DOSSIER DE SECURITE " AGILE " APPLIQUE AU SOUS-SYSTEME AVIONIQUE DU STRATOBUS™

Léa Dumont, Gilles Lecadre, Virginia Hettiger

DOSSIER DE SECURITE « AGILE » APPLIQUE AU SOUS-SYSTEME AVIONIQUE DU STRATOBUS™

"AGILE" SAFETY DOSSIER APPLIED TO THE AVIONIC SUBSYSTEM OF THE STRATOBUS™

Léa DUMONT
LIGERON Toulouse
8, rue Edouard Serres - BP 320
31700 COLOMIERS
05 62 74 30 14
lea.dumont@ligeron.com

Gilles LECADRE
THALES ALENIA SPACE France
26 avenue J.F. Champollion
31037 Toulouse Cedex 1 – France
05 34 35 63 95
gilles.le-cadre
@thalesaleniaspace.com

Virginia HETTIGER
THALES ALENIA SPACE France
26 avenue J.F. Champollion
31037 Toulouse Cedex 1 – France
05 34 35 43 44
virginia.hettiger
@thalesaleniaspace.com

Résumé

L'objet de cet article est de présenter une approche de structuration des données mise en œuvre pour établir le dossier de sûreté de fonctionnement d'un système à la fois innovant et complexe. Sur de tels projets, il n'est pas possible d'utiliser les démarches classiques de réutilisation des études antérieures, et il est nécessaire en revanche de pouvoir rapidement donner des orientations aux architectes du système.
Sur le sous-système avionique du Stratobus™, il a été possible de mettre en œuvre une modélisation fonctionnelle et dysfonctionnelle autours d'une base de données, permettant de rééditer plus facilement le dossier de sécurité en cas de modification d'architecture ou d'évolution des exigences, ce qui est courant dans les phases amont des projets.

Summary

The purpose of this article is to present a data structuration approach implemented to establish the dependability dossier of a system at the same time innovative and complex. On such projects, it is not possible to use classical approaches of reusing previous studies, and it is however necessary to be able to give quickly orientations to the system architects.
On the avionic subsystem of the Stratobus™, it has been possible to implement functional and dysfunctional modeling around a database, making it easier to republish the safety file in the event of architectural modifications or changes in requirements, which is common in the upstream phases of projects.

1 Objectifs

Cette communication a pour objet de partager une expérience de mise en œuvre d'une approche efficace de structuration des données d'analyse dysfonctionnelle sur un système très innovant et complexe.

2 Contexte

« Stratobus™ est une plateforme stratosphérique autonome multi-missions, que l'on peut situer à mi-chemin entre un drone et un satellite. En rupture technologique par rapport aux systèmes existants, Stratobus fait partie de la famille des HAPS [High Altitude Pseudo Satellite]. L'engin, destiné à des missions localisées, est un parfait complément du satellite traditionnel. Conçu pour évoluer à 20 kilomètres d'altitude (au-dessus des jet-streams et du trafic aérien), il est destiné à des applications régionales – civiles et/ou militaires – adaptées à différents domaines : télécommunications, navigation, observation (surveillance en particulier…). » [2].

Figure 1. Vue générale du Stratobus

Les phases de décollage et d'atterrissage en particulier font de cet engin un aérostat dont la sécurité d'exploitation devra être démontrée auprès des Autorités de Certification (EASA). Le référentiel de certification applicable nécessite de déployer des approches de Sûreté de Fonctionnement de type PSSA – SSA [1].

Le sous-système avionique du Stratobus™ joue un rôle central dans le pilotage autonome ou manuel de l'aérostat. Il corrige en permanence la flottabilité, les moteurs et les gouvernes en fonction des paramètres de navigation et de mission. Il gère également les défaillances et les reconfigurations du Stratobus™ en liaison avec les opérateurs de la station sol.
Ce sous-système avionique présente de très nombreuses interfaces internes et externes (capteurs, actionneurs, communication sol / bord, gestion de l'énergie). Il met en œuvre de nombreux matériels (hardwares) et logiciels (softwares).

Ce projet présente la particularité d'être très innovant, en particulier du point de vue du temps de mission et de la gestion de l'énergie. Cela signifie, qu'en cours de conception préliminaire, de fréquents changements d'architecture surviennent, en fonction de l'état de maturité des solutions technologiques disponibles pour l'ensemble des sous-systèmes de l'aérostat.

