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

Méthodologie d'accompagnement à la réalisation d'un Model Based Safety Assessment (MBSA)

Support methodology for the Model Based Safety Assessment (MBSA) realisation

BERTHIER Stéphane
MBDA –Sûreté de Fonctionnement
Le Plessis-Robinson
stephane.berthier@mbda-systems.com

CHAMPION Sylvain
MBDA –Sûreté de Fonctionnement
Le Plessis-Robinson
sylvain.champion@mbda-systems.com

HERPE Nicolas
MBDA –Sûreté de Fonctionnement
Le Plessis-Robinson
nicolas.herpe@mbda-systems.com

LUKAS Thomas
MBDA –Sûreté de Fonctionnement
Le Plessis-Robinson
thomas.lukas@mbda-systems.com

PELLOQUIN Gaëtan
MBDA –Sûreté de Fonctionnement
Le Plessis-Robinson
gaetan.pelloquin@mbda-systems.com

***Résumé* —** Le présent article détaille la méthodologie d'accompagnement à la réalisation du MBSA chez MBDA. La simple existence d'un modèle MBSA ne paraît pas suffisant pour satisfaire les ambitions de l'approche. Effectivement, le MBSA aspire à terme à être une alternative très prometteuse pour certains cas d'analyse vis-à-vis des arbres de défaillances « traditionnels », en intégrant la prise en compte des aspects séquentiels. Si l'ingénierie par les modèles s'installe peu à peu dans le quotidien des industriels, il reste primordial de pouvoir accorder une confiance au modèle, ceci étant rendu possible par une démarche claire et précise d'encadrement du modèle et du process de réalisation. Pour se faire, il est primordial de mettre en œuvre un processus ciblé permettant :

- D'accompagner l'utilisateur dans la modélisation : en fournissant des directives, en optimisant au mieux son efficacité et en guidant ses premiers pas dans l'outil.
- D'accompagner le modèle dans son cycle de vie : en identifiant des exigences auxquelles le modèle devra se confronter, en cadrant la réponse à ces exigences et en permettant au modélisateur de tracer les choix de modélisation au cours de sa réalisation.

Concrètement, il est suggéré dans cette proposition la réalisation de plusieurs documents venant accompagner le modèle, avec comme objectif de guider l'utilisateur tout au long de sa réalisation, mais également faciliter la modélisation au cours de son évolution. L'enjeu principal est d'implémenter cette démarche tout en assurant que la potentielle augmentation de la charge de travail reste mesurée. Des opportunités d'optimisation globales de la méthode sont également explorées. Les apports et bénéfices finaux de cette démarche sont en cours d'évaluation mais paraissent être multiples : uniformiser les pratiques au niveau société, renforcer le niveau de confiance dans les résultats obtenus, cadrer la démarche et assurer un bon niveau de traçabilité.

Mots-clefs — MBSA, accompagnement, documentation, exigences, hypothèses, traçabilité

***Abstract* —** This article details the methodology to support the MBSA completion used at MBDA. It appears that if an MBSA model has been created, the fact that it exists does not necessarily meets the ambitious expectations of this approach . Indeed, the methodology ultimately aspires to be a promising alternative instead of fault tree analysis including sequential concerns. If engineering by models is gradually expanding in the daily life of companies, it is mandatory to have a sufficient level of trust with the model, this would be only possible with a clear and accurate management approach of the model. To solve this problem, it is essential to implement a targeted process allowing:

- To support the user in modeling: via a set of instructions, helping to improve efficiency as far as possible, supporting getting up to speed with the modeling tool.
- To support the model in its life cycle: by identifying requirements with which the model must comply, by framing the compliance statement response to these requirements and allowing the modeler to trace the modeling choices during the completion.

Especially, it is suggested in this proposal the creation of several documents alongside the model, with the objective of supporting the user throughout its creation, but also the model during its evolution. The main goal is to apply this approach while ensuring that the potential increase workload is controlled**.** Opportunities of improvement on the complete method are also explored. The final contributions and benefits of this approach are currently being assessed but appear to be multiple: standardizing practices at the company level, strengthening the level of confidence in the obtained results, framing the approach and ensuring a good level of traceability.

Keywords — MBSA, support, documentation, requirements, assumptions, traceability

LISTE DES ACCRONYMES

AMDEC : Analyse des modes de défaillance, de leurs effets et de leur criticité
EPS : Etudes Probabilistes de Sûreté
FMES : Failure Modes and Effects Summary
IRT : Institut de Recherche Technologique
MBSA : Model-Based Safety Assessment
PDR : Preliminary Desgin Review

I. REVUE DE LITTERATURE

Lors du déploiement ou du test d'un nouvel outil (ou nouvelle démarche), les premiers efforts se concentrent généralement sur la familiarisation avec celui-ci, la confirmation de l'adéquation des fonctionnalités aux besoins, la cohérence des résultats préliminaires, etc. Concernant le MBSA et Cécilia (outil sélectionné), les premières activités se sont focalisées chez MBDA sur la modélisation de plusieurs chaînes de sécurité, et c'est alors que le besoin d'une méthodologie d'accompagnement a émergé.

Fort d'un partenariat et d'une participation dans le projet S2C, MBDA a été un des acteurs de la rédaction d'un guide multi-industriel aux côtés des partenaires de l'IRT Saint Exupery System X sur le sujet « MBSA modelling guide and validation report » (référence [R1]). Le sujet de confiance dans les résultats présentés auprès des autorités est par exemple cité : " *In order for internal or external reviewers, or for the certification authorites, to be confident in the presented results, it is necessary to build confidence in the model itself. One option could be asking reviewers to analyse exhaustively the producted model. However, this would necessitates reviewers to always fully master both the modelling language and the tool, and would be highly complicated by the great variety of modelling possibilities and strategies.*". En synthèse, ce propos précise qu'effectivement, pour être rassuré sur la qualité et la validité des résultats, il faut bâtir une réelle confiance dans le modèle lui-même.

Ce document a été une donnée d'entrée importante pour identifier les étapes clés à propos des concepts de spécification, vérification et validation du modèle. Cependant, l'étude de la charge de travail, du gain de temps et l'identification claire de documents/templates ne sont pas traités dans ce document, d'où l'intérêt de cette communication.

En analysant les recommandations dans d'autres secteurs que celui de la défense, il apparaît que les problématiques de vérification/validation sont bien considérées concernant les outils de démonstration. Le secteur du nucléaire et la réalisation des Etudes Probabilistes de Sûreté (EPS) sont concernés à travers les guides de démonstration de sûreté nucléaire, notamment le guide AIEA SSG-03 (référence [R2]) : « *Any calculational methods and computer codes used in the safety analysis shall undergo verification and validation. PSA involves a number of analytical methods. Depending on the scope of the analysis (Level 1, 2 or 3 PSA), these include the analysis of accident sequences and their associated systems, typically through the development of event tree and fault tree logic models along with methods for the solution of these logic models; the development of models of phenomena that could occur, for instance, within the containment and/or the spent fuel building of a nuclear power plant following core damage and/or fuel damage; and the development of models for the transport of radionuclides in the environment to determine their effects on health and the environment. Prior to their application, it should be demonstrated that these analytical methods provide an adequate representation of the processes taking place. In accordance with para. 4.60 of GSR Part 4 […], the computer codes that support these analytical methods are required to be adequate for the purpose and scope of the analysis, and the controlling physical and logical equations are required to be correctly programmed in the computer codes.*"

Par ailleurs, une investigation a été menée sur les publications des 5 dernières années pour les congrés LambdaMu : le sujet d'accompagnement méthodologique du MBSA n'a pas été traité dans une quelconque publication.

