Fiche Projet IMdR

FP - Model-Based Safety Assessment 2022

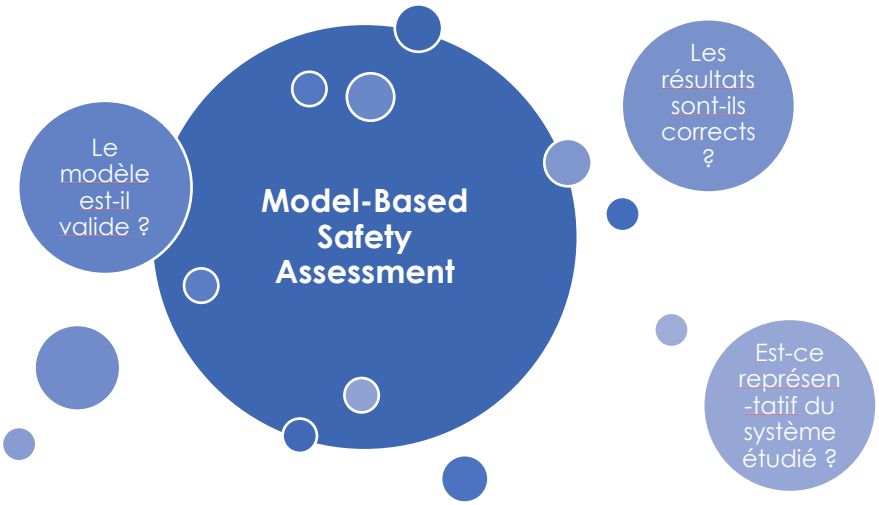
INTÉRÊT GÉNÉRAL

1. TITRE DU PROJET : REDACTION D'UN GUIDE DE REALISATION D'UNE ETUDE MBSA

2. CONTEXTE ET ENJEUX

Les méthodes « classiques » de Sûreté de Fonctionnement (Arbres de Défaillances, Diagramme de Fiabilité…) atteignent parfois leurs limites en ce qui concerne la prise en compte d'interactions et de comportements complexes (notamment dynamiques) des systèmes. Cette complexité grandissante nécessite de plus en plus de recourir à des approches Model-Based (MBSE[1], MBD[2]…). Dans le domaine de la Sûreté de Fonctionnement, des solutions de type Model-Based Safety Assessment (MBSA[3]) ont été développées pour permettre d'évaluer au mieux la sûreté et la disponibilité des systèmes complexes et d'optimiser leur maintenance.

La rupture méthodologique liée à ces solutions et la forte expressivité des langages associés peuvent parfois entraîner des questions concernant la représentativité du modèle et la pertinence des simulations réalisées. Ces doutes prennent souvent leur source dans une méconnaissance de la méthode ou des langages. Toutefois, cela révèle un enjeu majeur : comment apporter la preuve de la validité des résultats obtenus avec une approche MBSA ?



[1] MBSE : Model-Based System Engineering
[2] MBD : Model-Based Design

3. OBJECTIFS

Le but de cette initiative est de définir un cadre générique à ce type d'analyse (sans limitation à un langage ou à une solution logicielle) et de rédiger, en s'inspirant des travaux menés côté MBSE pour la norme ISO/IEC/IEEE 24641 [2], un guide de mise en œuvre de l'approche MBSA permettant de faciliter la compréhension du modèle et de garantir un fort niveau de confiance dans les résultats obtenus.

Les résultats de ces travaux seront mis en forme conformément à la trame du standard normatif international IEC, pour faciliter éventuellement une démarche normative nationale voire internationale ultérieure, si la décision en était prise.