Un autre enjeu est de pouvoir disposer rapidement de spécifications claires au niveau des produits matériels et logiciels ainsi qu'aux interfaces, intégrant dès la première itération les exigences de sécurité, et d'en assurer la traçabilité tout au long du projet.

Par rapport à ceux classiquement utilisés en aéronautique, l'approche et les outils pour réaliser la PSSA (Preliminary Sub-System Safety Assessment) doivent être ré imaginés, pour atteindre une grande efficacité de mises à jour, et devenir également une aide à la décision.

3 Méthode

Conformément à la démarche PSSA existant dans les référentiels normatifs aéronautiques [1], le point de départ de l'analyse est une liste d'évènements redoutés (« Failure Conditions ») identifiés au plus haut niveau (système aérostat) puis assignés, pour un certain nombre d'entre eux, au sous-système avionique. Pour chaque évènement redouté est assigné, en fonction de sa gravité, deux types d'exigence : probabilité maximale acceptable et niveau de qualité de développement (DAL : Development Assurance Level).

A partir de l'architecture et des fonctions du sous-système avionique et des sous-systèmes environnants, il a fallu pouvoir établir rapidement un premier ensemble cohérent d'AMDEC et d'arbres de défaillances (FTA : Fault Tree Analysis) afin d'initier très tôt le dialogue avec l'Equipe Projet, notamment concernant les points durs, ou encore la consolidation des architectures.

Cela a été rendu possible en mettant en œuvre de manière conjuguée :

- une **base de données relationnelle**,
- des **processus automatisés pour les analyses dysfonctionnelles**,
- et des **processus de publication des données**.

Ces trois outils sont présentés ci-dessous, avec quelques exemples d'illustration.

3.1 Base de données relationnelle

La base de données relationnelle est utilisée pour stocker essentiellement les données d'entrée constitutives de l'architecture, des fonctions, ainsi que les exigences assignées au sous-système :

- Modélisation de l'architecture (arborescence produit, routage des flux fonctionnels, redondances chaudes et froides) et traçabilité des hypothèses ;
- Modélisation fonctionnelle orientée analyse de flux (Matière, Energie, Information) ;
- Enregistrement des exigences système (probabilité et DAL associés à chaque Failure Condition) et des exigences assignées aux produits (taux de défaillance, détection, …).

Le diagramme ci-dessous constitue une représentation simplifiée de la structure de la base de données.

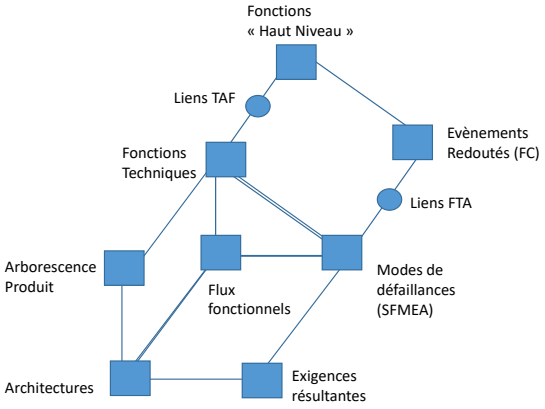

Figure 2. Structure schématique de la base de donnes

L'analyse fonctionnelle est un préalable classique dans les analyses de Sûreté de Fonctionnement. Mais ici la nouveauté réside dans l'analyse formelle des flux entrants ou sortants de chaque fonction. Du point de vue des défaillances, une table de paramétrage permet d'analyser différemment chaque type de flux : matière, énergie, ou information.

Par exemple, les liens entre les tables Arborescence Produit, Fonctions Techniques, Flux fonctionnels permettent d'obtenir un affichage en cascade de ces données tel que ci-dessous :