II. INTRODUCTION

Le MBSA est une méthodologie novatrice et déjà reconnue pour ses intérêts divers : générer automatiquement des séquences permettant de traiter des problèmes non accessibles par les autres méthodes d'analyses de sécurité, faciliter la comparaison entre plusieurs concepts de sécurité, visualiser la propagation de pannes au sein d'un système, etc. En plus de bénéfices pour le métier Sûreté de Fonctionnement, l'approche modèle est également un outil de communication collaboratif intéressant, entre responsables Sûreté de Fonctionnement et équipes design/architectes, permettant de fluidifier les explications, démonstrations ou prises de décision sur l'architecture de sécurité.

Du fait de ces bénéfices et de l'aspect déterminant d'un modèle partageable à l'ensemble d'une communauté, il apparaît rapidement un besoin de garantir la validité de ce qui est diffusé aux autres métiers, en plus de l'exploitabilité des résultats en sortie du modèle. La méthodologie MBSA restant à ce stade assez "nouvelle" ou peu répandue, un travail pédagogique et des démonstrations doivent être réalisés pour convaincre les responsables des projets ou les clients de ses possibilités de la maîtrise du développement et de la pertinence des résultats. La capacité du modèle à être audité est également primordiale. Les travaux sur cette méthode ont mis en avant le besoin de s'appuyer réellement sur le modèle comme produit de confiance pour communiquer. De plus, la construction d'un process est une étape clé pour passer d'une production d'un modèle simple au déploiement à la chaîne de multiples modèles.

Au regard du temps et de l'investissement nécessaire à la réalisation d'un modèle représentatif sur les systèmes complexes, la problématique principale est donc la suivante : garantir un niveau de qualité dans les activités de développement MBSA tout en maitrisant l'impact sur la charge travail additionnelle. L'objectif est donc de trouver un équilibre entre : fournir des éléments de justification complémentaires et ne pas rendre la réalisation globale d'un MBSA trop chronophage, ceci pour que la réalisation d'un modèle puisse toujours être bénéfique.

La méthode de démonstration sélectionnée dans le présent document est la suivante :

- Identifier les pistes d'amélioration ou manquements actuels sur la réalisation d'un MBSA seul, réduisant l'efficacité dans la réalisation et restreignant la confiance quant à la validité du modèle final,
- Basé sur l'identification de ces pistes d'amélioration ou manquements, fournir des solutions concrètes pour la prise en compte de ces éléments dans le processus de déploiement de la méthode et surtout les inscrire dans une démarche d'ingénierie Sûreté de Fonctionnement complète.

Les thématiques suivantes ont été sélectionnées comme axes de travail principaux dans le but de définir une démarche d'accompagnement du MBSA et répondre à la problématique mentionnée ci-dessus.

- 1) Définir le périmètre de modélisation,
- 2) Définir des exigences et justifier la conformité à ces exigences,
- 3) Maîtriser et connaître l'outil de modélisation,
- 4) Maîtriser les principes de modélisation,
- 5) Savoir intégrer le MBSA dans le cycle de vie du produit et d'une étude de Sûreté de Fonctionnement,
- 6) Tracer les hypothèses de modélisation,
- 7) Vérifier et valider le modèle.

A noter que l'hypothèse prise dans cette proposition est que le MBSA est pour l'instant produit seul, sans aucun document annexe et à partir de données d'entrées délivrées par l'autorité de conception (schéma d'architecture, synoptique, schéma électriques…). Dans les paragraphes suivants sont exposés les pistes d'améliorations considérées dans ce contexte.

III. MÉTHODOLOGIE

A. Axes d'améliorations

1) Définir le périmètre de modélisation

Etant donné la complexité grandissante des systèmes, la modélisation de ces derniers peut rapidement être couteuse en ressource humaine et financière. Pour des systèmes très complexes ou des systèmes de systèmes, une erreur à éviter serait de vouloir modéliser la totalité du système ou de reproduire à l'identique un schéma électrique ou synoptique. Pour éviter cela, la définition du périmètre de modélisation paraît primordiale, pour permettre de :

- Cibler les efforts de modélisation sur les fonctionnalités critiques en identifiant et en se limitant aux chaines de sécurité pertinentes,
- Observer certains évènements redoutés en priorité, par exemple ceux connus comme critiques pour la tenue d'objectifs de sécurité ou ceux pour lesquels le MBSA (et la propagation de pannes) a vraiment un intérêt. *Exemple : un évènement redouté ciblé sur la défaillance structurelle intrinsèque d'un composant n'est pas forcément intéressant à étudier dans un modèle, car aucune propagation de pannes n'est à observer,*
- Travailler sur certaines phases de vie spécifiques notamment lorsque le MBSA est utilisé pour éprouver une architecture de sécurité, par exemple celles étant connues comme représentant un risque important pour la sécurité. *Exemple : dans la défense ou l'aéronautique, un système en stockage non alimenté peut présenter moins de risque que lorsqu'il est utilisé dans un environnement « opérationnel ». Par conséquent, si le temps alloué à l'activité MBSA est restreint et que la génération de résultat ne peut être lancée sur toutes les phases, la priorité doit être donnée aux phases de vie les plus « sensibles » pour la sécurité.*

2) Définir les exigences et justifier de la conformité à ces exigences

La réalisation d'un MBSA s'inscrit dans une démarche de Sureté de Fonctionnement au sein d'un projet répondant à échéances. Lors de la définition de ce besoin et en toute première étape, il paraît indispensable de spécifier les éléments à modéliser et notamment de cadrer par des exigences pour les raisons suivantes :

- Formaliser explicitement la demande du programme afin d'éviter les écarts finaux par rapport au cahier des charges (données d'entrée, phases de fonctionnement et de mise en œuvre du produit, chaines de sécurité dédiées, modélisation de sous-systèmes en particulier, etc.),
- Cadrer le périmètre pour éviter la modélisation d'éléments superflus (cf. paragraphe 1)),
- Cadrer la réalisation pour que le modèle suive rigoureusement le processus de la société (utilisation d'une bibliothèque de composants spécifiques, règles de nommage des briques, libellé des modes de pannes, etc.).

Dès lors, la justification de la conformité du modèle à ces exigences permettra de tracer toutes les étapes de vérification et de s'assurer que le modèle est alors bien conforme au besoin d'origine. Les autorités de validation ou d'audit (internes ou externes)

pourront disposer alors d'éléments concrets leur permettant d'évaluer la qualité du « livrable », et se rassurer sur la fidélité des éléments modélisés avec le système :

- Exhaustivité des éléments modélisés,
- Exhaustivité des phases de vies modélisées,
- Exhaustivité des évènements redoutés modélisés,
- Conformité aux règles de modélisation.

