Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Définition d'une synergie entre une méthode et un outil pour une étude MBSA

Definition of a synergy between a method and a tool for an MBSA study

MONTEIL Laurène
Safran Aircraft Engines
Réau 77550 Moissy-Cramayel
laurene.monteil@safrangroup.com

AULNETTE Rudy
Safran Aircraft Engines
Réau 77550 Moissy-Cramayel
rudy.aulnette@safrangroup.com

DE BOSSOREILLE Xavier
Airbus Protect
31700 Blagnac
xavier.de-bossoreille@airbus.com

SAGASPE Laurent
Airbus Protect
31700 Blagnac
laurent.sagaspe@airbus.com

Résumé *— Cet article expose une méthodologie pour la conception, la validation et la vérification d'un modèle MBSA (Model-Based Safety Analysis), en s'appuyant sur l'outil SimfiaNeo d'Airbus Protect. Nous revenons sur la nécessité pour un industriel aéronautique de mettre en place des processus permettant de renforcer la confiance dans les analyses de sûreté de fonctionnement complexes portées par des modèles à propagation de panne. Au-delà de la méthode, nous nous attardons également sur l'implémentation de cette dernière, et la manière dont l'outil de modélisation permet d'articuler les besoins d'un motoriste comme Safran Aircraft Engines. Un exemple d'une étude de zone vient illustrer les synergies qui peuvent être trouvées entre la méthode et l'outil pour servir les études de sécurité. Enfin, les résultats permettent d'ouvrir sur le travail restant à accomplir dans la mise en place de cette synergie.*

Mots-clefs — Model-Based Safety Analysis (MBSA), Sûreté de fonctionnement, AltaRica Data Flow, SimfiaNeo, analyse zonale

Abstract *— This paper presents a design, validation and verification method of a MBSA (Model-Based Safety Analysis) model, using the Airbus Protect SimfiaNeo tool. We dwell on the need for an aeronautical manufacturer to implement processes to strengthen the confidence in complex systems safety analyzes carried out by failure propagation models. Beyond the method, we also linger on how to implement it, and how the modeling tool addresses engine manufacturer needs, such as the ones presented by Safran Aircraft Engines. In order to illustrate the synergies that we can find between the method and the tool to achieve a safety analysis, we propose a zonal safety analysis. Finally, the results provide insight into the work remaining to accomplish in implementing this synergy.*

Keywords — Model-Based Safety Analysis (MBSA), Safety, AltaRica Data Flow, SimfiaNeo, zonal safety analysis

I. INTRODUCTION

Dans un monde où les exigences économiques, environnementales et de sécurité sont toujours plus contraignantes, les industriels sont amenés à concevoir des produits toujours plus complexes. Les multiples configurations, redondances ou capacités de reconfiguration des systèmes d'aujourd'hui et de demain mènent à des scénarios de sécurité dont la combinatoire augmente de façon exponentielle.

Dans ce contexte, le MBSA permet d'armer les ingénieurs en sûreté de fonctionnement d'outils proposant une représentation graphique facilitant la communication avec les métiers de conception, de moteurs de calculs lui permettant d'assurer l'exhaustivité des scénarios menant aux évènements redoutés de son système et le regroupement des problématiques et des études de sécurité au sein d'un unique modèle.

Pour assurer l'efficacité de la mise en œuvre de ce nouvel outil, il est cependant impératif pour les industriels de s'armer d'une méthodologie adaptée qui permette d'accompagner les études de la conception à l'exploitation des résultats, en passant par la validation et la vérification. Safran Aircraft Engines travaille collectivement avec le reste des sociétés du groupe Safran à la montée en maturité et la mise en place de ces processus pour accompagner le développement de ses produits, travaux réalisés avec le soutien financier du Plan de Relance dans le cadre du plan de relance européen Next Generation UE. Un travail de fond

avec l'éditeur du logiciel SimfiaNeo, Airbus Protect, nous permet de rendre compte de la manière la plus efficace d'implémenter ces méthodes pour permettre de gains qualitatifs et quantitatifs sur nos études de sureté de fonctionnement, en conciliant nos besoins avec les recommandations de l'ARP 4761A. Dans cet article nous revenons sur les grandes lignes de la méthodologie mise en place et sur un exemple d'analyse de zone pour illustrer comment l'outil et la méthode permettent de servir nos études dans un contexte précis.

II. REVUE DE LITERATURE

Depuis plus d'une vingtaine d'années, le domaine aéronautique tente de développer des méthodes et des outils avancés pour identifier, évaluer et atténuer les risques liés à ses systèmes devenus de plus en plus complexes. Depuis les années 2000, à travers le projet ESACS (Enhanced Safety Assessment for Complex Systems) (2001 – 2003), le MBSA se dévoile et propose une nouvelle méthodologie. Le langage AltaRica est utilisé pour démontrer sa pertinence dans l'évaluation des risques des modèles dynamiques. Par la suite plusieurs projets européens, notamment ISAAC (Improvement of Safety Activities on Aeronautical Complex systems) (2004 - 2007) et MISSA (More Integrated Systems Safety Assessment) (2008 - 2011), et des projets internes aux industriels, se sont succédés afin de confirmer que tous les aspects de la sûreté de fonctionnement sont couverts par le MBSA.

Plus récemment, différents projets collaboratifs portés par des Instituts de Recherche Technologique (IRT) ont poursuivi ces travaux. Nous pouvons citer par exemple les projets MOISE, S2C (System & Safety Continuity , fin en 2023) et CoSMoS (débuté en 2024). Ceux-ci adressent non seulement la méthodologie MBSA, mais également des thématiques connexes telles que les liens avec le Model-Based System Engineering (MBSE) ou les problématiques d'entreprise étendue. Il est également à noter un projet actuel IMdR ayant vocation à la rédaction d'une norme internationale qui définirait ce qu'est le MBSA.

En tant que fournisseur logiciel, Airbus Protect n'a cessé de capitaliser la connaissance de cette méthode à travers son outil SimfiaNeo pour proposer une solution efficace aux différents domaines nécessitant des approches modernes pour mieux comprendre, prévenir et gérer les risques associés à ces systèmes essentiels. Cette méthode est maintenant reconnue par les autorités de certifications et un document officiel (ARP 4761A) donne des recommandations/exemples pour mener à bien ces analyses.

III. METHODOLOGIE

Le processus d'une étude MBSA s'appuie sur trois piliers : la méthode, le langage et l'outil. La méthode développée par Safran Aircraft Engines – en lien avec la nouvelle ARP 4761A – propose une démarche qui amène l'ingénieur à se poser les questions pertinentes à chaque étape de son étude, avec pour objectif d'assurer un niveau de confiance satisfaisant dans le résultat fourni par les modèles. Cette méthode, indépendante de l'outil, est illustrée aujourd'hui à travers l'outil SimfiaNeo, qui s'appuie lui-même sur le langage AltaRica Data Flow. Le but de cette première partie est de donner des éléments méthodologiques et outillés d'une étude classique, en se concentrant sur la réalisation d'une analyse zonale en MBSA.

A. Définir le besoin de modélisation

La conception d'un modèle commence par la définition du besoin de modélisation, comportant les éléments suivants :

- **Objectifs** du modèle : fiabilité, sécurité, obtention de résultats qualitatifs ou quantitatifs…
- Identification des **données d'entrée** : cela peut-être aussi bien la liste des évènements redoutés à étudier, les objectifs associés, la liste de fonctions du système d'intérêt, une AMDEC ou encore une étude MBSE (Model-Based System Engineering). La nature des données dépend de la phase de vie du projet et de l'objectif du modèle.
- Identification des **événements redoutés** que l'on souhaite étudier dans notre modèle.

Des éléments méthodologiques supplémentaires sont disponibles dans le guide S2C. Cette étape est primordiale pour un bon déroulement de l'étude et permet de réaliser un modèle au juste besoin et à la bonne granularité.

