8ème édition du congrès international pluridisciplinaire
QUALITA 2009 – Besançon (France)
Du 18 au 20 mars 2009

VERS UNE CONVERGENCE DES METHODES D'ANALYSES DE RISQUES DANS LE SPATIAL ET L'AERONAUTIQUE ?

FAURE Julien [1], CABARBAYE André [2&1], LAULHERET Roland [1]

[1] CNES, 18 av Edouard Belin,31401 Toulouse Cedex 04, France
05 61 27 31 31, julien.faure@cnes.fr

[2] CABINNOVATION, 3 rue de la Coquille,31500 Toulouse,France
05 61 54 68 08, andre.cabarbaye@cabinnovation.fr

Résumé :

Dans le spatial, le CNES adopte une approche consistant à identifier par une analyse préliminaire de risques au niveau système, les fonctions critiques, celles-ci étant par la suite étudiées avec des analyses détaillées telles que les AMDEC composants ou les analyses pires cas. Cette communication détaillera la vision d'ensemble développée au CNES au cours des dernières années.

Dans l'aéronautique civile, l'ensemble du processus est basé sur le cycle FHA (Functional Hazard Analysis), PSSA (Preliminary System Safety Assessment) et SSA (System Safety Assessment) qui mène à la certification de l'avion. Cette approche système est ensuite appliquée au niveau de chaque sous-système. Des standards de développement logiciels et matériels existent et sont mis en regard de la criticité des fonctions et donc des systèmes qui les supportent.

Cette approche est un exemple vers lequel le spatial converge, mais d'autres analyses comme les analyses de mode commun, les analyses de zone et les analyses de risques particuliers seraient très profitablement appliquées à notre secteur.

Notre propos sera donc d'exposer les pistes d'avenir que nous allons suivre prochainement, en nous adaptant au contexte de chaque projet.

Abstract:

In space projects, CNES follows a method consisting in performing a system preliminary risks analysis in order to identify the critical functions, that will be targeted by specific analyses such as components FMECA or Worst Case Analysis.

In aeronautics projects, the whole process is based on the FHA (Functional Hazard Analysis), PSSA (Preliminary System Safety Assessment) and SSA (System Safety Assessment) cycle that ultimately leads to the certification of the aircraft. This method is then applied at each sub-system level and allows to identify the criticality of functions that will be developed according to a set of software or hardware standards.

This standardized approach is interesting to follow by space projects and moreover, other analyses such as common cause analysis, zonal analysis or particular risks analysis are key studied to implement on our future developments.

That is what our communication is intending to expose in a bench marking effort between space projects and the aeronautics world.

Mots clés : Risques, analyses, spatial, aéronautique

Keywords : Risks, analysis, space, aeronautics

1 Maîtrise des Risques dans le Spatial

1.1 Contexte des projets spatiaux

Dans le spatial, à l'exception des vols habités, le système étudié qu'il soit satellite ou lanceur est non réparable une fois lancé et doit remplir des exigences de fiabilité élevées. C'est pourquoi des analyses de sûreté de fonctionnement sont prévues tout au long du cycle de développement du projet.

1.2 Définitions

Dans ce qui suit, on distinguera dans le satellite la plateforme qui fournit les différents services tels que l'alimentation électrique, les télécommunications avec le sol ou encore le contrôle d'attitude et d'orbite ; de la Charge Utile qui est à chaque fois un développement spécifique pour une mission donnée. (observation de la terre, étude de l'univers).

De plus, dans le spatial, le terme « système » désigne l'ensemble « satellite + segment sol de contrôle ». De ce fait, on parle d' « équipements » ou de « sous-système » pour les éléments constitutifs du satellite.

1.3 Approche développée par le CNES pour les satellites

La phasage des projets est le suivant, jusqu'au lancement :

Phase 0 : avant-projet ; Phase A : faisabilité technique, Phase B : design préliminaire ; Phase C : design définitif, lancement.