Note : l'application du MBSA chez MBDA a permis de souligner qu'il était préférable de statuer sur le périmètre de modélisation (voir paragraphe 1) avant de définir les exigences. En effet, si les exigences sont définies avant la définition des éléments à modéliser, bon nombre d'exigences peuvent être rédigées sans être finalement applicables. *Exemple : la présente proposition détaille (voir paragraphe B - Fig. 1) notamment des exigences sur la décomposition fonctionnelle et structurelle de n chaines de sécurité. Si ces chaînes de sécurité sont finalement hors périmètre, la définition d'exigences associées n'est pas pertinente et engendre une augmentation du temps de travail global (voir paragraphe IV.B.2).*

3) Maîtriser et connaître l'outil de modélisation

Chaque outil utilisé pour la réalisation d'un MBSA (SimfiaNeo, Cécilia…) présente des spécificités et nécessite un temps important de prise en main. La durée de modélisation « intrinsèque » dans l'outil peut être conséquente selon la complexité du système, d'où le besoin d'être agile rapidement dans l'environnement de travail. Il paraît donc nécessaire de :

- Connaître et comprendre rapidement la structure globale de l'outil (gestion des évènements à injecter, bibliothèque de composants, hiérarchisation en équipements/composants, etc.),
- Maîtriser les fonctionnalités de l'outil, étant donné qu'une connaissance partielle ou dégradée peut entrainer la multiplication de tâches unitaires alors que les outils permettent de gérer des tâches multiples. *Exemple : Cécilia offre la possibilité de lancer un calcul de « génération de séquences » pour un « batch » de cibles (potentiellement générer les résultats pour plusieurs évènements redoutés) sans avoir à les sélectionner unitairement,*
- Maitriser la capacité à exploiter un modèle MBSA et à traiter les données de sorties (simuler, générer des résultats, synthétiser les données de sortie…), sans quoi son application serait vaine,

De plus, des erreurs liées à l'absence de maitrise ou à une mauvaise connaissance de l'outil peuvent représenter une augmentation du temps de modélisation, voire même une modélisation d'un comportement supposé sûr à tort :

- Suite à une erreur, la « déconstruction » ou la suppression de composants peut laisser des liens orphelins et nécessiterait une mise à jour des composants environnants,
- Des erreurs dans le code rédigé permettant d'exprimer le comportement du composant (en fonction de l'état de ses entrées, de son « statut » ou des modes de pannes) sont rédhibitoires pour lancer un calcul ou lancer le modèle en mode « simulation ».

Pour traiter ces erreurs de code à l'origine, il est important de respecter une méthodologie et avoir à sa disposition une liste des bonnes pratiques, notamment sur les règles d'écriture de code ou de structure. Le débug ou la recherche des composants empêchant la compilation du modèle sont des éléments très chronophages dans la réalisation d'un MBSA.

Il apparait à travers ces divers exemples que la connaissance de l'outil et de l'ensemble de ses fonctionnalités permet au modélisateur d'éviter des erreurs le pénalisant dans sa réalisation. La capitalisation est également un élément important qui permet d'éviter les pièges classiques et diffuser les bonnes pratiques aux personnes d'un même département.

Finalement, il est donc pertinent de mettre à sa disposition des éléments lui permettant : de comprendre rapidement la structure et le fonctionnement de l'outil, prendre en main rapidement et efficacement l'outil sélectionné pour réaliser le MBSA et éviter les erreurs usuelles. Vis-à-vis de la problématique de gestion de charge de travail, ces éléments permettent de gagner du temps au global dans la réalisation d'un modèle et ainsi en efficacité. L'homogénéité des approches favorise également les étapes de revues et relectures par les pairs.

4) Maîtriser les principes de modélisation

Avec l'expérience de plusieurs programmes sur lesquels le MBSA est déployé, des principes de modélisation ont été capitalisés et sont déclinés sur les futures applications comme des « consignes » ou « suggestions ». Ci-dessous une liste non exhaustive de règles classiques de modélisation, qui doivent être considérées acquises au démarrage d'un MBSA.

- Modéliser au « juste besoin » : il paraît primordial d'évaluer le niveau requis pour un modèle MBSA. En effet, descendre à un niveau composant, surtout sur des cartes électroniques (résistance, capacité, diode…) dans un modèle n'est pas forcément pertinent car le niveau « fonctionnel » peut convenir au besoin de l'analyse sécuritaire. On peut s'autoriser par ailleurs de ne pas être homogène dans les niveaux de décomposition. *Exemple : Un modèle MBSA est réalisé pour étudier les propagations de pannes multi-système très-haut niveau (étude des interactions entre tous les systèmes d'un avion : hydraulique, freinage, commande de vol, distribution électrique…). L'effort de modélisation devra être mis avant tout sur l'exhaustivité des interactions entre les systèmes au niveau des interfaces. Une modélisation fine des composants de très bas niveau au sein de ces systèmes ne sera pas nécessaire,*

- Les phases de vie à représenter : le MBSA restant une méthodologie utilisée pour des analyses de sécurité, il paraît primordial d'inciter à réfléchir au démarrage d'un projet aux phases de vies pertinentes à modéliser. En effet, des configurations initiales particulières devront être fixées pour chaque phase de vie, ajoutant un besoin de fixer un nombre de variables non négligeable à des états donnés. Si aucun évènement redouté n'est étudié dans une phase de vie du système, elle ne paraît pas forcément pertinente à modéliser,

- Les états des flux physiques à représenter : des consignes peuvent être données pour préciser le besoin d'évaluer le nombre d'états strictement nécessaire pour chacun des flux. En effet, définir de nombreux états différents pour un même flux engendre une densification du code de chaque composant. Ceci rejoint le besoin de modéliser « au juste besoin » pour ne pas apporter une complexité inutile. *Exemple : pour un flux de type « électrique » (numérique, pas analogique), beaucoup d'états différents peuvent être considérés. Cependant, pour un bon nombre d'applications, les trois états suivants sont suffisants pour les analyses de sécurité : « Haut », « Bas », « Haute Impédance ». Ce qui est intéressant ici c'est que fonctionnellement, ces 3 niveaux aboutissent à des comportements différents et en fonction de la défaillance entraînant une ouverture de circuit. Il faut que les énumérés des flux puissent rendre compte du comportement fonctionnel et dysfonctionnel*,

- Les modes de pannes impliqués : les défaillances des composants listées dans l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC) ne sont pas toutes intéressantes pour les analyses de sécurité et spécifiquement pour le MBSA. Ajouter des modes de pannes n'ayant pas d'effet ou pas de conséquence sécuritaire ne sont pas pertinents pour l'analyse. Des consignes peuvent être données dans ce sens.

Il apparaît pertinent de fournir ces lignes directrices aux modélisateurs, afin de gagner du temps dans les premières étapes et cibler la modélisation sur un niveau suffisant pour correspondre au besoin du projet, tout en facilitant les échanges avec les pairs et leur relecture. Cependant, il revient au modélisateur d'avoir un avis critique sur les éléments à modéliser, et donc d'avoir une connaissance des méthodologies de sûreté de fonctionnement.