B. Définir le modèle préliminaire de propagation de pannes

Avant de modéliser le système dans l'outil, la deuxième étape consiste à définir sur papier *(i.e. en dehors d'un outil de modélisation)* et de manière préliminaire le modèle de propagation de pannes, l'idée ici est d'aborder les points suivants :

- Le niveau d'abstraction du modèle, qui précise le détail avec lequel nous allons modéliser un modèle. Il concerne à la fois la finesse avec laquelle nous allons déterminer les organes à modéliser, la prise de hauteur et la granularité associée aux grandeurs physiques des flux échangés entre eux. La granularité de modélisation peut être en partie définie grâce aux événements redoutés étudiés. Fixer cette dernière permet de réaliser un modèle *au juste besoin*, sans chercher à représenter le système dans sa globalité ce qui nous permet de gagner en temps de modélisation et de réduire la complexité du modèle. En revanche, si elle est mal définie à cette étape et qu'elle doit être évoluer ultérieurement, il faudra compter un temps conséquent pour ajuster le modèle.

- Une fois ce niveau déterminé, nous pouvons en conclure la liste des organes et des flux les traversant, ce qui nous permet d'établir une première vision sur feuille de notre modèle de propagation de pannes.

C'est également à cette étape que nous posons les premières hypothèses de modélisation qui seront capitalisées dans l'outil. Une fois la liste des organes établie, la conception de chaque organe commence par l'étude de son comportement fonctionnel, dysfonctionnel et des effets locaux associés. Ces informations peuvent être stockés dans une fiche de modélisation de l'organe et renseignés dans l'outil.

Ces deux éléments (besoin de modélisation et le modèle préliminaire de propagation de panne) doivent être validées avant de modéliser dans l'outil (cf. paragraphe V&V).

C. Modéliser dans l'outil avec les bibliothèques

Une fois la préparation de la modélisation effectuée, sa réalisation doit être lancée. Dans cette section, nous ne décrirons pas en détail cette étape, déjà présentée dans d'autres références telles que le projet S2C. Nous nous concentrons à la place sur les questions de gestion des bibliothèques et des hypothèses de modélisation.

La plupart des outils de MBSA permettent l'utilisation de bibliothèques, c'est-à-dire la réutilisation d'éléments au sein d'un même projet, mais également entre plusieurs projets. Cette réutilisation permet notamment d'accélérer les itérations, de faciliter la capitalisation tout en standardisant au sein d'une même entreprise et de tirer parti de la V&V unitaire (voir section suivante) précédemment réalisée pour gagner en efficacité et confiance dans une nouvelle étude.

SimfiaNeo permet de gérer la création et le suivi de version des bibliothèques, et – *en partie* – la dépendance des bibliothèques entre elles. Chaque bibliothèque est gérée comme un projet à part entière. Dans le cas de bibliothèques partagées au sein de l'entreprise, nous recommandons d'encadrer les droits et tracer les modifications des bibliothèques, afin de garder une cohérence dans le temps. L'idée pourrait être d'avoir une personne ayant la vision des différents projets responsable de la modification et l'ajout d'éléments dans les bibliothèques partagées, pour ainsi ne pas réaliser de conflit sur les modélisations en cours. A contrario, certaines personnes auraient uniquement le droit d'utiliser les bibliothèques existantes, sans droit de modification de celles-ci. Cette rigueur est d'autant plus importante pour tirer crédit de la V&V (Validation & Vérification) de la bibliothèque dans les projets qui l'utilisent.

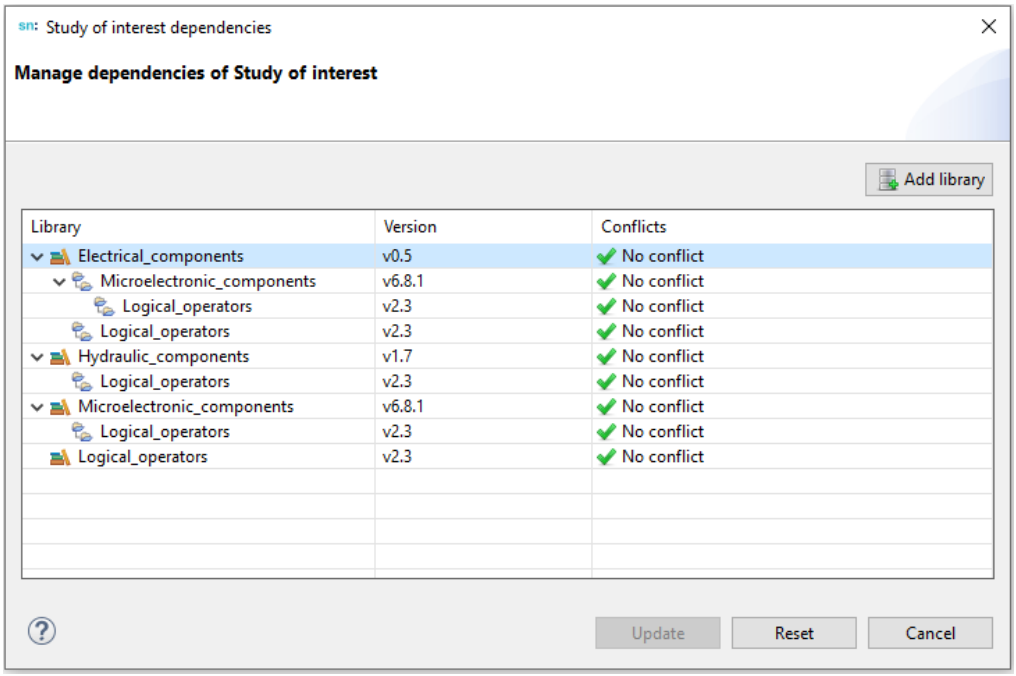


Fig. 1. Gestion des dépendances d'un projet

Dans la Fig. 1, le système étudié dépend directement des bibliothèques "Hydraulic components" et "Electrical components". Chacune de ces bibliothèques possède ses propres dépendances vers "Logical operators" et vers "Microelectronic components", automatiquement propagées. Dans la vie d'un ou des projets, voire dans la vie d'une entreprise, ces bibliothèques peuvent être amenées à évoluer. Ces évolutions peuvent correspondre à l'ajout de nouvelles briques, la modification de briques existantes, la modification de paramètres numériques… Dans ce cas, il est nécessaire de propager ces mises à jour à travers les dépendances.

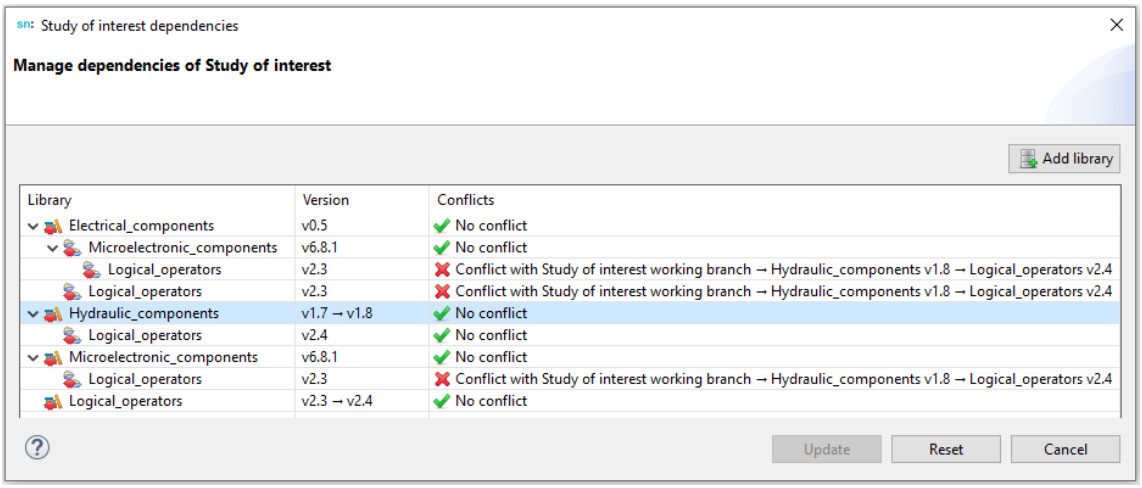


Fig. 2. Identification des conflicts dans la gestion des dépendances d'un projet

Dans l'exemple précédent, supposons une mise à jour (voir Fig. 2) de la bibliothèque "Logical_operators" pour passer de la version 2.3 à 2.4, et une mise à jour en conséquence de la bibliothèque "Hydraulic components" de 1.7 vers 1.8. au moment de la mise à jour dans notre système étudié, le conflit entre l'utilisation des version 2.3 dans "Microelectronic" et 2.4 dans "Hydraulic" est détecté. Ceci illustre le besoin à la fois d'organiser les dépendances entre bibliothèques, mais également de mettre en place une méthodologie rigoureuse de mise à jour de ces bibliothèques entre les projets.