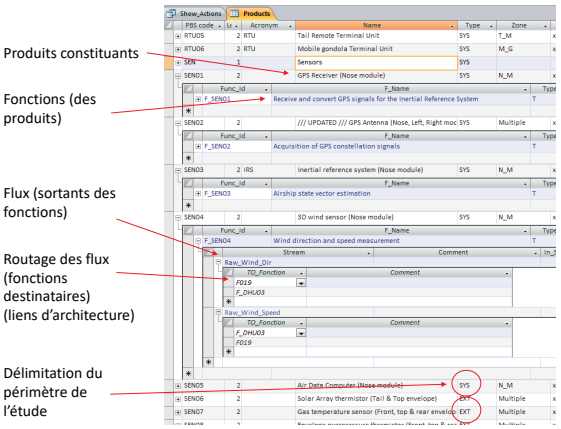

Figure 3. Exemple d'affichage des données : produits – fonctions - flux

Dans cet exemple la fonction « F_SEN04 : Wind direction and speed measurement » présente 2 flux sortants qui sont « Raw_Wind_Dir » et « Raw_Wind_Speed » (la vitesse et la direction du vent).
L'association d'une fonction et d'un flux est appelée « connexion », sachant qu'un flux peut transiter par plusieurs fonctions. C'est au niveau de chaque connexion

qu'on réalise l'analyse AMDEC. Plus une fonction émet de flux différents, plus elle porte de nombreux modes de défaillance potentiels.

Les flux sont de plusieurs natures possible : Matière, Energie ou d'Informations, produits par chaque fonction.

Le lien entre les fonctions techniques et les fonctions de haut niveau matérialise le Tableau d'Analyse Fonctionnel (TAF). Mais ici, le lien prend en compte également les flux fonctionnels.

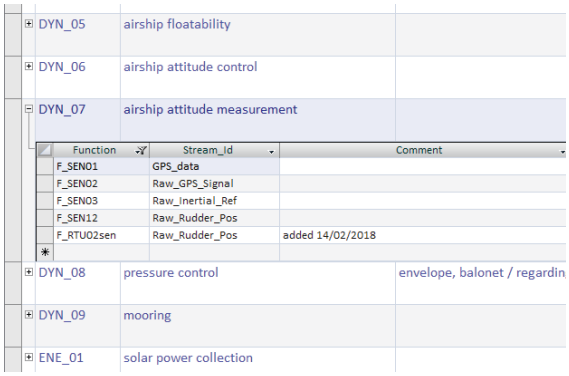

Figure 4. Exemple d'affichage des données TAF

Ce travail permet de modéliser les impacts système de chaque fonction technique, et sera utilisé ensuite dans la modélisation des effets de l'AMDEC, ainsi que pour la construction des arbres (FTA).

3.2 Processus automatisés pour les analyses dysfonctionnelles

Les processus automatisés sont utilisés pour pallier le caractère long et répétitif des analyses de dysfonctionnement sur un système complexe. Cette automatisation permet en outre d'apporter de la répétabilité et de la rigueur :

- Génération semi-automatique des modes de défaillance fonctionnelle, de leurs effets locaux, et effets de niveau aérostat.
- Génération semi-automatique des liens causes – effets pour la préparation des arbres de défaillance.
- Génération des exigences de sécurité assignées aux produits et de leurs justifications.

L'automatisation de l'identification des défaillances fonctionnelles est permise par l'analyse des flux décrite plus haut. La génération du libellé des modes de défaillance est paramétrable.

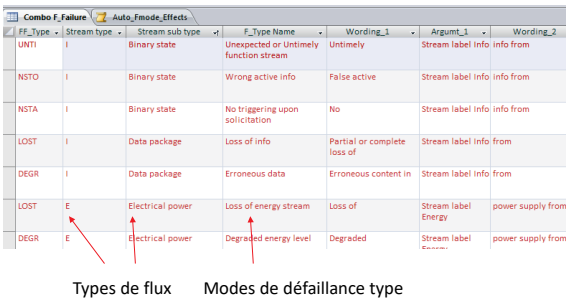

Figure 5. Table de paramétrage des modes de défaillance

En fonction du type de flux fonctionnel, une liste de modes type est pré déterminée par l'utilisateur.
En croisant cette table de paramétrage avec la table des connexions (liens flux-fonctions), une requête SQL de type jointure permet de générer la liste des modes de pannes potentiels, c'est-à-dire les premières colonnes de l'AMDE.

Ensuite une séquence de requêtes de type mise à jour permet de compléter les effets de chaque mode :

- par jointure avec la table de routage des flux pour les effets locaux,
- par jointure avec la table de liens TAF pour les effets finaux.