5) Savoir intégrer le MBSA dans le cycle de vie du produit

Le fait de cadrer la production du MBSA par rapport au cycle de développement du produit peut également être une opportunité de gagner en efficacité pour les raisons suivantes :

- Démarrer la réalisation d'un modèle dans la descente ou la remontée du cycle en V ne peut pas être dédié à la même finalité : au démarrage d'un programme, le MBSA peut être un outil pertinent pour étudier les sensibilités d'architecture et tester plusieurs concepts de sécurité. Dans la remontante du cycle, le MBSA peut être utilisé à des fins de démonstration de l'adéquation du produit aux objectifs de sécurité du cycle. La « finesse » de modélisation, les composants à modéliser et les événements redoutés à observer peuvent différer assez nettement selon l'une ou l'autre des options,

- Comme mentionné dans le paragraphe 3), les travaux de déconstruction des modèles MBSA sont chronophages. De plus, ils peuvent être à l'origine d'introduction d'erreurs car les changements sont trop nombreux ou leurs impacts mal propagés. Pour une application précoce du MBSA, il est préconisé d'attendre d'avoir des concepts d'architecture de sécurité au maximum figés avant de démarrer une quelconque modélisation. Une autre possibilité peut être la co-ingénierie : la construction du modèle en parallèle de la définition de l'architecture de sécurité au travers de séances de travail communes. Cela permet à l'analyste Sûreté de Fonctionnement de valoriser son travail et au projet de capitaliser sur les recommandations,

- Selon les modèles et le niveau de détail, la charge de travail pour aboutir à un modèle finalisé reste conséquente. Il peut être bénéfique de définir l'ensemble des tâches à réaliser afin de faciliter et sécuriser la gestion des ressources et des budgets associés à cette activité.

Basé sur ces éléments, il est intéressant de fournir aux modélisateurs des « recommandations » à consulter obligatoirement avant de se lancer dans une modélisation.

6) Tracer les hypothèses de modélisation

Le principe d'une modélisation inclus assez systématiquement des abstractions. Des écarts apparaissent régulièrement entre le comportement réel d'un composant et celui modélisé, par exemple pour les raisons suivantes :

- Une partie du comportement du composant n'est pas pertinent pour l'analyse de sécurité. *Exemple : mode de défaillance n'engendrant pas d'effet sécuritaire*,

- Des modes de défaillances ou états de flux peuvent être « rassemblés » car ils conduisent finalement au même effet et n'auraient pas d'impact spécifique dans la propagation de panne. *Exemple : sur une pièce mécanique, si un effort « nominal » ou un effort « maximal » mènent tous deux à la rupture, il n'est pas forcément nécessaire de traiter ces deux cas*. Ce procédé peut être comparé à celui de la production d'une « FMES », qui générée à partir d'une AMDEC, ceci pour rassembler des modes de pannes.

De plus, le modélisateur peut prendre le parti de ne pas modéliser certaines briques, de figer à un état donné certaines entrées/sorties, d'occulter volontairement certaines phases de vie, etc. ceci après avoir vérifié que cela n'impacte pas le comportement recherché pour le besoin du MBSA (cf. sa spécification IV.A.1). C'est pourquoi, ce type d'hypothèse doit être tracée, pour *in fine* servir les besoins du modèle final et parfaire la compréhension des personnes impliquées. Les bénéfices suivant en découlent :

- Faciliter la reprise et la mise à jour du modèle : en cas de changement de modélisateur, la personne comprendrait plus facilement les choix réalisés par son prédécesseur, ceci garantissant une prise en main plus rapide,
- Faciliter la relecture du code : un script commenté ou accompagné d'un document explicatif sera toujours plus facile à appréhender, qui plus est pour des problématiques de vérification/validation,
- La traçabilité des hypothèses pourra également permettre de cibler plus rapidement des écarts potentiels dans les résultats lorsque le MBSA est utilisé en parallèle des arbres de défaillances. En effet, les choix du modélisateur pourront potentiellement expliquer certaines incohérences, alors qu'il aurait été difficile de les identifier sans traçabilité.

7) Vérifier et valider le modèle

Une étape clé pour augmenter la confiance dans le modèle réalisé est de s'appuyer sur un processus de vérification/validation défini, clair et précis. En effet, même si le modèle produit des résultats qui semblent cohérents, il n'existe aucune garantie que le comportement modélisé soit bien cohérent (par rapport à l'analyse fonctionnelle, par rapport à la définition…) et que ces résultats puissent être considérés valides. Par conséquent, il est recommandé de passer obligatoirement par une étape de vérification et de validation : l'objectif est de vérifier chaque brique créée, de garantir que le modèle est représentatif du comportement attendu du système (en jouant par exemple les scénarios dysfonctionnels connus par les architectes systèmes) et en validant que le modèle répond correctement. Les niveaux de vérification peuvent être différents : au niveau structurel, au niveau des briques de base, ou au niveau de l'intégration globale. A travers ce travail de vérification/validation, le modélisateur pourra également obtenir un regard extérieur qui diffère d'une vision orientée « maîtrise des risques ».

Ceci est en adéquation avec le besoin d'offrir au projet/client des éléments justificatifs permettant d'attester que le modèle a bien suivi une phase de vérification, contribuant à démontrer un niveau de maturité suffisant du modèle en rapport avec l'objectif visé. Il est également intéressant de pouvoir faire participer d'autres métiers que celui du modélisateur, et ainsi avoir un regard extérieur sur les éléments modélisés.

B. Solution proposée

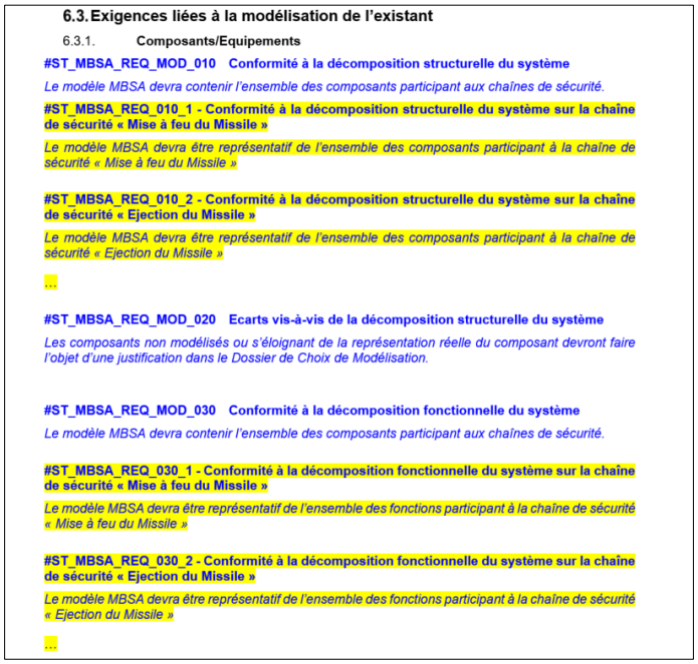
Au regard des pistes d'améliorations identifiées, il semble pertinent que le modèle soit accompagné par des lignes directrices et justifications complémentaires. La proposition est de fournir un corpus documentaire en marge du modèle, à initialiser avant le démarrage du MBSA et à faire vivre tout au long de sa réalisation. Ci-dessous un descriptif des livrables proposés :