Lors de la construction d'un modèle, il est fréquent de rencontrer des interrogations sur le système, ou d'en déduire de nouvelles exigences (par exemple une exigence d'indépendance de deux sources électriques). Dans ce cas, nous recommandons de tracer ces éléments directement dans SimfiaNeo pour être au plus près du modèle. Ceci passe par une table dite des "Safety parameters", rassemblant ces informations. Chaque "safety parameter" possède un statut pour tracer sa prise en compte dans le reste du processus d'étude du système.

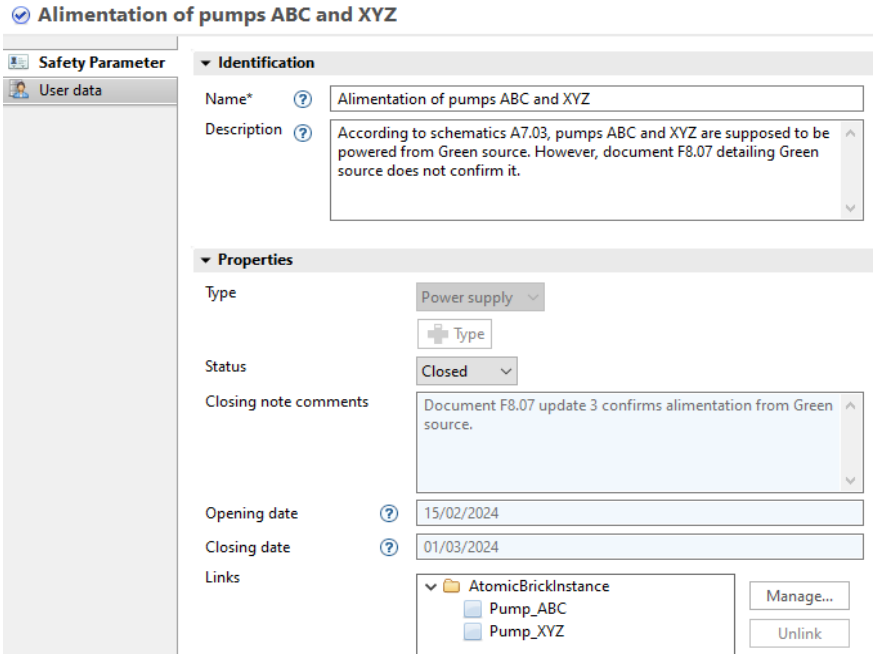


Fig. 3. Documentation, suivi du statut des hypothèses de sureté de fonctionnement et lien avec les éléments du modèle via les safety parameters

D. Valider & Vérifier les organes et le modèle

La validation & vérification (V&V) est réalisée à deux niveaux : le premier est sur l'organe modélisé et le second est sur un modèle complet. On entend par validation le fait de s'assurer que ce que nous avons défini pour implémentation est représentatif du système et du comportement réel. Ensuite, la vérification intervient et consiste à s'assurer que le modèle ou l'organe est correctement implémenté dans l'outil.

1) Validation & Vérification des organes

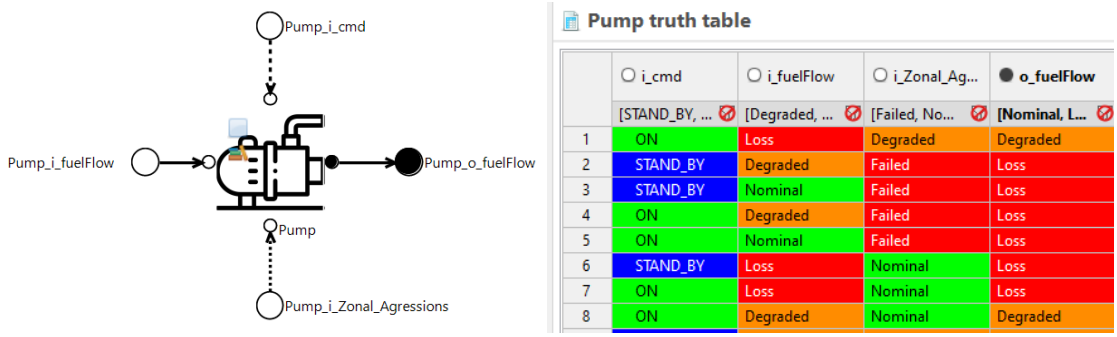
Avant de valider un modèle, nous validons nos bibliothèques d'organes. La validation de l'organe consiste à valider avec des experts concernés le comportement défini dans la fiche de modélisation réalisée au moment de la conception hors outil, pour s'assurer que l'élément que l'on va modéliser est représentatif du comportement fonctionnel et dysfonctionnel de l'organe réel. Ces éléments peuvent être validés dans une revue dédiée qui retrace :

- Les événements définis (fonctionnels & dysfonctionnels) et le comportement associé (la loi, leurs conditions d'apparition, leurs effets et leur probabilité/priorités intrinsèques - si applicable).
- Les effets locaux des événements (propagations des sorties),
- Les hypothèses de modélisation prises sur l'organe.

La vérification de l'organe consiste à vérifier que nous avons correctement implémenté l'organe précédemment validé dans le logiciel. La première étape, lors de l'implémentation de celui-ci sur le logiciel peut être de vérifier en simulation pas-à-pas que le comportement implémenté est bien celui voulu. Seulement cette vérification peut ne pas être exhaustive et donc elle n'est pas suffisante. Il faut s'assurer que chaque combinaisons d'états des variables locales et des entrées mènent à la sortie désirée. Cette vérification est généralement réalisée en deux étapes :

- Vérification de l'implémentation du comportement de l'organe, c'est-à-dire de de l'implémentation des transitions possibles entre les combinaisons d'états internes,
- Vérification de l'implémentation des effets locaux (soit de la propagation), c'est-à-dire que la définition des sorties est correctement définie en fonction des états internes et des entrées

Sous SimfiaNeo, il est possible de vérifier l'implémentation de la propagation grâce aux tables de vérité générées automatiquement sur les codes de propagation des organes. Celle-ci, explorée grâce à un système de filtre, peut alors être comparée à l'attendu détaillé dans la fiche de modélisation.



	i_cmd	i_fuelFlow	i_Zonal_Ag...	o_fuelFlow
	[STAND_BY, ...	[Degraded, ...	[Failed, No...	[Nominal, L...
1	ON	Loss	Degraded	Degraded
2	STAND_BY	Degraded	Failed	Loss
3	STAND_BY	Nominal	Failed	Loss
4	ON	Degraded	Failed	Loss
5	ON	Nominal	Failed	Loss
6	STAND_BY	Loss	Nominal	Loss
7	ON	Loss	Nominal	Loss
8	ON	Degraded	Nominal	Degraded

Fig. 4. Illustration de la génération d'une table de vérité pour la vérirification de la propagation des composants

2) Validation & Vérification des modèles

La validation du modèle consiste à s'assurer que le besoin de modélisation est conforme. En d'autre termes, l'ingénieur responsable de l'étude de sûreté de fonctionnement doit pouvoir vérifier que sa compréhension du fonctionnement du système, la manière dont celui-ci est utilisé (scénarios d'utilisation), les pannes (modes de défaillance), les conséquences (propagation) et les évènements redoutés étudiés, sont en adéquation avec ceux décrits par les métiers spécialistes, les architectes et les experts en sûreté de fonctionnement. La validation commence donc dès le tout début de l'étude au moment du besoin de modélisation ; celle-ci est réalisée sous forme de revues tout au long du projet.

