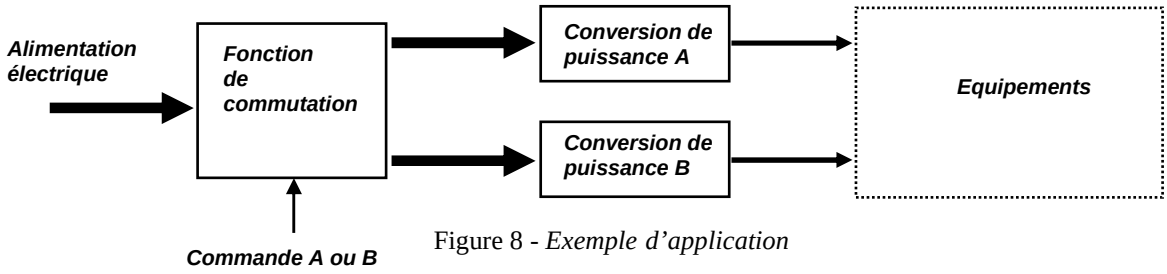

Figure 8 - *Exemple d'application*

Dans cet exemple, l'événement redouté que l'on considère est la perte de l'alimentation électrique des équipements, sur simple panne. Cet événement redouté est classé « Grave » car il entraîne la perte du satellite.
A ce stade de définition, l'APR permet de considérer comme acceptable la perte d'un convertisseur de puissance car ce dernier est redondé. Elle conduit à effectuer deux analyses plus poussées, une AMDEC limitée à la fonction de commutation pour mieux appréhender les risques de Points de Pannes Unique, et une analyse de pire cas du filtre d'entrée du convertisseur pour vérifier sa performance même en cas de pannes.
Enfin, l'APR impose certaines exigences de conception pour éviter la propagation de pannes électriques qui conduisent à la mise en place des protections :
- de l'alimentation principale contre les surconsommations (court-circuit, …) et contre les perturbations électromagnétiques (filtre robuste, …),
- en surtension en sortie du convertisseur, si chaque convertisseur peut alimenter l'ensemble des équipements en aval (cross-strapping),

et pour éviter la propagation de pannes par effets thermiques au moyen de :
- la ségrégation des voies nominale et redondante,
- la non proximité d'équipements sensibles aux dérives thermiques.

4.6 Conclusions

Contrairement à l'AMDEC, l'APR est une analyse précoce qui a un véritable impact sur la conception (mise en place de surveillances, de protections, de redondances, d'essais, ...). Elle permet ainsi de maîtriser les risques techniques en limitant les impacts éventuels sur le planning ou le budget.
Elle considère toutes les composantes du système (matérielles, logicielles et humaines) et leurs interactions. Le traitement des risques peut conduire à des actions diverses telles que l'application de règles de conception éliminant a priori les risques techniques (simplicité des architectures, ségrégation, robustesse intrinsèque, standardisation...), la réalisation d'AMDEC ciblées quand les risques de propagation de certaines défaillances sont difficiles à appréhender, ou d'autres types d'analyses (pire cas, …).
Elle permet de mémoriser la raison des choix techniques et améliore les spécifications vers les niveaux inférieurs (exigences de sûreté de fonctionnement libellées en terme d'événements redoutés vers les équipementiers). Elle favorise ainsi leur compréhension et les échanges entre clients et fournisseurs.

Néanmoins, certaines difficultés sont à noter dans son application.
Mise en œuvre dès le début de la conception elle suppose que des moyens adéquats (humains et matériels) soient disponibles suffisamment tôt. Plus que pour l'AMDEC, une réelle implication des experts est nécessaire pour que l'analyse de risques ne conduise pas à de simples généralités. De petits groupes de travail réunissant les responsables techniques de la chaîne fonctionnelle étudiée et le fiabiliste sont un bon moyen de parvenir à ce but.
Le chiffrage a priori du volume des analyses peut conduire à certains problèmes lors de la négociation des contrats (à la différence de l'AMDEC qui peut être évaluée aisément en fonction du nombre de composants du produit). Allouer une enveloppe forfaitaire peut être un moyen de pallier à cette difficulté.
Enfin, il est à noter un frein culturel dans certaines entreprises où les fiabilistes interviennent essentiellement pour vérifier la conception, sans participer réellement à cette dernière.
L'existence d'une norme internationale sur l'APR faciliterait sa diffusion et éviterait certaines confusions ou mauvaises compréhensions entre les intervenants.

Quelques références :
A. Pages & M. Gondran
Fiabilité des systèmes - Edition Eyrolles, Paris 1980
A. Villemeur
Sûreté de Fonctionnement des systèmes industriels - Edition Eyrolles, Paris 1987
R. Laulheret
Maîtrise des risques techniques - Cours de technologies spatiales, Edition Cepadues Toulouse 1998