TABLE I. DOCUMENTS DU CORPUS DOCUMENTAIRE

Document	***Piste d'amélioration du §B.***	***Type***	***Objectif***	***Période de mise en place***
Spécification Technique	1) Définir le périmètre de modélisation 2) Définir des exigences et justifier la conformité 7) Vérifier et valider le modèle	Template à saisir par le modélisateur	Cadrer par des exigences la réalisation du MBSA	Au démarrage du projet, avant l'initialisation du modèle
Dossier de Choix de Définition	2) Définir des exigences et justifier la conformité 7) Vérifier et valider le modèle	Template à saisir par le modélisateur	Analyser la conformité du MBSA avec les exigences fixées dans la Spécification Technique	Au démarrage du projet, à compléter tout au long de la vie du modèle
Procédure de Réaliation d'un MBSA	3) Maîtriser et connaître l'outil de modélisation	Document générique fourni au modélisateur	Description des étapes à suivre pour la construction d'un modèle en accord avec les règles du département et les spécificités de l'outil	Non applicable. A consulter avant le démarrage de la modélisation
Guide de Réalisation d'un MBSA	4) Maîtriser les principes de modélisation 5) Savoir intégrer le MBSA dans le cycle de vie du produit	Document générique fourni au modélisateur	Identifier les processus et justifier la pertinence de la réalisation d'un MBSA en accord avec les règles du département	Non applicable. A consulter avant le démarrage de la modélisation
Dossier de Choix de Modélisation	6) Tracer les hypothèses de modélisation	Template à saisir par le modélisateur	Justifier les différents choix de modélisation effectués en cas d'écarts vis-à-vis de la définition du système	Au démarrage du modèle, à compléter tout au long de la vie du modèle

Ci-dessous en détail, les diverses rubriques envisagées dans chaque document. Ces informations sont données à titre indicatif et ne présagent pas d'un contenu réel appliqué au sein de la société :

- Spécification Technique :
  - Les exigences qui traitent des objectifs de modélisation, notamment quels sont les résultats attendus,
  - Les exigences qui traitent de la réalisation (comment on modélise, règles de nommage, etc.),
  - Les exigences de représentativité du modèle (sur quelle base sera vérifiée la représentativité du modèle vis-à-vis de l'objet modélisé).



6.3. Exigences liées à la modélisation de l'existant

6.3.1. **Composants/Equipements**

#ST_MBSA_REQ_MOD_010 Conformité à la décomposition structurelle du système

Le modèle MBSA devra contenir l'ensemble des composants participant aux chaînes de sécurité.

#ST_MBSA_REQ_010_1 - Conformité à la décomposition structurelle du système sur la chaîne de sécurité « Mise à feu du Missile »

Le modèle MBSA devra être représentatif de l'ensemble des composants participant à la chaîne de sécurité « Mise à feu du Missile »

#ST_MBSA_REQ_010_2 - Conformité à la décomposition structurelle du système sur la chaîne de sécurité « Ejection du Missile »

Le modèle MBSA devra être représentatif de l'ensemble des composants participant à la chaîne de sécurité « Ejection du Missile »

...

#ST_MBSA_REQ_MOD_020 Ecarts vis-à-vis de la décomposition structurelle du système

Les composants non modélisés ou s'éloignant de la représentation réelle du composant devront faire l'objet d'une justification dans le Dossier de Choix de Modélisation.

#ST_MBSA_REQ_MOD_030 Conformité à la décomposition fonctionnelle du système

Le modèle MBSA devra contenir l'ensemble des composants participant aux chaînes de sécurité.

#ST_MBSA_REQ_030_1 - Conformité à la décomposition fonctionnelle du système sur la chaîne de sécurité « Mise à feu du Missile »

Le modèle MBSA devra être représentatif de l'ensemble des fonctions participant à la chaîne de sécurité « Mise à feu du Missile »

#ST_MBSA_REQ_030_2 - Conformité à la décomposition fonctionnelle du système sur la chaîne de sécurité « Ejection du Missile »

Le modèle MBSA devra être représentatif de l'ensemble des fonctions participant à la chaîne de sécurité « Ejection du Missile »

...

Fig. 1. Exemple d'exigences formalisées dans la Spécification Technique. En bleu sont proposées les exigences génériques à appliquer par le modélisateur, en jaune sont proposées des exigences spécifiques au modèle.

- Dossier de Justification de Définition : matrice de conformité aux exigences de la Spécification Technique (avancement, jalon, analyse de conformité, justification de la potentielle non-conformité, etc.).