Pour la vérification globale, on ne cherchera pas ici à être exhaustif comme dans la vérification unitaire car cela serait très chronophage et reviendrait à vérifier chaque scénario déterminé par le modèle. Il est donc nécessaire d'établir une liste de cas de tests scénarios pertinents à tester sur le système pour vérifier que son implémentation a été réalisée correctement. Ces cas de tests doivent remplir les critères suivants :

- Permettre de s'assurer que pour un jeu d'entrée donnée, le modèle obtient des sorties attendues (cohérentes du système).
- Permettre de s'assurer que les comportements fonctionnels indispensables à la représentativité du modèle sont vérifiés.
- Permettre de s'assurer que les dysfonctions du système se propagent comme attendu.

Cette liste de cas de tests étant une donnée d'entrée pour la vérification globale, il faudra l'établir au préalable et la présenter au sein d'une revue en amont de l'activité de vérification. Les scénarios peuvent être revus au même moment que les besoins de modélisation, permettant de s'assurer avec les mêmes participants (experts systèmes, architectes, et experts sûreté de fonctionnement) que les besoins sont couverts par la liste des cas de test.

E. Gérer les itérations & gérer la configuration

La capitalisation des documents et la gestion de configuration/des versions du modèle peut se faire directement dans l'outil SimfiaNeo. Les documents sont tous stockés au même endroit. Le modèle, ainsi que les bibliothèques, peuvent être versionnés et nous pouvons réaliser des comparaisons entre les différentes versions, permettant d'avoir accès aux ajouts, aux suppressions et aux modifications apportées au modèle. Cette fonctionnalité permet d'identifier puis de valider plus facilement les modifications entre deux versions.

De plus, l'extension « aéronautique » permet de stocker les différentes hypothèses prises sur l'étude, de les catégoriser, de leur attribuer un statut et de les relier à des éléments du modèle au besoin. Sur chaque projet, les hypothèses doivent être tracées. Cette extension permet également de remplir les informations sur les événements redoutés étudiés, les DAL (Development Assurance Level) associés, ainsi que les fonctions & dysfonctions du système.

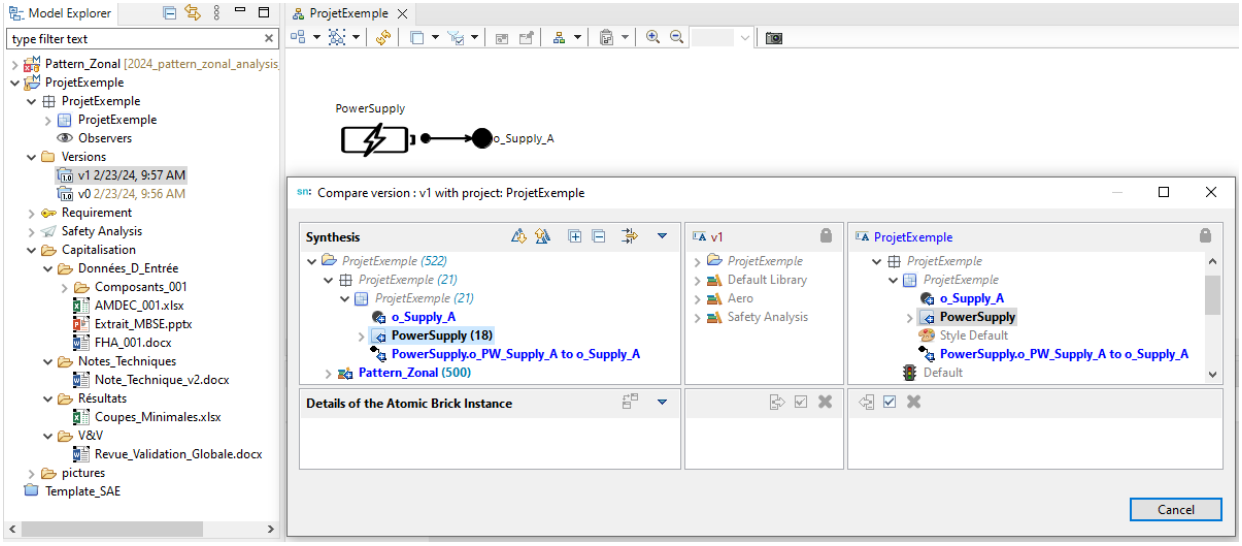


Fig. 5. Illustration de la gestion de configuration documentaire d'un projet MBSA sous SimfiaNeo

Enfin, SimfiaNeo est connecté à GitLab, plateforme officielle de management de dépôts Git* (système de contrôle de version open source mature et activement maintenu, utilisé par des milliers de développeurs à travers le monde) de Safran Aircraft Engines, cette plateforme est dédiée au stockage, contrôle de version et développement collaboratif de code source, ce qui permet donc d'avoir un versionnage des documents stockés, ainsi que l'accès aux modèles par plusieurs utilisateurs quel que soit le poste de travail.

F. Exploiter des résultats

Différents calculs peuvent être réalisés sur un modèle MBSA, en fonction des objectifs de l'étude. Dans notre cas, nous nous focalisons sur la génération de coupes minimales ou de séquences minimales ou non-minimales, ainsi que leur analyse.
Une coupe minimale est la plus petite combinaison d'évènements menant à l'événement redouté, ne prenant pas en compte l'ordre d'apparition de ceux-ci. La séquence minimale, quant à elle, est similaire aux coupes mais prend en compte la dynamique du système et l'ordre dans lequel arrivent les événements. Si le système est statique, les coupes et les séquences seront équivalentes.
Deux grandes méthodes permettent cette génération sur un modèle :

- Déductive : génération en partant de la situation redoutée étudiée, pour remonter aux événements. Cette méthode est plus rapide, mais ne peut générer que des coupes.
- Inductive : génération en partant des événements, pour les combiner jusqu'à atteindre la situation redoutée. Cette méthode est plus longue, mais permet de générer des séquences.

L'adoption de l'une ou l'autre de ces méthodes peut dépendre de l'objectif courant de l'analyse. En phase préliminaire, les comportements implémentés dans le modèle sont souvent abstraits, et donc un calcul de coupes via la méthode déductive peut être suffisant tout en ayant la vitesse adaptée pour des comparaisons d'architectures. En phase plus poussée, la granularité est plus fine, avec une inclusion de la dynamique du système. La méthode déductive permet alors des résultats plus proches du système réel.

Une fois les coupes ou séquences obtenues, le travail de l'analyste ne s'arrête pas là. Plusieurs analyses peuvent être réalisées selon le contexte :

- Quantitative : des formules spécifiques pour le calcul de probabilité sont définies dans l'APR4761A. Ces formules sont adaptées pour des coupes, mais pas par pour des séquences. Des travaux existent (projet CoSMoS débuté en mars 2024) pour étendre ces formules aux séquences. Dans l'intervalle, il peut être nécessaire de retransformer les séquences en coupes équivalentes pour l'évaluation quantitative. Dans SimfiaNeo, cela passe par des post-traitements directement intégrés au logiciel et activables par l'utilisateur. Des règles claires d'utilisation de ces post-traitements sont mises en place chez Safran.
- Qualitative : le contexte aéronautique peut imposer des règles qualitatives sur l'allocation des DAL (Development Assurance Level) ou l'absence de point de panne unique pour certaines situations redoutées. Ces règles peuvent être directement implémentées dans les outils MBSA pour gagner en efficacité, notamment lors les itérations. Dans SimfiaNeo, ceci se traduit par des vérifications automatisées (appelées "checks") de ces règles en cas d'activation par l'utilisateur.
- Autres : des analyses supplémentaires des coupes ou séquences peuvent être réalisées pour des thématiques telles que les modes communs (CMA : Common Mode Analysis), y compris les analyses de zones (ZSA : Zonal Safety Analysis). La plupart de ces analyses exploitent le concept de données utilisateurs ("user data"). L'illustration de cette activité est l'objet de la section suivante.

IV. Comment realiser l'analyse zonale en MBSA ?

L'analyse zonale (ou analyse de zone) réalisée dans l'exemple qui suit a pour but de mettre en évidence les défaillances liées à l'implantation physique des composants dans le système d'intérêt, là où une analyse des scénarios de défaillance basé sur l'architecture organique seule se révèlera insuffisante.