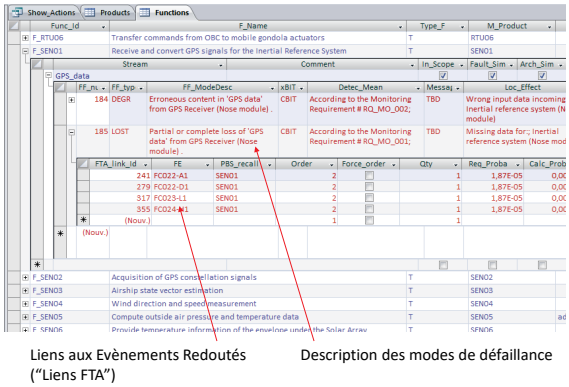

Figure 6. Lignes d'AMDE générées pour chaque connexion fonctionnelle

Une autre requête jointure avec les liens TAF permet de générer une première version des liens entre modes de défaillances et évènements redoutés (liens FTA). Cette table est retravaillée ensuite manuellement par l'analyse SDF si besoin.

Pareillement, l'AMDE générée est ensuite relue et corrigée manuellement pour certains cas particuliers.

A partir de ces premières analyses, il devient possible de générer deux types d'exigences de sécurité pour chaque mode de défaillance :

- Exigences quantitatives : probabilité et taux de défaillances requis en fonction de la gravité des évènements redoutés (CAT, HAZ, MAJ, MIN). Cette allocation est générée par une séquence de requêtes, en fonction de la table de liens FTA et des redondances existantes.
- Exigences qualitatives et hypothèses : détection ; reconfiguration ; architecture ; maintenance. Ces exigences sont rédigées manuellement de manières regroupées et assignées par une table de liens aux différents modes.

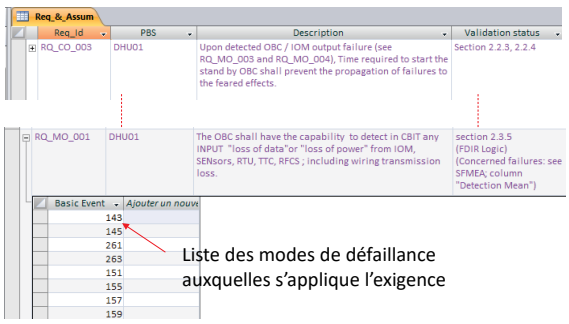

Figure 7. Exigences qualitatives et liens d'application sur les modes.

Un processus similaire permet de faire automatiquement une allocation du niveau de DAL requis pour chaque

fonction : la table de liens FTA permet en effet, par requête jointure, de déterminer la participation de chaque fonction dans chaque évènement redouté, et du niveau de gravité de ce dernier [1].

Pour toutes les exigences (qualitatives et quantitatives), une série de requêtes utilisant la table liens FTA permet de générer le champ « rationale », c'est-à-dire le lien de traçabilité de l'origine des exigences, tel que demandé dans les référentiels aéronautiques type ARP [1].

3.3 Processus de publication

Les processus de publication permettent de faciliter la construction des arbres de défaillance et de générer les éléments démonstratifs du dossier PSSA :

- Listing d'Analyse Fonctionnelle permettant de valider la modélisation.
- Listings structurés d'Arbres de Défaillance et exportation des évènements de base, permettant de charger efficacement l'outil d'Arbres de Défaillance (dans le cas du projet : FTA Pro).
- Synthèses structurées des scénarios d'évènements redoutés.
- Edition des exigences de sécurité assignées aux produits : taux de défaillance, commande-contrôle, architecture, niveaux de DAL, contrôle périodiques.

Ces publications sont des rapports générés en .pdf ou .rtf, basés sur des requêtes qui lisent les tables de la base de données relationnelle.
Ces rapports, exportés en .rtf peuvent également être copiés facilement dans le document Word du dossier PSSA.

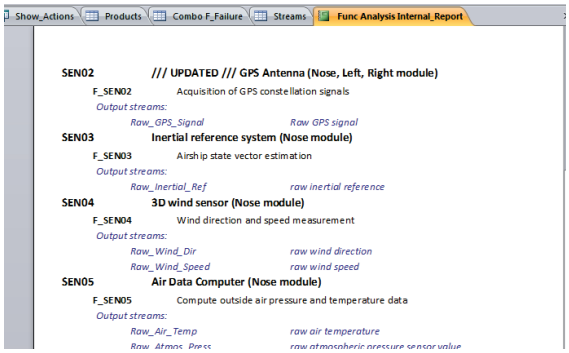

Figure 8. Listing d'Analyse Fonctionnelle (fonctions et flux associés aux équipements)

Pour publier les arbres de défaillance le processus est plus complexe.
Une base de données additionnelle reconstruit l'arbre en utilisant une modélisation type, qui est adapté selon le type d'architecture :

- Equipement simple (non redondé) ou groupe fonctionnel : porte OU ;
- Equipement en redondance chaude : porte ET simple ;
- Equipement en redondance froide (avec élément de commutation) : combinaison ET / OU.