Item Exigence	Catégorie	Libellé	Description	Paragraphe de la ST	Avancement	Jalons	Type de justification	Conformité prévisionnelle	Eléments de justification	Justification de la non-conformité
#ST_MBSA_REQ_PROC_010	PROCESS	Etapes de développement du MBSA	Les étapes présentées dans le Guide de Réalisation du MBSA devront être suivies et les livrables attendus pour chaque jalon devront être initiés et mis à jour tout au long du développement.	§6.1						
#ST_MBSA_REQ_PROC_010_1	PROCESS	Pertinence et applicabilité de la modélisation	Le modélisateur devra s'assurer de la pertinence et de l'applicabilité de l'utilisation du MBSA pour sa problématique.	§6.1.1						
#ST_MBSA_REQ_PROC_010_2	PROCESS	Définition du périmètre	Plusieurs réunions préliminaires devront être organisées entre le responsable de l'étude et le modélisateur afin de définir le périmètre de modélisation.	§6.1.1						
#ST_MBSA_REQ_PROC_010_3	PROCESS	Définition de l'utilisation future du modèle	Le modélisateur devra définir l'utilisation future qui sera faite du modèle MBSA, afin d'identifier la granularité de modélisation nécessaire.	§6.1.2						
#ST_MBSA_REQ_PROC_010_4	PROCESS	Mise à jour de la bibliothèque métier	Le modélisateur devra mettre à jour la bibliothèque métier en continu pour être suivie dans la base de gestion RTC.	§6.1.3						
#ST_MBSA_REQ_PROC_010_5	PROCESS	Archivage des versions du modèle	Le modèle devra être archivé dans ces différentes versions et mis à jour suivant les différents besoins présentés dans le Guide de Réalisation du MBSA.	§6.1.3						
#ST_MBSA_REQ_REG_010_1	REGLES	Utilisation de la Bibliothèque Métier	La bibliothèque générique en vigueur au sein du Département SdF devra être utilisée en priorité pour la modélisation des composants, équipements et flux.	§6.2.1						
#ST_MBSA_REQ_REG_010_2	REGLES	Ecarts vis-à-vis de la Bibliothèque Métier	Les items conçus en écart à la bibliothèque devront faire l'objet d'un paragraphe dédié dans le Dossier de Choix de Modélisation.	§6.2.1						
#ST_MBSA_REQ_REG_020_1	REGLES	Libellé des briques et des flux du modèle	La dénomination des composants dans le modèle MBSA devra permettre d'identifier clairement et distinctement chaque composant de l'architecture du système afin de pouvoir faire le lien avec les autres documents d'architecture (schémas d'architecture, synoptiques, MBSE...).	§6.2.2						
#ST_MBSA_REQ_REG_020_2	REGLES	Respect des conventions de nommage des briques et des flux du modèle	La dénomination des composants dans le modèle MBSA devra respecter les conventions de nommages prescrites dans la Procédure.	§6.2.2						
#ST_MBSA_REQ_REG_020_3	REGLES	Etats des flux de type « énumérés »	Le typage des flux de type énumérés devra respecter les prérogatives de la Procédure.	§6.2.2						
#ST_MBSA_REQ_REG_030	REGLES	Respect des conventions de nommage de l'arborescence sous Cécilia	La dénomination des objets créés dans l'arborescence (Projet, Equipement, Composant, Type) de Cécilia devra respecter les conventions de nommages prescrites dans le document « MBSA - Règles de nommage ».	§6.2.3						
#ST_MBSA_REQ_REG_040_1	REGLES	Libellé des Modes de Pannes et cohérence avec l'AMDEC	La dénomination des modes de pannes dans le modèle MBSA devra permettre d'identifier clairement et distinctement chaque mode de panne identifié dans l'AMDEC. Si les libellés ne sont pas similaires entre le MBSA et l'AMDEC, un tableau de correspondance devra être fourni.	§6.2.4						
#ST_MBSA_REQ_REG_040_2	REGLES	Respect des conventions de nommage des Modes de Pannes	La dénomination des modes de pannes dans le modèle MBSA devra respecter les conventions de nommages prescrites dans le document dédié « MBSA - Règles de nommage ».	§6.2.4						
#ST_MBSA_REQ_MOD_010	MODELISATION	Conformité à la décomposition structurelle du système	Le modèle MBSA devra contenir l'ensemble des composants participant aux chaînes de sécurité.	§6.3.1						
#ST_MBSA_REQ_MOD_010_1	*MODELISATION*	*Conformité à la décomposition structurelle du système sur la chaîne de sécurité « Mise à feu du Missile »*	*Le modèle MBSA devra être représentatif de l'ensemble des composants participant à la chaîne de sécurité « Mise à feu du Missile »*	*§6.3.1*						
#ST_MBSA_REQ_MOD_010_2	*MODELISATION*	*Conformité à la décomposition structurelle du système sur la chaîne de sécurité « Ejection du Missile »*	*Le modèle MBSA devra être représentatif de l'ensemble des composants participant à la chaîne de sécurité « Ejection du Missile »*	*§6.3.1*						
#ST_MBSA_REQ_MOD_020	MODELISATION	Ecarts vis-à-vis de la décomposition structurelle du système	Les composants non modélisés ou s'éloignant de la représentation réelle du composant devront faire l'objet d'une justification dans le Dossier de Choix de Modélisation.	§6.3.1						

Fig. 2. Matrice de conformité aux éxigences de la Spécification Technique MBSA. En noir sont proposées les exigences génériques à appliquer par le modélisateur, en jaune sont proposées des exigences spécifiques au modèle.

- Procédure de Réalisation d'un MBSA :
  - Procédures générales descriptives : structure globale de l'outil, gestion des icônes, types, création d'une brique, vue globale d'un système, gestion des attributs quantitatifs, gestion des fichiers de résultats et exploitation,
  - Règles méthodologiques de la société : hiérarchisation, règles de nommage, gestion des bibliothèques, spécification des types de flux à utiliser, traitement des composants spécifiques.
- Guide de réalisation d'un MBSA : méthodologie et processus Sûreté de Fonctionnement de la société, principales étapes à dérouler en fonction de la phase de développement du produit.
- Dossier de Choix de Modélisation : présentation du modèle, description des interfaces extérieures, phases de vies modélisées, évènements redoutés considérés, types de flux, description et justification des choix de modélisation.

Ces cinq documents permettent de concaténer l'ensemble des informations permettant de répondre aux différentes pistes d'améliorations détaillées dans le paragraphe A.

IV. Resultats

A. Retour d'experience sur la mise en œuvre

MBDA a sélectionné plusieurs programmes pour mettre en œuvre cette méthodologie d'accompagnement au MBSA : un projet A en développement a un jalon équivalent à une Revue de Design Préliminaire (PDR) et un projet B où le MBSA est utilisé dans la remontée du cycle en V à des fins de validation des résultats des arbres de défaillances.

1) Spécification Technique

Sur les projets A et B, l'objectif est que le MBSA soit représentatif de l'ensemble des chaînes de sécurité des systèmes. De ce fait, les limites physiques du modèle sont assez rapidement identifiées. La rédaction du document permet surtout d'introduire les exigences associées aux règles génériques du processus de réalisation MBSA de la société et de lister tous les éléments « à modéliser », qui seront donc à vérifier/valider à travers le Dossier de Justification de Définition.

Il apparaît une certaine difficulté pour le modélisateur à prendre en main le document et au client/responsable projet de rédiger les exigences. Si le processus de vérification/validation aspire à être exhaustif, la définition des exigences liées à la décomposition structurelle du système, aux flux définis, aux phases de vies et aux ER représentés doit être très précise. Cet aspect peut être perçu comme assez lourd lorsque le modélisateur a à sa charge la réalisation du modèle et potentiellement la compréhension du système à modéliser.

Au démarrage de ce type d'activité, le travail de rédaction d'exigences peut être conséquent. Deux visions se sont d'ailleurs opposées lorsque ce besoin a été proposé comme première étape pour la réalisation du MBSA, avec en priorité :

- le besoin de réaliser un modèle rapidement pour évaluer si l'architecture en place sur le projet A (projet en développement) est convenable en terme de principes sécurité, quitte à privilégier la réalisation intrinsèque par rapport à la définition des exigences ;
- le besoin de spécifier dès le départ le modèle comme un produit réel pour qu'il réponde aux attentes du projet.

A noter que les responsables programmes étaient particulièrement sensibles à la manière de vérifier et valider le modèle, justifiant encore plus l'intérêt d'un tel document.

2) Dossier de Justification de Définition

Voir ci-dessus le retour d'expérience sur la Spécification Technique, qui découle en terme de vérification de conformité sur le Dossier de Justification de Définition.

3) Procédure de Réalisation d'un MBSA

Selon ce que l'entité rédactrice veut y voir figurer et en fonction de l'outil sélectionné, la procédure peut être un document assez volumineux à produire. Dans le cadre de l'application sur les programmes A et B, les modélisateurs étaient assez habitués au fonctionnement de l'outil et aux principes généraux, donc la procédure a plus fait figure d'un « support » plutôt que d'une aide continue.

Cependant, il apparaît pour les personnes non initiées que cette procédure est réellement pertinente sur la navigation dans l'outil et l'uniformisation des règles (conventions d'écriture, gestion des bibliothèques communes, homogénéisation des flux à utiliser…). Il peut s'agir d'un complément à la documentation technique utilisateur mise à disposition par l'éditeur du logiciel, en apportant par exemple des captures d'écrans sur les étapes clés classiques.

