FORMALISATION DU RETOUR D'EXPÉRIENCE EN SÛRETÉ DE FONCTIONNEMENT DANS LE DOMAINE SPATIAL
DEPENDABILITY LESSONS LEARNED IN THE SPACE FIELD

Karine Etienne[1], Julien Faure1, André Cabarbaye[1&2]

[1]Centre National d'Etudes Spatiales (CNES)
18, avenue Edouard Belin - 31401 Toulouse
Tél. 0561282689 / Fax. 0561282231
julien.faure@cnes.fr
karine.etienne@cnes.fr
andre.cabarbaye@cnes.fr

[2]CAB INNOVATION
3, rue de la Coquille - 31500 Toulouse
Tél. 0561546808 / Fax. 0561543332
andre.cabarbaye@cabinnovation.fr

Résumé

Après une brève présentation des spécificités du domaine spatial et de la problématique du Retour d'Expérience, cette communication porte sur la présentation d'un outil nommé SAFE (pour SAtellite Feeback Experience) développé par le Centre National d'Etudes Spatiales afin de capitaliser l'expérience en Sûreté de Fonctionnement des systèmes satellitaires. Il recense et décrit notamment les principaux risques rencontrés dans les architectures et les règles de conception mises en œuvre pour les maîtriser. Il propose également des fiches méthodologiques sur les méthodes probabilistes illustrées d'exemples concrets. Cette expérience acquise par le service Sûreté de Fonctionnement et les Services Techniques est proposée en intranet à tout concepteur ou fiabiliste désireux de traiter les problématiques de fiabilité au cours de la conception d'un satellite.

Summary

After a brief presentation of specificities of the space field and problems of lessons learned, this communication relates to the presentation of a tool named SAFE (for SAtellite Feeback Experience) developed by the Centre National d'Etudes Spatiales in order to capitalize the dependability experience of the satellite systems. It counts and describes in particular the principal risks met in architectures and the design rules implemented to control them. It also provides methodology sheets on probabilistic methods illustrated with concrete examples. This experience acquired by the Dependability Service and the Engineering Services is proposed in Intranet to any designer or reliability engineer eager to treat the problems of reliability during the design of a satellite..

1. Introduction

Sous le vocable de « Retour d'Expérience », la politique de gestion et de capitalisation des connaissances concerne tout particulièrement la maîtrise des risques. Aussi, le REX en Sûreté de Fonctionnement se développe-t-il progressivement dans les organisations. Certaines privilégient le stockage d'informations sur les incidents passés, d'autres tentent d'enrichir leurs référentiels par diverses règles de conception. Mais toute la difficulté réside dans l'identification de l'information pertinente et sa traduction dans un langage adapté aux utilisateurs potentiels. Cette information peut être de nature qualitative, comme des listes de risques génériques à des filières de produits, ou quantitative sur des données statistiques en opération. Elle peut également concerner des méthodes de calcul adaptées aux problématiques rencontrées.

Par ailleurs, la capitalisation de l'expérience est particulièrement cruciale dans le domaine spatial car les satellites et les lanceurs sont des systèmes « mono-coup » qu'il n'est plus possible de réparer après utilisation (hormis des logiciels téléchargeables dans les satellites). De plus, ce domaine possède certaines spécificités qui ne facilitent pas le retour d'expérience :
- les systèmes sont inaccessibles une fois mis en orbite, ce qui amène à faire des conjectures sur les causes éventuelles de dysfonctionnements à partir des seuls observables reçus par télémesures,
- l'environnement radiatif et la présence de micrométéorites ou d'oxygène mono atomique, propre à l'espace, conduit à des modes de défaillance spécifiques (usure et pannes fugitives de composants, détérioration des caractéristiques des matériaux…),
- la construction de satellites en très faibles séries relève du domaine du prototypage et ne peut conduire à la production d'un recueil de données statistiques fournies,
- la durée de vie d'un satellite est longue (de 5 à 20 ans), ce qui nécessite l'implantation de redondances à bord qu'il faut préserver de toute propagation de panne et gérer correctement,
- les cycles de développement sont également de longue durée (de 3 à 10 ans), ce qui conduit à une certaine volatilité des connaissances du fait de changements inéluctables qui interviennent au sein d'équipes de conception rassemblant des spécialistes de métiers très divers,
- la documentation (référentiel normatif, documentation projet, revues, commissions d'enquête…) et les recommandations qui en sont issues sont particulièrement abondantes et disparates,
- la maîtrise des risques sur ce type de produit passe tout particulièrement par un renforcement des analyses de dimensionnement (en pire cas) et de calcul prévisionnel (fiabilité, disponibilité …).