Ce processus de publication est plus complexe et fait appel à des propriétés récursives utilisables dans les requêtes SQL : une table peut être reliée en jointure à elle-même.

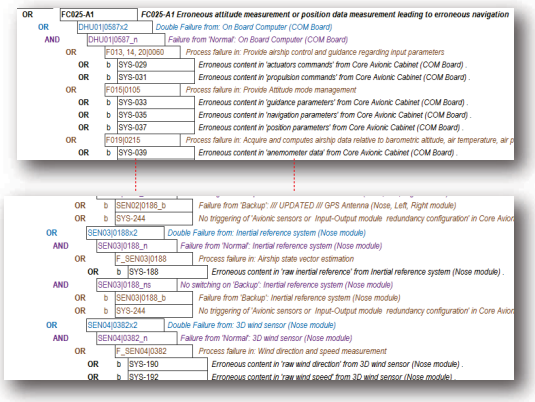

Figure 9. Listing structuré d'Arbre de Défaillance

Dans ce processus de publication on dispose d'un principe de numérotation des portes permettant de repérer de manière simple et originale les groupes de défaillances identiques permettant de constituer les branches communes (évènements renvois) dans les Arbres de Défaillance.
Dans l'exemple de la figure 9, la porte « F015|0105 » a été nommée « 0105 » en faisant la somme des n° des modes de défaillance concernés (033 + 035 + 037) ; le préfixe F015 étant tout simplement l'identifiant de la fonction concernée.
Cet identifiant pourra être considéré comme univoque par l'analyste SDF, ce qui lui facilitera le recours à des renvois lors de la construction des arbres dans l'outil d'Arbres de Défaillances.

L'outil de publication comporte également une option d'exportation des évènements de base, au format .XML attendu par FTA Pro. Seul le traçage des liens entre les portes reste à faire manuellement.

Enfin, pour aider l'analyste SDF à réaliser la synthèse des scénarios d'évènements redoutés dans le rapport PSSA, un rapport permet de publier au format .rtf une structuration de chaque évènement redouté, en se limitant à la défaillance des groupes fonctionnels (voir exemple figure suivante).

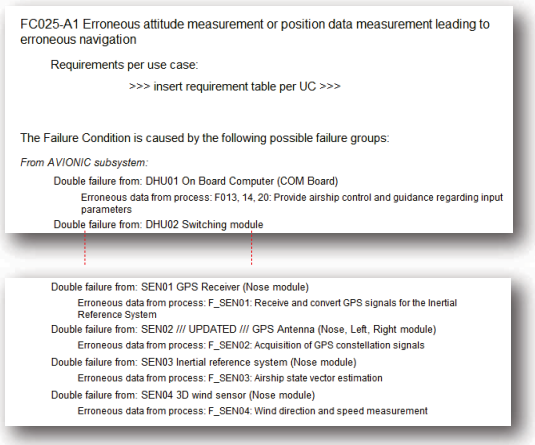

Figure 10. Listing structuré des scénarios d'évènements redoutés

Ainsi, après mise à jour d'une donnée d'architecture, l'ajout ou la suppression d'une fonction ou d'un flux dans la base de données, il devient facile de rééditer

rapidement ces listings et d'établir une mise à jour d'un rapport PSSA.

3.4 Exemples de mises à jour « agile » du Dossier de Sécurité

Dans le présent article nous utilisons le vocable « agile » dans son acception courante : flexible ; adaptable.

Les exemples ci-dessous sont des cas d'évolution courants dans les projets.

Bien que fictifs, les exemples développés ici sont des modifications encore couramment rencontrés dans la phase actuelle du projet Stratobus™. Sans les outils présentés plus haut, chaque évolution pourrait nécessiter un temps de mise en œuvre beaucoup plus long, sans réelle garantie de cohérence des données.