Le système d'intérêt est un système de dosage de débit carburant piloté, dont la vanne de dosage est alimentée en débit par une pompe principale (présentant une redondance froide sous la forme d'une pompe de backup – la pompe de backup doit s'activer lorsque la pompe principale ne permet plus d'envoyer un débit suffisant pour alimenter le doseur). Une mesure de débit est effectuée à l'aide d'un capteur bi-voie à la sortie de la pompe principale. Un système de contrôle électrique permet de transmettre l'information et de commander la pompe principale, la pompe secondaire et la vanne de dosage. L'ensemble des informations électriques sont véhiculés entre les différents organes du circuit via des faisceaux de câbles électriques, communément appelés « harnais ».

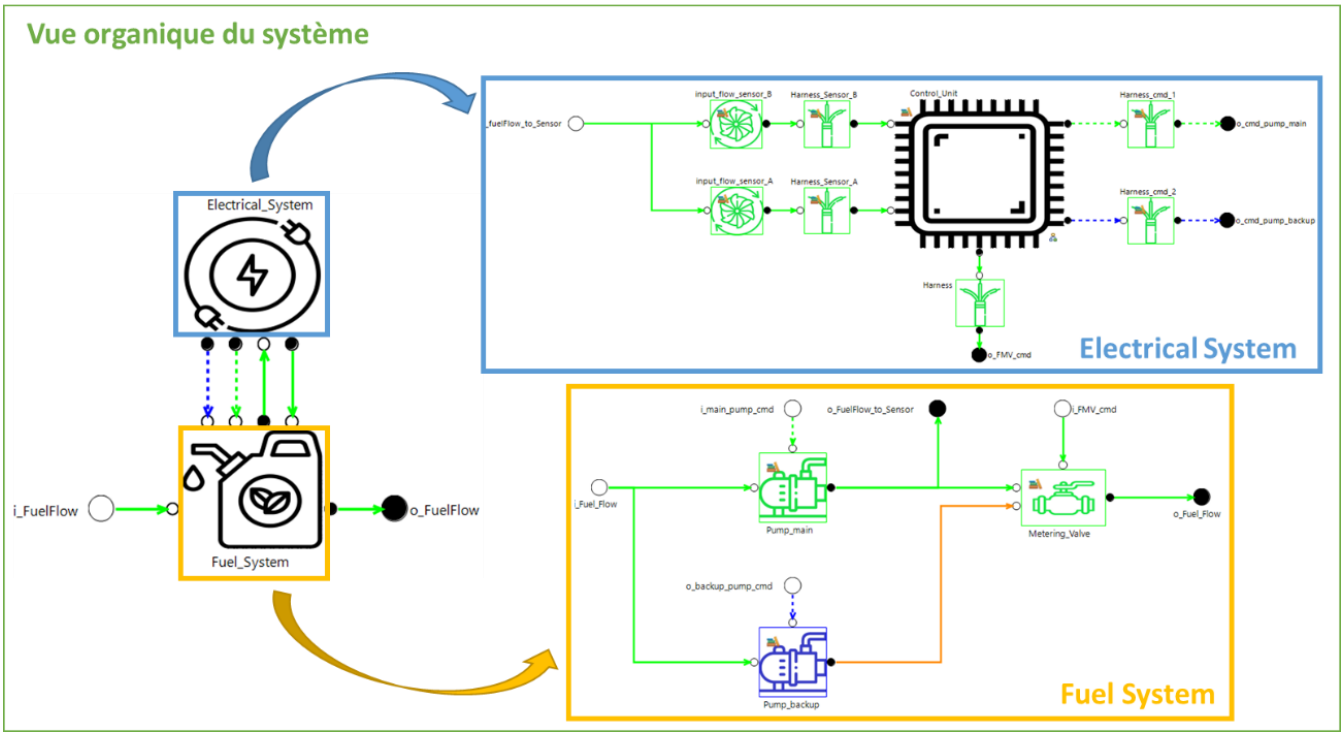


Fig. 6. Architecture organique du système d'intérêt

Les équipements sont répartis dans quatre zones autour du moteur : « Above Engine », « Left Side », « Right Side » et « Under Engine ».
Dans chaque cas, l'évènement redouté que nous chercherons à capter est la dégradation du débit de carburant en sortie du système de dosage.

Toutes les méthodes ci-dessous s'appuieront sur le même système pour illustrer leur mise en œuvre. Dans chacun des exemples, les pannes des organes sont connues, ainsi que la zone physique à laquelle chaque organe appartient.

A. *1er cas de figure : connaissance de l'architecture physique, pas de connaissance des agressions liées aux zones*

Dans une première configuration, nous supposons que les agressions liées à chaque zone ne sont pas encore connues au stade où l'analyse de sûreté de fonctionnement est effectuée. Pour cette première approche, une fois le modèle organique implémenté, il est nécessaire de renseigner l'existence de zones et de lier ces dernières à chacun des organes instanciés dans le modèle. Pour se faire, nous nous appuyons sur la fonctionnalité « user data » proposé par l'outil SimfiaNeo. Les « user data » correspondent à des paramètres personnalisés, et peuvent être associés à des éléments du modèle. Nous définissons donc ici la donnée utilisateur « Zone », qui est une énumération des quatre zones physiques du système. Nous choisissons d'appliquer ce paramètre aux briques matérialisant les constituants de notre système. Une fois ces propriétés attachées à notre modèle, il nous est possible de les utiliser pour traiter les résultats de calculs.

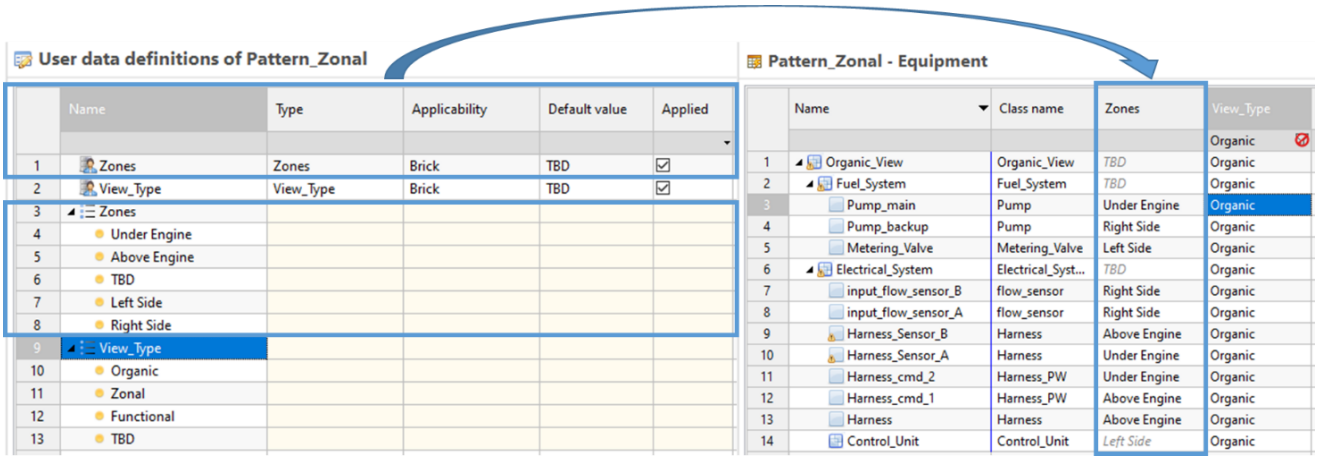


Fig. 7. Ajout des propriétés de zones pour chacun des équipements de l'architecture organique

Si nous examinons les coupes minimales menant à l'évènement redouté « Dégradation du débit carburant en sortie du système de dosage », on constate qu'hormis la panne de la carte de commande de notre calculateur, seules des coupes d'ordre 2 contenant des pannes organiques sont identifiées. Ce premier résultat peut alors être traité en remplaçant les pannes organiques par les zones auxquelles appartiennent chacun des composants. Nous réduisons ensuite horizontalement les coupes (pour grouper les évènements se produisant dans la même zone), puis verticalement (pour grouper les coupes similaires suite aux précédents traitements). On constate alors qu'une coupe classée comme coupe d'ordre 2 contient des défaillances d'organes situés dans une même zone (Under Engine). Il s'agit alors pour l'ingénieur en sûreté de fonctionnement d'aller interroger les spécialistes pour s'assurer qu'aucune agression menant à la perte simultanée de ces deux organes ne peut se produire dans cette zone. Le cas échéant, cette coupe organique d'ordre 2 se transformerait en coupe d'ordre 1 en cas d'agression de la zone.