Le service de Sûreté de Fonctionnement du Centre National d'Etudes Spatiales (CNES) de Toulouse, en charge de la maîtrise des risques sur des systèmes particulièrement peu tolérants à l'erreur de conception, a tenté de formaliser l'expérience acquise et de la transmettre efficacement aux concepteurs. L'objet de cette communication est de présenter les résultats de ce travail qui est notamment matérialisé par l'outil SAFE (pour « SAtellite Feedback Experience »). Développé pour capitaliser l'expérience en Sûreté de Fonctionnement sur les systèmes spatiaux, cet outil, qui a été dévoilé au congrès Lambdamu 15, s'est fortement enrichi et recouvre aujourd'hui tant les aspects qualitatifs que quantitatifs.

2. L'outil Safe

L'expérience acquise par le Service Sûreté de Fonctionnement et les Services Techniques du CNES est proposée en Intranet à tout concepteur ou fiabiliste. En rupture avec les pratiques répandues d'accumulation dans des bases de données, une présentation innovante de l'information a été choisie, basée sur la technologie HTML utilisée pour la création de sites web.

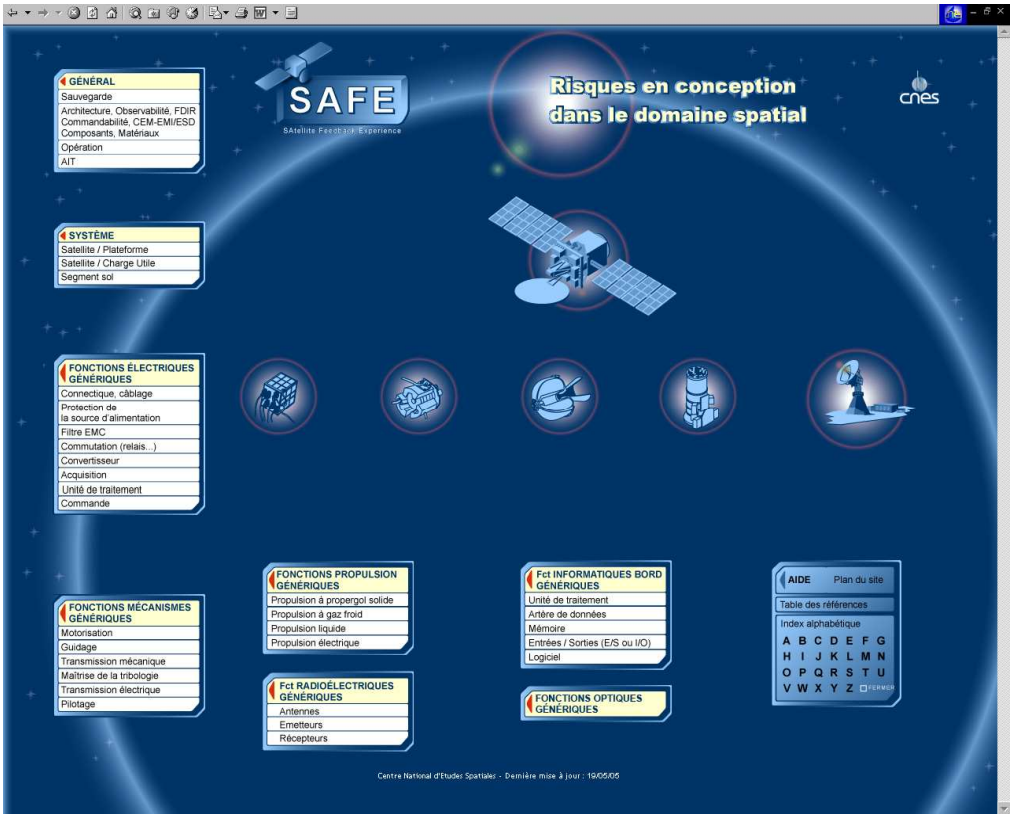


Figure 1. Page d'accueil de l'outil SAFE

2.1. Risques génériques et règles de conception

Sur le plan qualitatif, l'outil SAFE décrit les principaux risques rencontrés dans les architectures de satellites et les règles de bonne conception mises en œuvre pour les maîtriser. La première étape de réalisation a consisté en une analyse documentaire pour en extraire les informations pertinentes portant notamment sur les dysfonctionnements passés. Les mêmes causes racines ont ainsi été regroupées dans des risques génériques au détriment d'une exhaustivité d'exemples qui aurait nuit à la clarté du propos. Les connaissances recueillies ont été validées par des experts des différents métiers concernés (mécanisme, alimentation électrique, etc).