Dès la phase A, le CNES réalise une Analyse Préliminaire de Risques (APR) consistant à déterminer à partir d'événements redoutés de niveau système (ex. perte du satellite) les différentes causes possibles (matérielles, logicielles, humaines). Cette APR permet dès le départ d'identifier les fonctions critiques du satellite sur lesquelles un effort particulier sera porté.

En phase B, grâce à la connaissance d'une architecture préliminaire, notamment électronique, il devient possible de réaliser des AMDE fonctionnelles sur les cartes des équipements nouveaux développés dans la Charge Utile.

En phase C, la définition détaillée de l'architecture permet de mener les analyses nécessaires plus poussées sur les fonctions critiques préalablement identifiées par l'APR et les AMDE fonctionnelles.

Ces analyses approfondies sont des AMDEC de niveau composants, des analyses pire cas et des analyses de derating (part stress) voire des prévisions de fiabilité. Une attention spéciale est donnée aux interfaces entre la charge utile et la plateforme pour étudier les risques de propagation de pannes. Ainsi, les circuits d'interface d'alimentation et d'échange de données sont étudiés à l'aide d'AMDEC composants.

Pour toutes les phases, les équipements récurrents des plateformes sont couverts par des mises à jour de leurs analyses de risques ou AMDE si nécessaire.

1.4 Standards de développement du spatial

Le CNES contribue à l'élaboration des normes européennes ECSS (European Coopération for Space Standardization) avec l'Agence Spatiale Européenne (ESA) et les industriels majeurs du spatial.

Ces standards couvrent les règles de conception et aussi les analyses de sûreté de fonctionnement et de

sécurité.

1.5 Exigences qualitatives et quantitatives

Les exigences qualitatives sont exprimées au niveau de la sécurité des personnes et des biens avec le critère classique de tolérance à la double défaillance pour des événements catastrophiques. (ce qui ce traduit dans le design par la présence de trois « barrières » de sécurité indépendantes.

Les exigences quantitatives sont adaptées au contexte de chaque projet au niveau des performances et au niveau de chaque autorité de lancement (Centre Spatial Guyanais par exemple) pour la sauvegarde. (sécurité des personnes et des biens)

1.6 Echange d'exigences

Des outils logiciels d'échange et de traçabilité des exigences sont progressivement déployés dans les projets. Nous espérons une généralisation à moyen terme.

2 Maîtrise des Risques dans l'Aéronautique

2.1 Contexte des projets aéronautiques

Les projets aéronautiques de transport civil sont régis par le processus de certification JAR / FAR 25 qui est appuyé par les standards ARP 4754 (certification de systèmes aéronautiques à haut niveau de complexité), ARP 4761 (guide et méthodes pour le processus de certification), DO-178B (niveau de développement logiciel ou DAL « Development Assurance Level ») et DO-254 (niveau de développement matériel). Cet ensemble de règles procure un cadre très bien déterminé, mais laisse peu de liberté dans les moyens de démonstration de la sécurité du futur avion.

Ceci est évidemment dû à la nature inacceptable du risque de crash dans l'opinion publique, ce risque doit donc être extrêmement improbable.

Enfin, la caractéristique majeure de l'aéronautique est la présence du pilote, capable de corriger les défaillances du système ce qui peut améliorer la résilience du système.

2.2 Définition

Dans l'aéronautique, le terme « système » désigne un ensemble d'équipements réalisant une même fonction (par ex. les commandes de vol). Seul le terme « avion » est utilisé pour caractériser les analyses relatives à l'ensemble des systèmes assemblés en un tout.

2.3 Méthode d'étude des risques

Chaque système de l'avion est étudié selon le cycle suivant :

En phase A et B, une analyse de risques fonctionnels (FHA pour Functional Hazard Analysis) est menée. Elle identifie les conséquences des défaillances de chaque fonction du système en cas de perte, de déclenchement intempestif ou de fonctionnement erroné. L'échelle de classification des risques illustre leur impact sur la sécurité des passagers et la charge de travail de l'équipage.