Cette méthode permet donc de mettre en lumière une coupe qui aurait pu être considérée comme acceptable d'un point de vue qualitatif, et permet de challenger l'implantation géographique des composants du système avant même d'avoir connaissance des agressions externes.

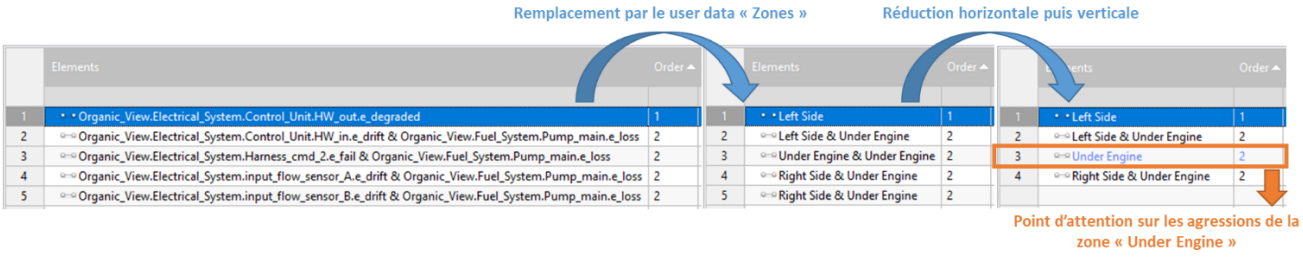


Fig. 8. Traitement des coupes organiques pour analyse zonale

B. *2nd cas de figure : connaissance de l'architecture physique et des agressions liées aux zones*

Dans le second cas nous considérons que nous avons connaissance des agressions liées aux zones. Nous allons exposer deux méthodes pour adresser l'analyse zonale dans ces configurations. On considérera pour l'exemple :

- Une agression électromagnétique dans la zone « Right Side », qui génèrera une erreur les signaux électriques transitant par cette zone
- Une agression feu dans la zone « Under Engine », qui mènera à la perte des équipements de cette zone.

1) 1ère méthode : synchronisations

La première méthode consiste à s'appuyer sur la table des équipements et sur le « user data » « Zones » que nous avons définie précédemment. Il s'agit simplement de filtrer zone par zone pour définir les synchronisations liées aux agressions des équipements de la zone. Si l'on reprend l'exemple précédent, il est possible de sélectionner les équipements de la zone « Under Engine » : Pompe principale, Harnais du capteur de débit voie A et harnais de commande 2 (le terme « harnais » est employé ici pour parler de faisceaux de câbles électriques). La même manipulation peut être faite pour les équipement de la zone « Right Side » qui peuvent être impactés par une agression électromagnétique. En l'occurrence, trois équipements sont dans cette zone : la pompe backup et les deux capteurs : seuls les deux capteurs sont impactés par une dérive de leur signal (la pompe backup est soit fonctionnelle, soit perdue, elle n'est donc pas impactée par cette agression).

On peut ensuite lancer les calculs concernant notre évènement redouté, et retrouver la coupe d'ordre 1 « Fire Under Engine », correspondant à la zone identifiée dans le cas de figure 1 comme potentiellement vulnérable.

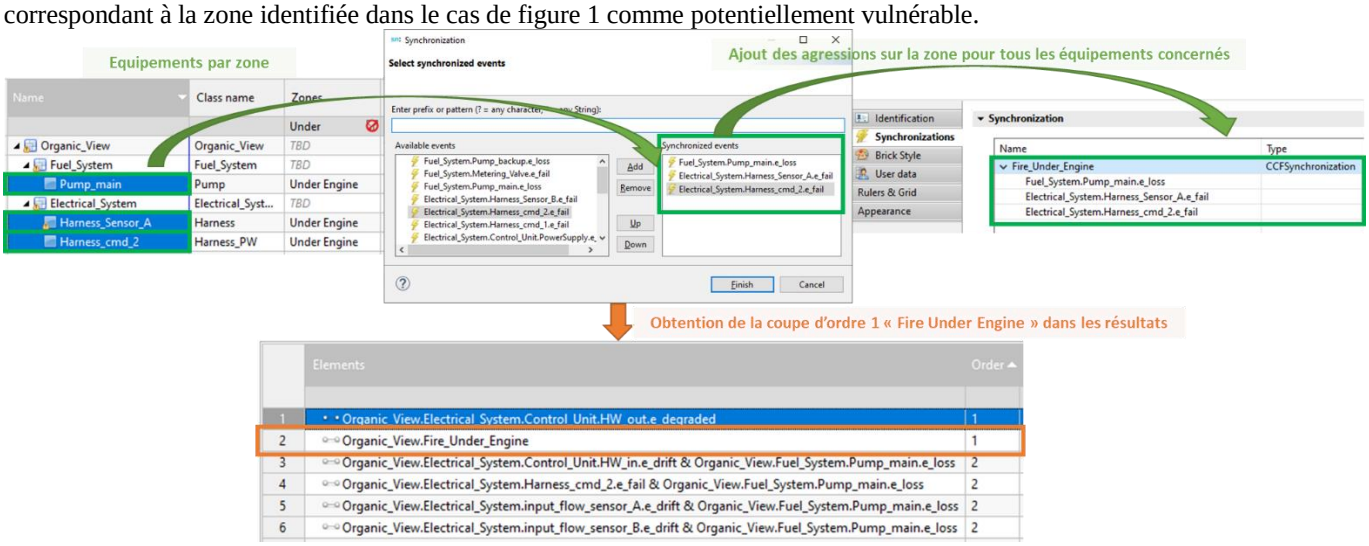


Fig. 9. Illustration de la méthode avec synchronisations

2) 2nde méthode : propagation de la vue zonale vers la vue organique

Une seconde méthode pour adresser ce type d'étude consiste à créer, en supplément de la vue organique, une vue zonale du système. On associe aux briques de la vue zonale les agressions relatives à l'emplacement physique représenté, et on propage ensuite cette agression via les sorties des briques. Il est nécessaire d'adapter la vue organique pour les équipements afin qu'ils possèdent une entrée relative à la propagation des agressions de zone. Chaque organe va alors être connecté à sa zone par un lien de propagation (de la zone vers l'organe). Pour ne pas encombrer la vue organique, il est possible d'associer les éléments graphiques à des ***layers*** (couches graphiques personnalisables auxquelles on peut associer des éléments du modèle, que l'on peut choisir ou non d'afficher) correspondant à la vue organique et zonale, et de masquer le layer zonal lorsque l'on souhaite simplement consulter ou présenter l'architecture organique.