Cette expérience a ensuite été formulée dans un langage clair et accessible à tous sous forme de check-lists de règles de conception et de risques génériques propres aux divers constituants des systèmes spatiaux. Elle est accessible par différents moyens :
- Des thèmes généraux : Sauvegarde, Architecture, FDIR (Failure Detection Isolation and Recovery), Observabilité / Commandabilité, Environnement, Composants, Matériaux, Opérations, Assemblage/Intégration/Tests…),
- L'arborescence fonctionnelle d'un satellite ou d'un segment sol,
- La décomposition de fonctions génériques (électrique, mécanisme, optique, propulsion, radioélectrique, informatique bord),
- Des mots-clés.

Une page d'aide (Figure 2), accessible depuis la page d'accueil, présente les liens hypertextes disponibles et le modèle sur lequel sont construits les pages HTML du site.
Pour chaque thème ou fonction traité, on trouve sur la page HTML correspondante :
- Une description succincte du thème ou de la fonction,
- Un accès hypertexte aux risques et règles correspondants,
- Un accès à des définitions de termes si nécessaire,
- Un icône d'impression de la page HTML en cours de consultation,
- Le chemin d'arborescence des pages visitées accessible en liens hypertexte,
- Le menu principal.

Egalement accessible depuis la page d'accueil, une page des références (Figure 3) consigne tous les documents exploités pour l'écriture des règles de conception, schémas et illustrations.
Chaque règle de conception de l'outil SAFE est indexée de la référence du document qui a servi à son élaboration.

A partir de la page d'accueil, il est également possible d'accéder à l'information à partir de mots-clés consignés dans un index alphabétique (Figure 4).