En phase C, grâce au design détaillé disponible, la FHA évolue en PSSA (Preliminary System Safety Assessment) qui enrichit l'analyse par le calcul des probabilités d'occurrence des événements redoutés.

Avant la certification, la PSSA mûrit en SSA (System Safety Assessment), ce qui illustre que les points à confirmer ont tous été consolidés.

A chaque étape, les concepteurs et aussi les pilotes sont mis dans la boucle de validation des analyses de sécurité.

En parallèle la même analyse est menée au niveau de l'avion complet. Elle s'enrichit au fur et à mesure des résultats qualitatifs et quantitatifs des analyses des systèmes.

Enfin, des analyses de causes communes sont menées pour toutes les fonctions critiques : Analyse de mode commun (électriques, thermiques), analyse de zone (défaillance affectant un système proche), analyse de risque particulier (foudre, éclatement de pneu etc.)

2.4 Exigences qualitatives et quantitatives

Au niveau de chaque système, selon la criticité de chaque fonction, un objectif qualitatif (règles de développement logiciel et matériel) et quantitatif lui est alloué (par ex. 10^-9 par heure de vol pour un événement catastrophique mettant en jeu la sécurité du vol). Les tables de conversions sont standardisées pour tous les projets.

Au niveau de l'avion, l'objectif quantitatif tient compte de la somme des contributeurs possibles à ce même événement, et donc est fixé à 10^-7 par heure de vol.

Il est important de noter qu'étant donné l'importance du trafic aérien, les événements très rares considérés sont malheureusement observables.

Enfin, on notera également qu'une des forces des designs d'avion est la dissymétrie des redondances, qui permet de s'affranchir des modes de pannes communs. Ainsi, le système de navigation principal, outre le fait qu'il est redondé, est secondé en cas d'urgence par un système plus basique mais cependant suffisant pour assurer un retour vers l'aéroport le plus proche en toute sécurité.

2.5 Echange d'exigences

Le processus d'échange des exigences de sécurité est bien rôdé. Cela permet de diffuser et valider le respect d'exigences envers l'ensemble des systèmes utilisateurs d'une ressources comme l'alimentation électrique par exemple.

3 Approches à retenir pour les projets de satellites

3.1 Une adaptation du processus avion au contexte satellite

Afin de préserver une certaine flexibilité dans la gestion des risques, et surtout pour tenir compte des caractéristiques de l'objet étudié, à savoir le satellite, objet inhabité, il est intéressant d'examiner les possibilités de simplification du processus de certification avion comme dans [Audard] qui s'est penché sur le cas des drones. Cette piste sera certainement à considérer dans notre approche car une application stricte est totale des référentiels aéronautique n'a pas de sens.

3.2 Echange des exigences

La convergence est déjà en cours. D'ici quelques années nous espérons avoir standardisé le processus.

3.3 Standards de développement

Les standards de développement du spatial ont déjà évolué dans le domaine logiciel afin de formaliser les niveaux de développement logiciel en fonction de la criticité de ces derniers. En revanche, cela ne semble pas être le cas pour le matériel, surtout électronique.

3.4 Analyses des causes communes et résilience des systèmes

C'est certainement la piste la plus intéressante à l'heure actuelle. En effet, si ces analyses sont menées au niveau des lanceurs, elles ne le sont que très rarement au niveau des satellites. Ceci est dû au contexte des projets qui ont des architectures de plus en plus simplifiées dépourvues de redondances (l'accent ayant été mis sur l'augmentation de la fiabilité intrinsèque). Dans ces circonstances, l'étude de modes de défaillance susceptibles d'affecter les deux éléments d'une redondance perdent leur pertinence.