Vis-à-vis de l'application sur les projets A et B, il apparaît également que ce document peut être une base de capitalisation intéressante pour diffuser les informations à l'ensemble d'un département travaillant sur le MBSA. Une fois rédigée, la procédure a notamment été utilisée pour :

- Synthétiser les conseils et astuces non décrites dans la documentation technique utilisateur ;
- Compléter aux fur et à mesure les règles méthodologiques liées aux règles d'écriture de code ou règle de nommage par exemple ;
- Décrire le fonctionnement d'outils développés et utilisés en marge du MBSA, notamment pour post-traiter les fichiers de sortie.

Finalement, ce document est une aide non négligeable pour faire ses premiers pas dans le MBSA et pour comprendre son application dans l'entité qui utilise l'outil. Il est possible de gagner du temps dans la période de formation du modélisateur. Il est tout de même à noter que les descriptions des étapes ne sont valables que pour l'outil concerné, ce document devant être adapté en cas d'hypothétique changement de logiciel.

4) Guide de Réalisation d'un MBSA

A l'instar de la Procédure de Réalisation d'un MBSA, le Guide de Réalisation est un document permettant de faciliter la compréhension de la méthodologie et des étapes clés associées. Pour les personnes non initiées à la modélisation et aux règles du département, il a été possible d'identifier si la réalisation d'un modèle était vraiment pertinente au vu de la complexité du système ou du jalon programme considéré. De plus, le modélisateur ou le projet a pu faire un état des lieux précis du travail total qu'il aura à réaliser en marge du modèle : identification des objectifs, traçabilité et gestion de configuration au sein de la

bibliothèque de composants métier, étapes de vérification/validation, etc. Au vu de l'application sur les cas réels, les modélisateurs s'étant appuyés sur le Guide de Réalisation d'un MBSA ont pu organiser la réalisation du modèle avec plus de clarté : ils ont pu bénéficier en amont des éléments attendus dans chaque phase de vie du modèle. Ce document est donc primordial en première approche avant de démarrer un projet de modélisation. Finalement, il permet aussi une uniformisation du processus à travers les différents programmes.

5) Dossier de Choix de Modélisation

Suite à l'application sur différents projets, plusieurs aspects du Dossier de Choix de Modélisation ont été remontés comme intéressants pour l'accompagnement d'un modèle MBSA.

- Présentation du modèle et des interfaces modélisées : un document autoporteur peut permettre aux parties prenantes extérieures de comprendre ce qui a été modélisé ;
- Liste des évènements redoutés analysés dans le modèle : intéressant pour comparer les évènements redoutés de l'Analyse Préliminaire de Risques (APR) avec ceux étudiés dans le modèle MBSA, et évaluer ainsi la capacité du modèle à alimenter les démonstrations de sécurité ;
- Liste des choix et des hypothèses : ceci permet de dresser un état des lieux des potentiels écarts entre le système physique et le système modélisé, et d'identifier ainsi rapidement s'il s'avère que les résultats du MBSA diffèrent de ceux des Arbres de Défaillances ;
- Maintenabilité du modèle : en cas de reprise, le retour d'expérience démontre que la personne reprenant le modèle peut plus facilement comprendre la manière dont le MBSA a été réalisé et les choix qui ont été faits.

B. Impact sur le temps total de travail

Pour rappel, la problématique initiale de cette étude est la suivante : s'assurer qu'il est possible de s'appuyer sur les résultats avec un niveau de confiance suffisant en garantissant une charge de travail supplémentaire raisonnable et maîtrisée. Il est donc intéressant de quantifier, dans la mesure du possible, l'impact sur la charge de travail de la mise en place du corpus documentaire décrit ci-dessus.

Lors de la rédaction de ce document, des métriques précises n'étaient pas disponible sur le temps de déploiement du package documentaire et sur le gain de temps généré sur les projets A et B. De plus, la rédaction des Templates du TABLE I. dépendent fortement de la taille du modèle, d'où le fait qu'il est difficile de donner des données temporelles précises.

1) Diminution du temps de travail

Au vu des bénéfices exposés dans le paragraphe IV-A il est considéré que la fourniture du package documentaire permet de faire gagner du temps au modélisateur :

- Procédure de Réalisation d'un MBSA : faciliter les premiers pas et éviter de rester bloqué sur une problématique technique liée à la non maîtrise de l'outil,
- Guide de Réalisation d'un MBSA : percevoir directement le bon niveau de modélisation, éviter la « déconstruction » d'éléments du modèle et ne pas s'orienter vers une modélisation trop fine si elle n'est pas nécessaire,
- Dossier de Choix de Modélisation : gagner du temps dans la compréhension du modèle si une reprise par un autre modélisateur est nécessaire, supporter la vérification du code, identifier plus rapidement les potentielles coupes minimales « absurdes » liées à des choix de modélisation….

Une estimation de la baisse de la charge de travail a été réalisée pour évaluer les bénéfices du corpus documentaire vis-à-vis de celle du modèle MBSA, au vu du retour d'expérience sur les deux programmes mentionnés.

Légende : t représente le temps total pour la réalisation du modèle MBSA dans l'outil

TABLE II. DIMINUTION DE LA CHARGE DE TRAVAIL ASSOCIEE A LA PRODUCTION DU CORPUS DOCUMENTAIRE

Document	***Diminution du travail estimé de par la production des documents***
Spécification Technique	-
Dossier de Choix de Définition (incluant la tracabilité associée aux étapes de vérification/validation)	-
Procédure de Réaliation d'un MBSA	-15% t
Guide de Réalisation d'un MBSA	-5% t
Dossier de Choix de Modélisation	-10% t

2) Augmentation du temps de travail

Une estimation de l'augmentation de la charge de travail est également réalisée pour évaluer la part de rédaction du corpus documentaire vis-à-vis de celle du modèle MBSA. Contrairement aux chiffres mentionnés dans le TABLE II. , ces données ont

pu être recueillies avec plus de facilité car le modélisateur a pu facilement identifier le temps passé à réaliser ces activités. Une plus grande confiance peut être accordée à ces chiffres.

Légende : t représente le temps total pour la réalisation du modèle MBSA dans l'outil

TABLE III. AUGMENTATION DE LA CHARGE DE TRAVAIL LA PRODUCTION DU CORPUS DOCUMENTAIRE

Document	***Augmentation du travail estimé pour la production des documents***
Spécification Technique	+10% t
Dossier de Choix de Définition (incluant la tracabilité associée aux étapes de vérification/validation)	+30% t
Procédure de Réaliation d'un MBSA	45 jours à temps plein
Guide de Réalisation d'un MBSA	30 jours à temps plein
Dossier de Choix de Modélisation	+30% t

Il est donc estimé une augmentation de charge de 70% pour remplir les Templates du package documentaire accompagnant le modèle (Spécification Technique, Dossier de Choix de Définition et Dossier de Choix de Modélisation), et environ 75 jours pour produire les deux documents accompagnant l'utilisateur (Procédure de Réalisation d'un MBSA et Guide de Réalisation d'un MBSA). A noter que ces deux documents ne sont bien sûr pas à produire pour tout nouveau modèle MBSA.

Une synthèse de l'impact sur le temps de modélisation complet est disponible ci-dessous. Les chiffres donnés dans chaque colonne ont été calculés sur une base de temps de réalisation du modèle MBSA t = 360 jours, et représentent donc les jours passés et gagnés associés à la production de chaque document.