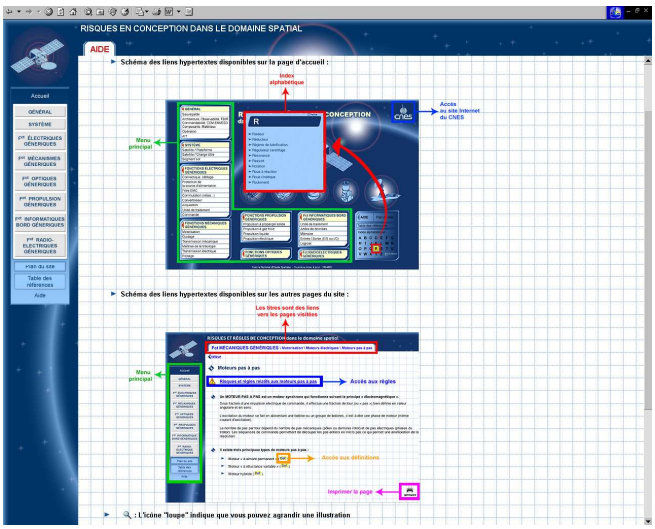


Figure 2. Page d'aide

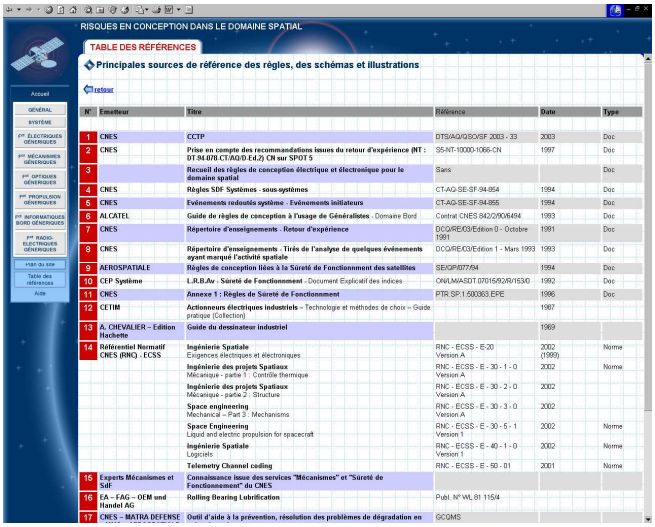


Figure 3. Page des références

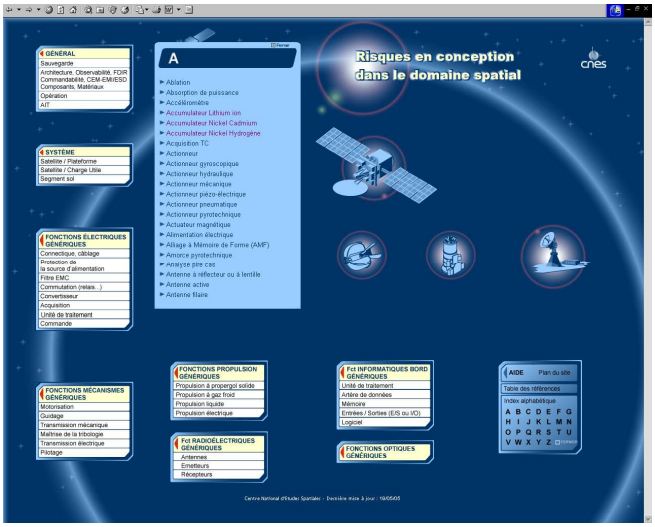


Figure 4. Index alphabétique de mots-clé à la lettre « A »

A titre d'illustration, les fonctions électriques génériques (figure 1) regroupent les fonctions élémentaires que l'on rencontre habituellement dans tout équipement électrique, telles que :
- Connectique et câblage (permettent d'assurer la connexion électrique entre les différents équipements),
- Protection de la source d'alimentation (protège la source d'alimentation électrique des dysfonctionnements en aval),
- Filtre EMC (permet de limiter les perturbations électromagnétiques émises par l'équipement sur la barre de puissance ainsi que de

protéger l'équipement des perturbations transmises par la barre de puissance),
- Commutation (permet la mise sous tension et hors tension des équipements et l'activation ou l'inhibition des signaux électriques),
- Acquisition & commande (constituent des interfaces analogiques ou numériques dédiées au contrôle des équipements ou échanges d'informations entre eux),
- Convertisseur d'énergie électrique (assure une conversion en tension),
- Unité de traitement (gestion du protocole, traitement des télécommandes, génération des télémesures, gestion du temps bord, détection et passivation des pannes et anomalies et gestion des reconfigurations selon la stratégie FDIR),

Le lien hypertexte « Convertisseur » conduit à une description de la fonction convertisseur ainsi qu'à un découpage fonctionnel (figure 5).