Cependant, deux facteurs clés tendent à infléchir cet état de fait : premièrement le risque des débris spatiaux et deuxièmement la sensibilité accrue des électroniques aux radiations.

Les derniers mois ont vu une augmentation significative des risques d'impact de débris spatiaux sur les satellites évoluant en orbite basse. Par rapport à 2005, le risque a été multiplié par … (source CNES)

Les débris de grande taille peuvent être détectés et évités suffisamment tôt. Cependant, les débris d'une taille caractéristique inférieure à 1 cm, tels les particules de peintures, sont indétectables mais peuvent occasionner des dommages conséquents. C'est pourquoi, il semble urgent d'envisager d'améliorer la robustesse des architectures de satellites avec l'installation de redondances bien séparées spatialement dans le satellite lui-même.

Concernant les composants électroniques, la diminution de leur finesse de gravure augmente sensiblement leur sensibilité aux radiations. Des analyses poussées sont menées à chaque fois afin de les qualifier vis-à-vis du risque radiation (induisant un fonctionnement erroné voire une perte du composant). Ne pourrait-on pas envisager une dissymétrie des architectures avec des redondances basées sur des technologies plus robustes, à l'image de ce qui se fait sur un avion où les commandes de vols électriques sont secondées en cas d'urgence par un circuit hydraulique de secours ?

Ceci nous amène à dépasser le cadre de la sûreté de fonctionnement pure pour aborder la notion de résilience des systèmes, soit leur capacité à survivre à des événements imprévisibles a priori lors de leur conception, comme il est montré dans [Gajewski].

4 Conclusion

De manière pragmatique, il y a certainement des éléments à reprendre de la maîtrise des risques dans l'aéronautique, comme tout ce qui va dans le sens de la standardisation des pratiques. Cependant, dans le spatial, chaque projet souhaite conserver la liberté d'adapter les exigences à ses besoins. C'est ici que l'on constate que notre domaine reste encore une industrie de prototypes et reste loin des grandes séries de l'aéronautique.

Enfin, on retiendra comme proposition porteuse d'avenir les recherches sur la résilience des systèmes spatiaux dont la garantie de fonctionnement est de plus en plus vitale aux intérêts de la société moderne. (Internet, télécommunications, navigation et positionnement, imagerie, météorologie)

C'est dans cette optique et afin de continuer à développer la vision système procurée par l'Analyse Préliminaire de Risques que nous serons moteurs dans l'implémentation croissante des analyses de modes communs et de robustesse d'architecture de nos satellites.

Références

Articles

[Audard] Audard C. , *Innovative Methodology for Safety Assessment of medium to large civil Unmanned aerial vehicle*. EURO-UAV 2006

[Gajewski] Gajewski, Bezard, Cabarbaye. *De la Sûreté de Fonctionnement à la Résilience des Systèmes*. Lambda Mu 16, Avignon, 07-09.10 2008.

Normes et standards de développement

Spatial

[European Cooperation for Space Standardization], *ECSS-Q-30B: Dependability*, 08.03.2002

[European Cooperation for Space Standardization], *ECSS-Q-40B: Safety*

[European Cooperation for Space Standardization], *ECSS-Q-80B Software Product* Assurance,10.10.2003

[European Cooperation for Space Standardization], *ECSS-Q-80C Software Product Assurance DRAFT2*, 15.02.2008

[ISO], *ISO 14620-1: "Space Systems Safety Requirements"*

Aéronautique

[RTCA], *DO-178B: Software considerations in airborne systems and equipment certification*, 26.03.1999

[RTCA / EUROCAE], *DO-254: Design Assurance Guidance for Airborne Electronic Hardware, 04.2000*

[SAE], *ARP 4754: Certification considerations for highly-integrated or complex aircraft systems*, 11.1996

[SAE], *ARP 4761: Guidelines and methods for conducting the safety assessment process of civil airborne systems and equipment*, 12.1996