Exemple 1 : Evolution de la FHA.

Dans cet exemple nous nous intéressons à l'évènement redouté (« Failure Condition ») suivant :
FC025-A1: Erroneous attitude measurement or position data measurement leading to erroneous navigation.

Initialement les fonctions contributrices sont les suivantes (extrait) :
Haut niveau :
DYN_07 airship attitude measurement :
Connexions contributrices (fonctions techniques et flux, extrait partie capteurs) :
...
F_SEN03 Raw_Inertial_Ref
...
PLA_02 position measurement
Connexions contributrices (fonctions techniques et flux, extrait partie capteurs) :
F_SEN02 Raw_GPS_Signal
F_SEN04 Raw_Wind_Dir
F_SEN04 Raw_Wind_Speed
...

La modification correspond à une évolution du libellé de l'évènement redouté qui devient :
FC025-A1: Erroneous position data measurement leading to erroneous navigation.
Egalement son niveau de criticité passe de HAZ (hazardous) à MAJ (major).

Outre l'impact sur les exigences de probabilité ; cette modification supprime toutes les contributions de la fonction de haut niveau « DYN 07 » dans les tables de lien FTA et liens FC – Fonctions de Haut Niveau.

Avant application de la modification, la branche SEN03 est présente (car contribue à DYN07) :

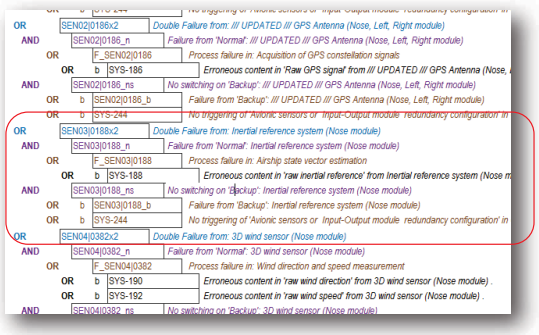

Figure 10. Listing structuré FTA / branche SEN03 présente

Après application de la modification, la branche SEN03 ne doit plus faire partie du développement de l'arbre, puisque DYN07 n'est plus traité :

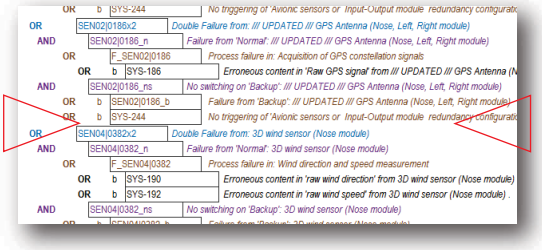

Figure 11. Listing structuré FTA / branche SEN03 supprimée

D'autre part, Initialement les probabilités de défaillance (sur la durée d'exposition) assignés aux modes de F_SEN02 sont :

FF_num	Req_Proba
186	1,92E-05
187	1,87E-05

Tableau 1. Probabilités assignées aux modes (exemple)

Après application de l'évolution l'exigence de probabilité assignée au mode n°186 passe à $6{,}17^{E}$-05 pour sa seule contribution à l'évènement redouté FC025-A1 passé MAJ. Mais comme des contributions de l'évènement de base 186 apparaissent dans 3 autres arbres HAZ, la valeur finale assignée reste inchangée.

La probabilité assignée au mode n°187 reste inchangée également, mais simplement parce que ce mode ne contribue pas à l'évènement redouté FC025-A1.

Exemple 2 : Réassignation d'une fonction ou d'un flux

Cet exemple correspond au cas d'une fonction qui n'est plus réalisée par le même produit dans le sous-système ; ou lorsqu'un flux est produit par une autre fonction.

L'équipement SEN15 : Static pressure sensor (Nose module) est supprimé.
Sa fonction F_SEN15 : Provide static pressure information est désormais portée par l'équipement SEN05 Air Data Computer (Nose module).

Il est très simple de procéder à cette modification : Dans la table de fonctions, il suffit de changer l'identifiant du produit qui porte la fonction :
M_Product = « SEN15 » devient M_Product = « SEN05 ».
Implicitement le flux « Raw_Atmos_Press » reste associé à la fonction, même si elle est portée par un autre équipement.