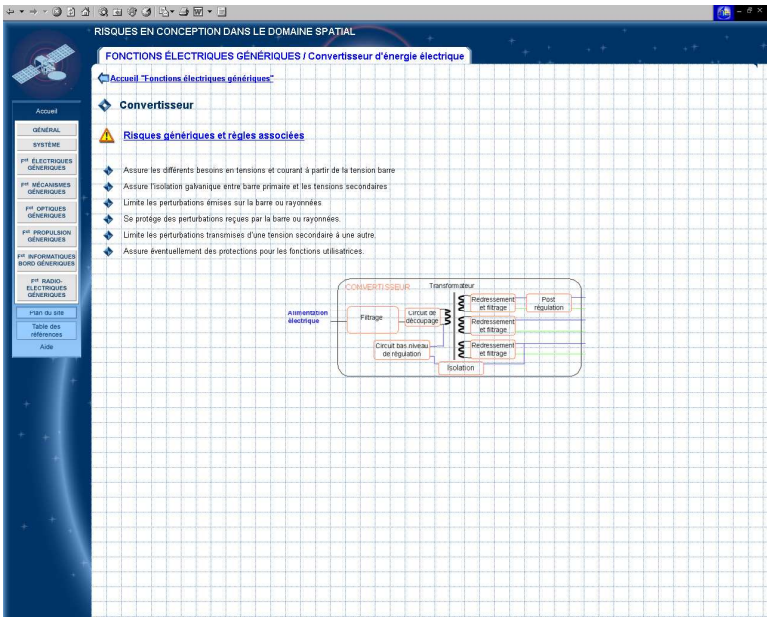


Figure 5. Descrition de la fonction convertisseur

Le lien hypertexte « Risques génériques et règles associées » conduit à la liste des risques associés à la fonction convertisseur (figure 6).

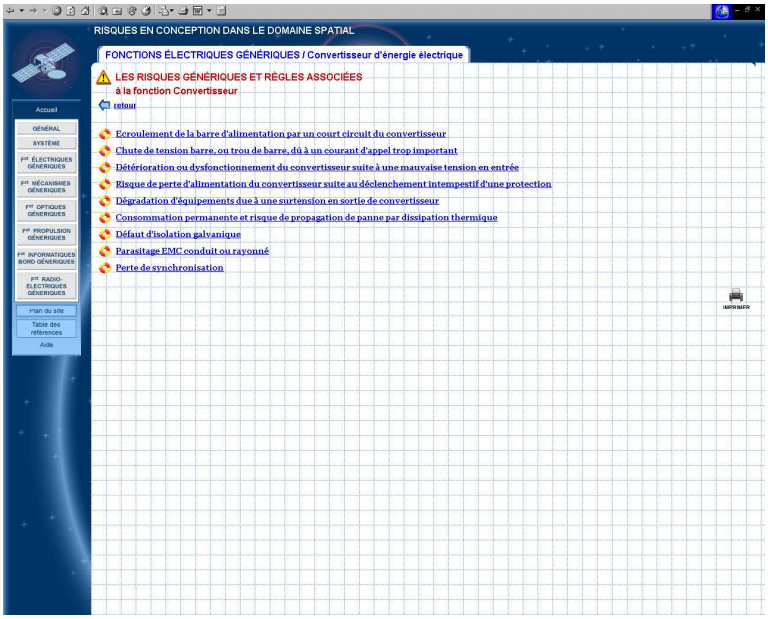


Figure 6. Risques génériques associés à la fonction convertisseur

Le lien hypertexte « Chute de tension barre, ou trou de barre, dû à un courant d'appel trop fort » permet d'afficher la page décrivant les règles de conception à mettre en œuvre pour supprimer ou réduire le risque correspondant.