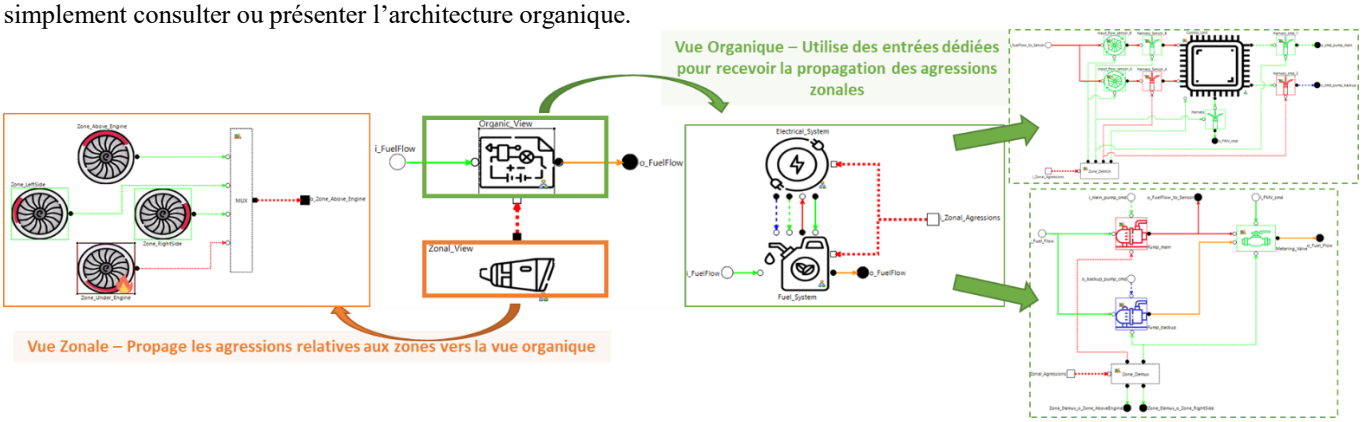


Fig. 10. Utilisation de la propagation de la vue zonale vers la vue organique – exemple de l'agression feu dans la zone « Under Engine »

A l'instar de la méthode des synchronisations, lorsque que l'on calcule les résultats qualitatifs menant à l'évènement redouté étudié, nous retrouvons bien la coupe d'ordre 1 liée à l'agression feu « Under Engine ». La coupe apparait cette fois comme un évènement feu attaché à une brique implémentée dans la vue zonale alors qu'elle apparaissait logiquement comme un évènement lié à la vue organique dans la méthode exploitant les synchronisations.

	Elements	Order
1	Organic_View.Electrical_System.Control_Unit.HW_out.e_degraded	1
2	Zonal_View.Zone_Under_Engine.e_fire	1
3	Organic_View.Electrical_System.Control_Unit.HW_in.e_drift & Organic_View.Fuel_System.Pump_main.e_loss	2
4	Organic_View.Electrical_System.Harness_cmd_2.e_fail & Organic_View.Fuel_System.Pump_main.e_loss	2
5	Organic_View.Electrical_System.input_flow_sensor_A.e_drift & Organic_View.Fuel_System.Pump_main.e_loss	2
6	Organic_View.Electrical_System.input_flow_sensor_B.e_drift & Organic_View.Fuel_System.Pump_main.e_loss	2

Fig. 11. Coupes minimales menant à notre évènement redouté dans l'approche avec propagation des pannes de la vue zonale vers une vue organique

V. RESULTATS

Les résultats sont présentés en deux parties pour ainsi dans un premier temps conclure sur la méthodologie complète mise en place par Safran Aircraft Engines, puis pour présenter les résultats sur la méthode d'analyse zonale.

1) Le retour d'expérience sur la méthodologie complète

La méthode appliquée chez Safran Aircraft Engines permet essentiellement de renforcer la confiance dans les modèles. L'enjeu est de réaliser les études de fiabilité et de sécurité en ayant des résultats dans lesquels nous pouvons avoir un maximum confiance. L'étude amont « sur papier » du besoin de modélisation et des scénarios opérationnels permet de faciliter la validation des modèles en revue. Elle permet également de se poser au mieux les bonnes questions sur la granularité des modèles et la finesse de modélisation des organes. Ce point est un enjeu majeur dans la modélisation MBSA, car la modification de ces hypothèses peut conduire à reprendre une grande partie du modèle et donc à perdre beaucoup de temps. En revanche, un des avantages de la méthode est la démarche de conception des organes à travers l'utilisation des bibliothèques qui permet de faciliter la vérification & la réutilisation des organes.

2) Les cas d'utilisations des méthodes d'analyse zonale

Chacune des méthodes exposées précédemment présentent des avantages et inconvénients, mais aussi des contextes d'applications qui leurs sont propres.

La première méthode se détache des deux autres car elle s'applique plutôt dans une phase amont de développement d'un produit, lorsque les informations d'agression de zone ne sont pas encore connues. Sa force est de pouvoir lever au plus tôt des alertes sur de potentiels modes communs et de pouvoir ajuster rapidement l'implantation des composants dans un système. Elle ne permettra cependant pas directement d'apporter les coupes minimales liées aux agressions de zone, il faudra s'y ramener a posteriori par post-traitement des résultats.

Les deux autres méthodes peuvent être mises en œuvre plus tard dans le projet, puisqu'elles nécessitent de connaître les agressions liées aux zones. Les deux méthodes permettent d'obtenir les mêmes résultats en termes de coupes minimales. Cependant, leur mise en œuvre leur confère des avantages et inconvénients plus ou moins importants en fonction du contexte.

La méthode exploitant les synchronisations permet de ne pas surcharger un modèle en ajoutant des flux de propagation. Les entrées et sorties des briques restent les flux naturels gérés par les composants qu'ils représentent, évitant toute confusion sur l'utilisation d'un composant. Cette méthode est très rapide à mettre en œuvre sur un modèle de taille raisonnable *(i.e. de l'ordre d'une vingtaine de composants environ, avec un niveau de profondeur d'une couche ou deux)*. Elle nécessite une rigueur plus importante dans le sens où elle n'établit pas de lien direct entre les pannes liées aux zones (synchronisation) et l'appartenance de chaque composant à une zone. En effet, chaque synchronisation est construite sur le traitement de la table des équipements, et la vérification de la cohérence entre cette table et les synchronisations est une opération manuelle, plus difficile à maintenir et à faire évoluer sur un modèle de taille importante, et potentiellement soumis à des erreurs.

La méthode exploitant les liens de propagation présente quant à elle le désavantage principal de surcharger le visuel de la vue organique en ajoutant des entrées « abstraites » et des liens de propagation relatifs aux zones. Ce désavantage peut être limité par l'utilisation des ***layers***, permettant de masquer ou non les éléments identifiés comme appartenant au zonal dans la vue organique. Les avantages sont toutefois de permettre la création d'une vue zonale, rendant beaucoup mieux compte de l'implantation des composants dans le système. Cette vue permet la mise en place de manière aisée des agressions liées à chaque

zone, et limite grandement les erreurs. Chaque composant de la vue organique doit être lié à une zone, il est donc impératif pour l'ingénieur en charge de la modélisation de se poser la question de sa zone d'appartenance pour chacun des organes. En mode simulation pas-à-pas des événements, il sera également possible de déclencher des pannes de zone et de suivre la propagation de celles-ci dans l'architecture organique, rendant les discussions avec les métiers d'architecture et de bureau d'étude plus fluide sur les aspects de sureté de fonctionnement lié aux zones. Cette méthode permet également d'adresser la problématique aux défaillances intrinsèques du système (par exemple, l'explosion d'un condensateur dans une électronique de puissance peut mener à la défaillance de composants ou de cartes situées dans la même boite ou la même armoire électrique).

SYNTHESE DE LA COMPARAISON DES METHODES D'ANALYSES ZONALES EN MBSA

Méthode	**Cas d'utilisation**	**Avantages & inconvénients**	
		Avantages	***Inconvénients***
Méthode "user data"	Applicable dans une phase amont de développement d'un produit, lorsque les informations d'agression de zone ne sont pas encore connues	- lève au plus tôt des alertes sur de potentiels modes communs - pas d'impact graphique sur le modèle, pas de modification des briques (évènements, entrées et sorties)	- oblige le post-traitement pour obtenir les coupes minimales liées aux agressions de zone
Synchronisations	Adaptée aux petits modèles & sur des systèmes avec peu de zones, convenant aux systèmes Safran Aircraft Engines tels que les turboréacteurs	- ne surcharge graphiquement pas le modèle - implémentation facile	- instaure un risque d'erreur d'implémentation & une vérification difficile
Propagation d'une vue "zonale"	Adaptée sur des systèmes à plus grandes échelles avec des systèmes avec beaucoup plus de zones, comme les systèmes à l'échelle de l'avion	- pousse à se poser la question de l'implémentation zonale de chaque organe	- surcharge graphiquement le modèle en ajoutant des flux de propagation - implémentation plus longue - les bibliothèques de composantes vérifiés doivent être adaptés

VI. DISCUSSION ET PERSPECTIVES

1) Evolutions & perspectives de la méthode présentée

La méthode présentée possède de nombreuses limites et axes d'améliorations, qui sont, pour certains d'entre eux, reliés aux problématiques MBSA retrouvées dans la littérature.