Initialement le libelle des modes de défaillance de « SEN15 » se présentent comme suit :

FF_num	FF_ModeDesc
218	Erroneous content in 'raw atmospheric pressure sensor value' from Static pressure sensor (Nose module) .
219	Partial or complete loss of 'raw atmospheric pressure sensor value' from Static pressure sensor (Nose module) .

Tableau 2. Modes de « SEN15 », avant

Après application de l'évolution et lancement de la séquence de mise à jour l'AMDE, les mêmes modes de pannes sont libellés différemment. Les n° de modes sont inchangés, mais désormais rattachés à l'équipement SEN05 :

FF_num	FF_ModeDesc
218	Erroneous content in 'raw atmospheric pressure sensor value' from Air Data Computer (Nose module)
219	Partial or complete loss of 'raw atmospheric pressure sensor value' from Air Data Computer (Nose module)

Tableau 2. Modes de « SEN05 », après

Le libellé "…from Air Data Computer" est correct. On voit toutefois que le libellé long du flux 'raw atmospheric pressure sensor value' mérite d'être changé en 'raw atmospheric pressure value' plus simplement. Au lieu de changer le libellé dans l'AMDEC, on le change directement le libellé dans la table des flux. La mise à jour du nom du flux, dans toutes les lignes de l'AMDEC concernés sera automatique.

Exemple 3 : Modification du périmètre sous-système :

Dans cet exemple, il s'agit d'un produit initialement inclus dans le périmètre du sous-système est désormais considéré comme milieu extérieur, en interface.

L'équipement SEN14 : Outside temperature sensor est désormais sorti du périmètre avionique.

Pour réaliser la modification, on change, Dans la table Produits, la valeur de Type qui devient "EXT" au lieu de "SYS".

Après application de la mise à jour, le préfixe de l'identifiant des modes évolue :

FF_num	FF_ModeDesc
EXT-216	Erroneous content in 'raw air temperature' from Outside temperature sensor (Nose module) .
EXT-217	Partial or complete loss of 'raw air temperature' from Outside temperature sensor (Nose module) .

Tableau 3. Modes de défaillance, désormais aux interfaces

Le préfixe « EXT » permet d'identifier que ces modes sont externes, en interface avec le sous-système étudié.

Néanmoins les exigences de monitoring et de contrôle (pour la détection & reconfiguration) # RQ_MO_002 et # RQ_MO_001 sont toujours applicables au sous-système avionique, car les flux sont rentrants (ce sera à l'avionique de détecter les défaillances et d'engager les reconfigurations).

Exemple 4 : Modification d'une redondance :

Dans ce type de modification, une redondance de produit est supprimée, ou encore, son type de redondance est modifié.

L'équipement SEN03 : Inertial reference system est passé en redondance chaude (ou statique), alors qu'il était en redondance froide (ou dynamique : avec élément de commutation).

Pour réaliser la modification, on change, dans la table Produits, la valeur de champ « Cold_Red » qui devient « False » au lieu de « True ».

Avant la modification, l'arbre de défaillance la Failure Condition « FC030-H1 : Loss of processing to determine navigation state vector » se présente comme suit en ce qui concerne la branche de l'équipement SEN03 :

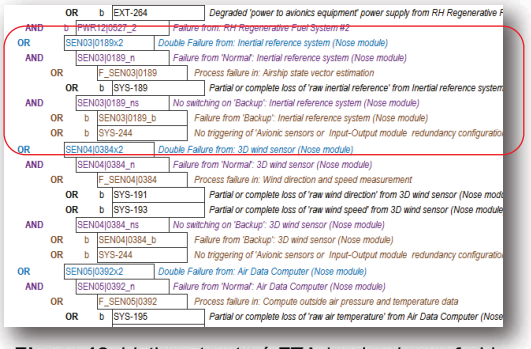

Figure 12. Listing structuré FTA / redondance froide

Dans l'état initial, la branche SEN03 fait bien appel à la défaillance d'un élément de commutation (typique d'une redondance froide).

Après application de la modification, la même branche ne fait plus apparaître l'élément de commutation. La branche est caractéristique d'une redondance chaude.