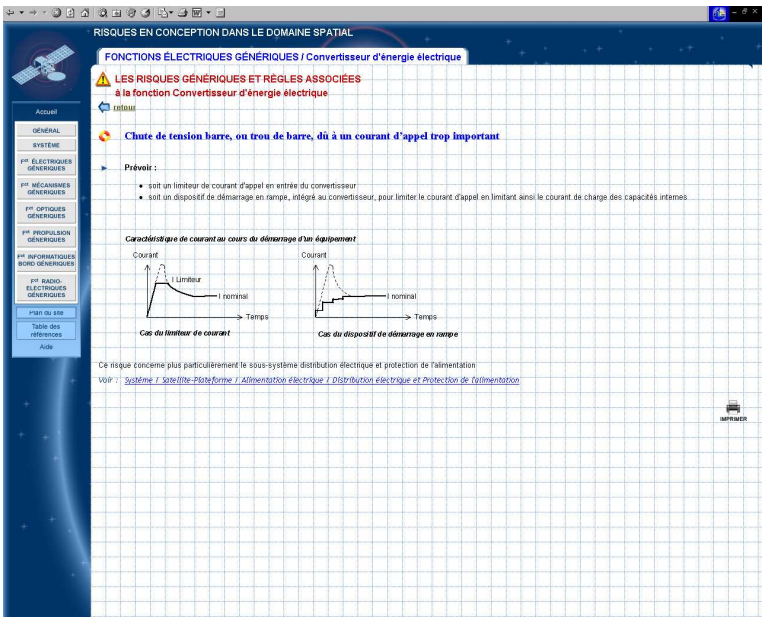


Figure 7. Règles de conception associées au risque

"Chute de tension barre, ou trou de barre, dû à un courant d'appel trop fort »

2.2. Rex sur les méthodes probabilistes

Sur le plan quantitatif, la vulgarisation de méthodes parfois complexes est un exercice difficile. Le REX doit être clair et synthétique pour permettre leur application immédiate tout en donnant la possibilité aux lecteurs d'approfondir la théorie s'ils le souhaitent. Aussi a-t-il été choisi une présentation sous forme de fiches accessibles sur l'outil à partir d'une liste de thèmes (problématiques) ou de méthodes.

Afin d'assurer une certaine homogénéité, les fiches présentent toutes les mêmes rubriques :
- objectif : il est rappelé dès le début de la fiche afin de comprendre rapidement les enjeux,
- principe: il s'agit uniquement d'une version simplifiée de la théorie sur laquelle repose la méthode,
- mise en œuvre : cette partie explicite concrètement comment appliquer la méthode,
- illustration par plusieurs exemples concrets,
- annexes : cette partie contient les approfondissements théoriques.

Ces fiches comprennent de nombreuses insertions de tableaux au format Excel qu'il est possible d'ouvrir afin de pouvoir traiter directement les exemples présentés, en utilisant éventuellement des outils spécifiques (dont notamment l'atelier SUPERCABPRO de la société CAB INNOVATION).

Les premières fiches réalisées portent sur
- les analyses pire cas,
- les anneaux de redondance,
- la modélisation du déploiement et du renouvellement d'une constellation de satellites,
- la simulation de Monte-Carlo et les techniques de réduction de la variance,
- l'estimation et les intervalles de confiance,
- l'estimation bayésienne,
- les techniques d'ajustement,
- la loi de Weibull,
- les essais accélérés,
- les critères de choix parmi les diverses méthodes de modélisation et de traitement,
- le couplage avec divers outils d'optimisation,
- les techniques markoviennes,
- la modélisation récursive,
- les arbres de défaillances,
- le bloc diagramme de fiabilité