Premièrement, la granularité du modèle et le besoin de représentativité peuvent être variable d'un système à l'autre et d'un projet à l'autre. Cette notion n'est pas complètement systématique et nécessite une part de jugement technique de la part de la personne en charge de l'étude.

Dans le même esprit, la validation des modèles est réalisée aujourd'hui par des revues métiers retraçant des scénarios opérationnels représentatifs du fonctionnement du système. Cette méthodologie est basée sur un rapport effort/gain : plus le nombre de scénarios couverts sera important, plus la confiance quant à la représentativité du modèle sera grande, mais plus l'activité nécessitera un investissement de temps important. Il est donc important d'ajuster au bon niveau en fonction des objectifs du modèle et du projet, et d'identifier des scénarios les plus couvrant, afin de maximiser le gain de confiance vis-à-vis du temps passé à vérifier l'implémentation.

Pour que la méthode présente un intérêt optimal, chaque étude nécessitera une évaluation a priori des besoins qui sont propres à son système et du contexte projet dans lequel elle s'inscrit.

Les travaux de développement de liens outillés entre les modèles MBSA et les modèle MBSE sont un autre axe de travail majeur autour de la méthodologie et de sa synergie avec les outils. Ils pourront à l'avenir ouvrir sur des évolutions sur le traitement des données d'entrée pour les analyses de sûreté de fonctionnement, sur la façon d'aborder la granularité des modèles ou encore sur la manière d'effectuer la validation des études portées par le MBSA.

2) Evolutions & perspectives de l'outil SimfiaNeo

L'outil SimfiaNeo est construit autour de la méthode MBSA, dans un but de couvrir au fur et à mesure l'ensemble des étapes de l'analyse Sûreté de Fonctionnement. Comme illustré dans les sections précédentes, celui-ci ne traite pas uniquement de la construction et l'exécution d'un modèle AltaRica, mais adresse également les autres étapes de l'analyse telles que la documentation des hypothèses de l'étude, l'aide à l'analyse des résultats et la capitalisation des composants. Ces fonctionnalités ont pour but d'augmenter la confiance dans l'analyse réalisée, mais leur utilisation reste au choix des utilisateurs et/ou de leur organisation.

Parmi ces étapes complémentaires, les étapes de validation peuvent se placer à plusieurs niveaux : brique élémentaire, versions des bibliothèques, résultats du modèle. Une perspective envisagée de l'outil serait d'apporter une nouvelle vue aux utilisateurs concentrée sur la validation des éléments du projet. En fonction des étapes de validation réalisées par l'utilisateur, cette vue permettrait d'indiquer un taux de confiance justifiée dans le modèle réalisé. Ces étapes prendraient la forme d'une check-list, proposée par l'outil ou personnalisable au sein d'une organisation.

Dans le cadre d'une approche qualité, les différentes étapes d'une analyse doivent être enchaînées selon différents profils d'acteurs. Par exemple, un profil type de "validateur" doit pouvoir parcourir l'ensemble du projet SimfiaNeo, suivre l'évolution des commentaires, statuer sur les éléments de la check-list précédemment citée, mais sans pouvoir modifier le modèle. Cette mise en place de différents profils sera facilitée à travers la mise à disposition d'un SimfiaNeo dans sa version web [6].

VII. CONCLUSION

Les points abordés dans ce document offrent des solutions pratiques pour renforcer la fiabilité des modèles et la confiance dans les résultats des études de sûreté de fonctionnement utilisant le MBSA. Il propose aux utilisateurs des solutions outillées en termes de gestion des projets, des bibliothèques et de gestion de configuration, ainsi que sur la validation & la vérification des modèles, et enfin sur comment réaliser une analyse de zones sur SimfiaNeo.

La figure suivante permet de résumer le processus proposé :

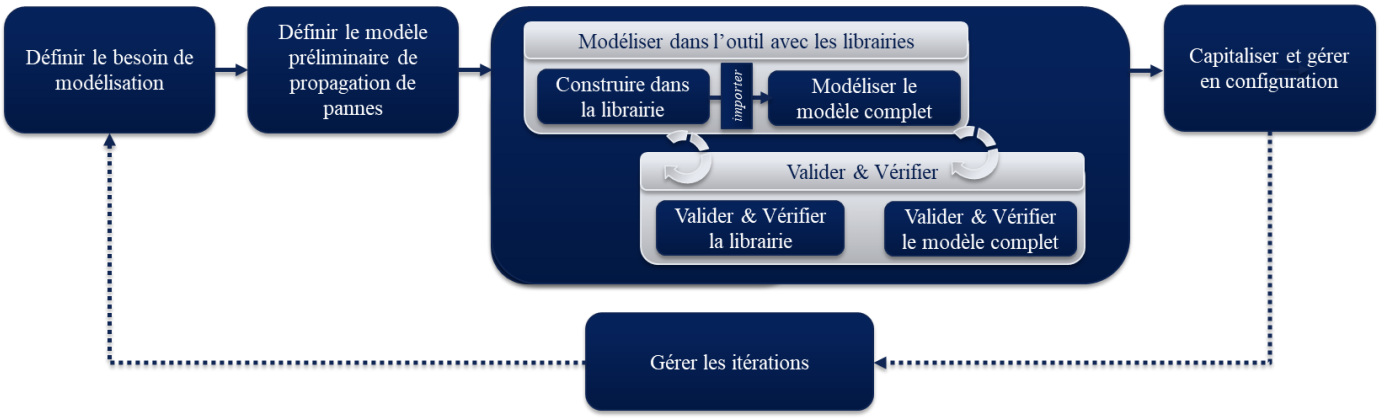


Fig. 12. Processus d'étude et de modélisation d'un modèle MBSA chez Safran Aircraft Engines

Comme souligné dans le paragraphe sur les discussions et perspectives, les méthodes et outils présentés ici donnent un état des lieux des pratiques actuelles, mais elles seront certainement amenées à évoluer avec l'ouverture de nouvelles passerelles, de nouveaux champs d'études ou contextes projet

REMERCIEMENTS

Nous tenons à remercier tous les participants et les relecteurs pour leur contribution précieuse à cet article du Lambda Mu 23, de Airbus Protect et de Safran Aircraft Engines. Vos idées et vos commentaires ont été essentiels pour enrichir et améliorer notre travail. Merci pour votre implication et votre collaboration. Nous voulons également remercier le soutien financier (côté Safran Aircraft Engines) du Plan de Relance dans le cadre du plan de relance européen Next Generation UE.

BIBLIOGRAPHIE

[1] BIEBER PIERRE, BOUGNOL CHRISTIAN, CATSEL CHARLES, HECKMANN JEAN-PIERRE, KEHREN CHRISTOPHE, METGE SYLVAIN AND SEGUIN CHRISTEL, SAFETY ASSESSMENT WITH ALTARICA (2004)

[2] DE BOSSOREILLE XAVIER, MACHIN MATHILDE, SAGASPE LAURENT. UN NOUVEL OUTIL DE SAFETY POUR MAITRISER LA COMPLEXITE DES SYSTEMES. CONGRES LAMBDA MU 21, « MAITRISE DES RISQUES ET TRANSFORMATION NUMERIQUE : OPPORTUNITES ET MENACES », OCT 2018, REIMS, FRANCE

[3] HUMBERT, S., SEGUIN, C., CASTEL, C., BOSC, J-M, DERIVING SAFETY SOFTWARE REQUIREMENTS FROM AN ALTARICA SYSTEM MODEL (2008)

[4] IRT SAINT EXUPERY. (2023, MARCH 31). THE S2C PROJECT (SYSTEM & SAFETY CONTINUITY). SITE DE L'IRT SAINT EXUPÉRY. RETRIEVED FEBRUARY 29, 2024, FROM HTTPS://WWW.IRT-SAINTEXUPERY.COM/S2C/

[5] FAIDA MHENNI, JEAN-YVES CHOLEY, NGA NGUYEN, CHRISTOPHE FRAZZA, FLIGHT CONTROL SYSTEM MODELING WITH SYSML TO SUPPORT VALIDATION, QUALIFICATION AND CERTIFICATION, IFAC-PAPERSONLINE (2016)