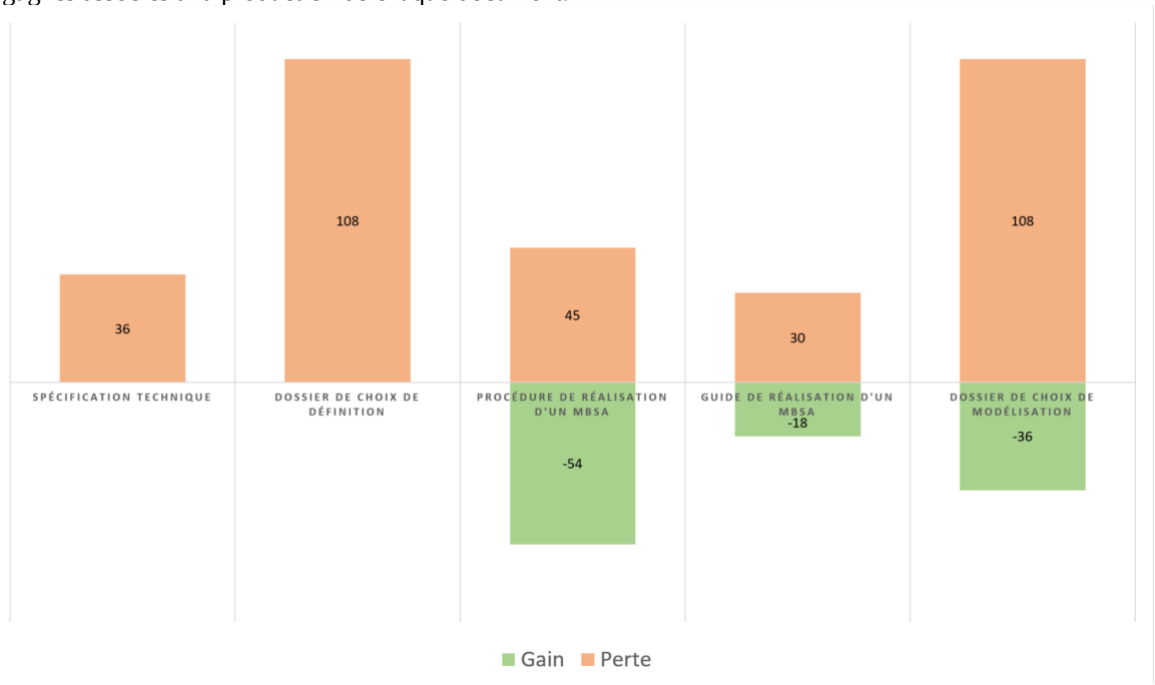


Fig. 3. Synthèse du gain et perte de temps estimé pour chaque document du Corpus Documentaire

V. DISCUSSION ET PERSPECTIVES

La réponse est partielle à ce stade et les résultats obtenus sont mitigés : selon un premier retour d'expérience, la méthodologie d'accompagnement permet vraisemblablement d'uniformiser les pratiques, mieux tracer et renforcer le niveau de confiance des décideurs dans les résultats obtenus notamment grâce au processus de vérification/validation. L'augmentation de la charge de travail, relevé à travers la problématique, est un point important : le temps de production des templates d'accompagnement du modèle est estimé à 70% du temps dédié à la modélisation, tandis que le temps pour produire les documents d'accompagnement de l'utilisateur a été évalué à 75 heures pour l'outil Cécilia. Cependant, la méthodologie permet en parallèle de diminuer le temps nécessaire sur quelques axes spécifiques de la réalisation d'un modèle.

Concernant les futures perspectives, il s'agira de mettre en application cette méthodologie sur d'autres projets pour confirmer les estimations fournies dans les TABLE II. et TABLE III. , et surtout statuer sur la pertinence de la démarche au global. Il faut bien noter que cette méthodologie ne sera mise en place sur les programmes que si le gain est effectivement avéré.

La méthode et le corpus documentaire pourront également être critiqués et optimisés, pour notamment améliorer les sujets suivants : traçabilité des exigences, définition des check-list propres de vérification/validation…Un des principaux chantiers sera

de travailler sur la génération automatique du contenu des Templates définis dans le paragraphe III à travers l'outil sélectionné pour le MBSA, permettant ainsi de fournir en quelques clics les hypothèses de modélisation, les exigences et le statut de leur traitement. Concernant Cécilia, ce sujet est déjà remonté et en cours de traitement par l'éditeur du logiciel.

Il est à noter que le sujet de ce document porte sur la « Méthodologie d'accompagnement à la réalisation d'un Model Based Safety Assessment (MBSA). La problématique pourrait être considérée à plus grande échelle, pas forcément au niveau du MBSA, mais potentiellement sur la réalisation des Arbres de Défaillances ou les calculs de fiabilité par exemple. Les sujets méthodologiques (notamment la vérification/validation) sont rarement travaillés et cadrés par des méthodes claires.

VI. Conclusion

Cette proposition fournie des résultats intéressants en vue de donner plus de garantie au MBSA. Au regard du retour d'expérience et des demandes des parties prenantes extérieures, l'accompagnement de l'utilisateur, la traçabilité des hypothèses et la vérification/validation du modèle paraît importante pour pouvoir s'appuyer sur celui-ci et alimenter les démonstrations de sécurité. La production de MBSA à la chaine est une ambition réalisable, mais le niveau de qualité associé est primordial pour entretenir la confiance dans les modèles. Comme sur toute application, la rigueur et la qualité ont un coût initial et un coût de réalisation.

Le fait de fournir des informations complémentaires en marge du modèle paraît réalisable, tout l'enjeu réside dans la gestion de la charge de travail supplémentaire et la fourniture de documents structurants que chacun puisse s'approprier. Après un retour d'expérience, même si la méthodologie proposée augmente nécessairement la charge de travail, elle permet en un sens de réduire le coût et d'augmenter très positivement la qualité de ce qui est modélisé. Elle permet également d'améliorer la capacité des modèles à être audités, condition semblant indispensable pour que le client puisse se convaincre de la validité de ce qui est modélisé.

L'objectif à court terme au sein de la société sera d'éprouver la méthodologie au complet pour confirmer les estimations de charge associée, analyser la viabilité de la méthodologie et dégager d'autres potentielles pistes d'améliorations. Ce travail reste en l'état un sujet d'investigation, l'exploration va ainsi continuer pour consolider les conclusions de l'étude et les bénéfices identifiés.

Remerciements

Les rédacteurs de la présente publication tiennent à remercier l'ensemble des participants et relecteurs de ce projet. Nos remerciements également aux parties prenantes du projet S2C, qui ont permis de cibler les axes de travail principaux sur la méthodologie d'accompagnement. De plus, tous nos remerciements aux modélisateurs des différents projets sur lesquels la méthode a été appliquée, qui ont su faire preuve de réactivité et d'esprit critique dans la remontée d'information concernant le retour d'expérience attendu.

Bibliographie

[R1]. S2C Project Team, IRT SystemX ISX-S2C-LIV-1285_v4. MBSA Modelling guide and validation report.

[R2]. IAEA Safety Standards, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants No. SSG-3 (Rev.1)