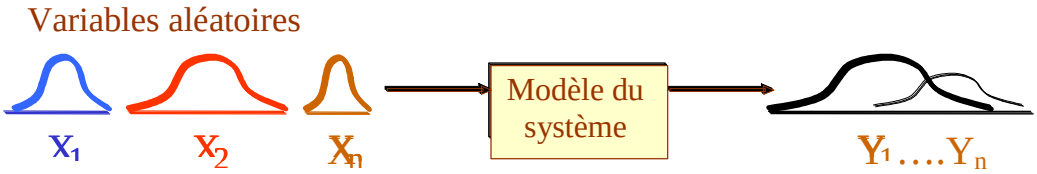
A titre d'exemple, nous présentons ci-après la fiche « Réduction de la variance » de manière très succincte :

Objectifs

- Augmentation de la précision des résultats des simulations de Monte-Carlo (intervalles de confiance).
- Estimation des probabilités d'apparition d'évènements rares.
- Diminution des temps de simulation.

Principe

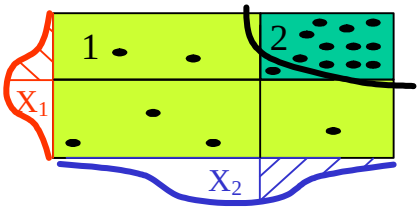
Avant de présenter le principe de la réduction de la variance, il est nécessaire d'introduire la simulation de Monte Carlo :



La méthode de simulation de Monte Carlo consiste à réaliser des tirages aléatoires des valeurs des données d'entrées d'un système (ces données X1, X2,…, Xn étant définies par une loi de probabilité). Pour chaque configuration de valeurs tirées, on évalue la valeur des données de sortie (Y1…, Yn). La répétition des simulations permet d'obtenir des distributions de ces valeurs et, par là même, divers estimateurs dont notamment leur moyenne. Définie par l'intervalle de confiance, la précision des résultats obtenus est liée au nombre de simulations et à la variance des résultats.

Réduction de la variance

La réduction de variance consiste à privilégier un domaine d'intérêt au cours de la simulation puis à pondérer les résultats obtenus par application du théorème des probabilités totales.



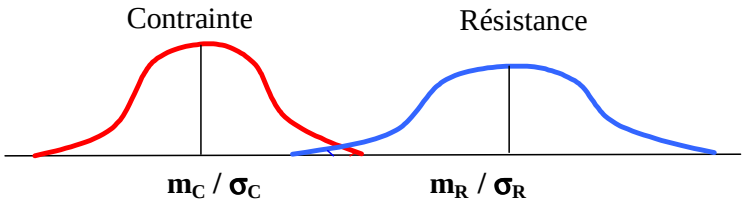
Dans cet exemple, on privilégie les tirages dans la zone 2 (vert foncé) qui correspond à des fortes valeurs de X1 et des faibles valeurs de X2.

Les différentes méthodes utilisées (échantillonnage stratifié et échantillonnage d'importance) sont développées dans cette fiche.

Exemple

La réduction de la variance est bien adaptée à la méthode « résistance / contrainte ». Ce problème consiste à rechercher la probabilité de défaillance d'un matériel de résistance R soumis à une contrainte C. Le matériel est défaillant si C est supérieur à R.

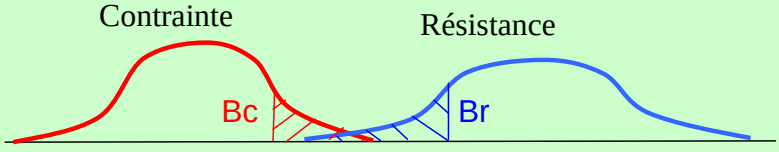
Dans cet exemple, R et C suivent une loi normale de moyenne m et d'écart type σ.



Résistance (R) : moyenne mR=16 *écart type : σR=3*
Contrainte (C) : moyenne mC=8 *écart type : σC=2*

La simulation de Monte Carlo consiste à réaliser des tirages des valeurs de R et C à partir de leur loi de probabilité et à évaluer la probabilité que la contrainte soit supérieure à la résistance.
Pour ce problème, l'espace d'état que l'on souhaite étudier plus particulièrement est celui où l'on a les plus fortes probabilités de défaillance, c'est-à-dire lorsque la contrainte est forte et la résistance est faible. Nous allons donc privilégier les tirages dans cette zone (bornes Br et Bc) et pondérer le résultat de la simulation.