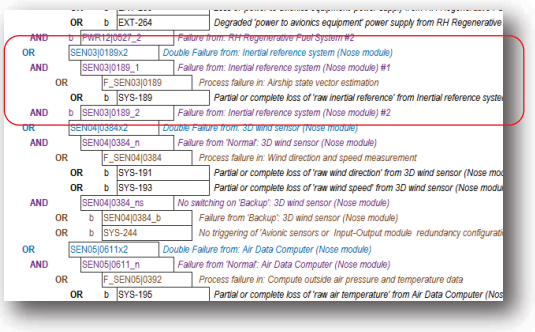

Figure 13. Listing structuré FTA / redondance chaude

Exemple 5 : modification de l'architecture :

Dans cet exemple, le routage d'un flux fonctionnel est modifié.

Le flux fonctionnel "Raw_Air_Temp" de l'équipement SEN14 "Outside temperature sensor" n'est plus désormais envoyé dans l'équipement SEN05 "Air Data Computer (Nose module)", mais uniquement au calculateur central.

Pour mettre en œuvre cette modification, nous ouvrons la table architecture qui définit le routage des flux fonctionnels. On filtre sur le flux "Raw_Air_Temp" et on supprime la ligne qui contient : TO_Function = « F_SEN05 ». On vérifie que les autres lignes correspondent bien à un envoi du flux au calculateur central.

Avant modification, les modes et effets locaux des défaillances de SEN05 se présentent comme suit :

FF_num	FF_ModeDesc	Loc_Effect
216	Erroneous content in …	Wrong input data incoming to:; OBC (On Board Computer) (COM Board); Input output module; Air Data Computer (Nose module)
217	Partial or complete loss of …	Missing data for:; OBC (On Board Computer) (COM Board); Input output module; Air Data Computer (Nose module)

Tableau 4. Modes de défaillance, avant changement du routage des flux

Après application de l'évolution et lancement de la séquence de mise à jour de l'AMDE, les effets locaux des mêmes modes de pannes sont libellés différemment :

FF_num	FF_ModeDesc	Loc_Effect
216	Erroneous content in …	Wrong input data incoming to:; OBC (On Board Computer) (COM Board); Input output module
217	Partial or complete loss of …	Missing data for:; OBC (On Board Computer) (COM Board); Input output module

Tableau 5. Modes de défaillance, après changement du routage des flux

On constate qu'il n'est plus fait mention de « Air Data Computer (Nose module) » dans les effets locaux (donc SEN05 n'est plus impacté localement par la défaillance).

4 Résultats

Très concrètement cette approche a permis d'effectuer dans un temps assez court plusieurs mises à jour des analyses préliminaires de sécurité (PSSA), après des évolutions significatives des architectures. Le temps investi dans l'analyse fonctionnelle orientée flux est très rapidement amorti par la suite.

L'approche démontre la possibilité d'effectuer des mises à jour cohérentes et synchronisées sur un sous-système de complexité significative. Parmi l'ensemble des exigences « safety » générées (près de 350 sur ce sous-système), il est possible que certaines ne puissent être tenues et feront l'objet d'une négociation. L'outil et les processus mis en place facilitent la conduite des « trade-off » concernés.

Les processus semi automatiques apportent également une rigueur et une répétabilité de l'analyse. Néanmoins, le jugement de l'analyste SDF reste indispensable pour interpréter les résultats et corriger les points singuliers.

Tout ce qui n'est pas justifié doit être proscrit : cet adage du management de projet s'applique particulièrement au contexte, lorsqu'on connait le coût de mise en œuvre de certaines exigences de sécurité. L'édition de la justification de chaque exigence, permise par les processus de publication, donne à l'Equipe Projet les clés d'une approche de type Analyse de la Valeur : plusieurs solutions techniques peuvent satisfaire les exigences de sécurité. Mais le critère de la masse embarquée et du coût global de possession seront décisifs par la suite.

Dans la suite du projet, il est également possible de voir d'autres applications de cette modélisation fonctionnelle et dysfonctionnelle du sous-système. D'autres requêtes d'édition pourront permettre de construire les logiques de détection et de localisation des défaillances, et ainsi d'établir les bases des processus de reconfigurations automatique et les manuels de « trouble-shooting ».

5 Remerciements

Les auteurs tiennent à remercier MM. Guy GREGORIS et Damien FORESTIER de Thalès Alénia Space pour leur regard bienveillant sur ce travail, et sur cet article.

6 Références

[1] SAE ARP 4761 - guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment.

[2] https://www.thalesgroup.com/fr/monde/espace/news/quoi-de-neuf-pour-stratobus