Données



mc :	8	**mr :**	16
σc :	2	**σr :**	3
Bc :	11	**Br :**	12

Résultats

	moyenne	Ecart type	Borne inf.	Borne sup.	Delta
Sans réduction de variance	0,984	0,125537882	0,97747017	0,99052983	0,01305966
Avec réduction de variance	0,986427107	0,026196898	0,98506448	0,987789734	0,002725254

On constate bien une réduction de l'écart type du résultat obtenu et donc un resserrement de l'intervalle de confiance pour un même nombre de simulations.

Conclusion

La formalisation et l'accessibilité des connaissances constituent la clef de toute tentative réussie de diffusion et de capitalisation. La mémorisation d'informations nombreuses sur des dysfonctionnements dus à une même cause apparaît ainsi inutile si une recommandation claire peut être formulée pour éliminer celle-ci. La collecte d'informations sur les incidents est d'ailleurs délicate, notamment quand elle révèle, in fine, des d'erreurs humaines. Outre des enseignements relatifs à des règles ou risques nouveaux, elle ne présente en fait un intérêt qu'à titre d'illustration ou de sensibilisation.
En ce qui concerne les méthodes de calcul et plus particulièrement les méthodes utilisées en probabilité et statistiques, elles sont souvent difficilement accessibles aux profanes. L'information disponible est parcellaire et dispersée, le plus souvent cachée derrière un barrage théorique inutile. Des méthodes indispensables à l'ingénieur sont alors méconnues voire ignorées telles que l'estimation probabiliste, la simulation de Monte-Carlo ou les techniques d'optimisation. On note par ailleurs, dans la plupart des manuels, l'absence de cas d'application concrets entrant véritablement dans les préoccupations des utilisateurs ainsi que de guides méthodologiques (neutres vis-à-vis des phénomènes de mode ou intérêts partisans) les aidant à choisir les méthodes et outils les mieux adaptés à leurs problématiques.

Cette formalisation et présentation du retour d'expérience constituent la finalité de l'outil SAFE qui tente d'apporter aux utilisateurs la facilité d'accès à l'information pertinente quelle soit de nature qualitative, sous forme de listes de risques génériques et de règles associés aux différentes composantes d'un satellite, ou quantitative sous forme de fiches méthodologiques.

L'outil est aujourd'hui pleinement opérationnel et disponible sur l'intranet du CNES. Il permet de tenir compte dès les phases de conception de l'expérience accumulée sur les précédents projets afin de rendre les systèmes plus robustes et de tenir les échéances dans un contexte de réduction des coûts et des délais de développement. Il facilite par ailleurs la réalisation d'analyses quantitatives, soit prévisionnelles pour optimiser les architectures des systèmes et leur exploitation, soit simplement probabilistes en support à la prise de décision. Cet outil est mis à jour périodiquement et pourrait s'enrichir prochainement d'une base de données de fiabilité propres aux équipements spatiaux.

Cette manière originale de formaliser et d'exploiter l'expérience en Sûreté de Fonctionnement peut être transposée à tout autre domaine : aéronautique, automobile, processus industriel...

Références

[1] - FRIEDBERG E., TERSSAC (de) G., Coopération et conception. Toulouse : Editions Octares, 1996, coll. Travail.
[2] - AUPIED J., Retour d'expérience appliqué à la sûreté de fonctionnement des matériels en exploitation. Paris : Editions Eyrolles, 1994.
[3] - Etienne K., Faure J., Laulheret R., Cabarbaye A.. Retour d'Expérience en Sûreté de Fonctionnement dans le Spatial – Lambda mu 2005 - Lille