4. RESULTATS ATTENDUS

Les résultats attendus sont les suivants :

- Etat de l'art bibliographique
- Description de la méthodologie
- Rédaction d'un guide d'utilisation (en français et en anglais)
- Traitement d'une application sur la base du guide
- Résumé de trois pages format A4 et un jeu de diapositives

5. CONSTITUTION DE L'EQUIPE PROJET

L'équipe projet est constituée des personnes suivantes :

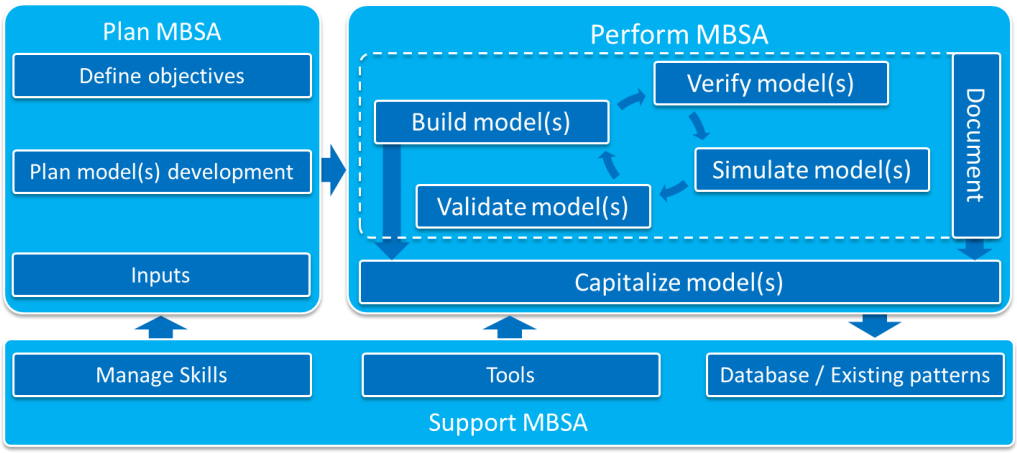
- Chef de projet : Le chef de projet est un des souscripteurs ; il aura pour rôle de piloter le projet et de gérer techniquement la prestation d'animation
- Experts MBSA :
    - Les experts MBSA seront fournis par les souscripteurs, leur participation aux travaux sera à la charge des souscripteurs
    - Les experts MBSA s'engagent à participer aux travaux durant toute la durée du projet (estimation de leur charge : 2h / mois en réunion d'avancement + travaux externes en entreprise selon le programme et l'avancement du projet)
    - Les experts MBSA auront une bonne connaissance de la mise en œuvre de la démarche MBSA dans leur entreprise
    - Leur rôle sera de prendre en charge les aspects techniques du projet.
- Animateur des travaux (prestataire)
    - Son rôle sera de :
        - Organiser et gérer l'avancement des travaux décrits par le cahier des charges, il devra avoir une bonne connaissance des processus et formalismes normatifs pour que les résultats des travaux soient mis en forme conformément aux règles de rédaction des documents normatifs IEC (normes, ou rapport technique)
        - Planifier les travaux entre experts
        - Recueillir, synthétiser et mettre en forme les éléments fournis par les experts

- Mettre en forme les résultats des travaux dans un rapport suivant les règles de rédaction d'un document normatif IEC
- Ses travaux seront financés par le projet
- Un appel d'offres sera lancé pour déterminer la meilleure proposition
- L'animateur des travaux devra avoir des connaissances en Sûreté de Fonctionnement et, si possible, une expérience de la mise en œuvre de la méthodologie MBSA

6. PROGRAMME DES TRAVAUX

Ce programme est donné à titre indicatif. Il sera bien évidemment précisé dans un cahier des charges adapté aux besoins des souscripteurs.

Tâche 1 : Définition d'un processus global en partant de la proposition de l'eSRel 2021[1] (voir figure ci-après) et en s'inspirant de la norme ISO/IEC/IEEE 24641[2] et définir le niveau de profondeur des travaux.



Tâche 2 : Définition d'un cadre générique d'analyse.

Les principaux points à traiter sont :

1. Etat des lieux (historique, état de l'art)
2. Terminologie Abréviations
3. Méthodologie MBSA
4. Domaine d'application du MBSA
5. Eléments clef du MBSA
6. Processus général
7. Planifier le MBSA

7.1. Définir les objectifs
7.2. Ajuster et Planifier le développement
7.3. Données d'entrée

8. Accompagner le MBSA

8.1. Compétences
8.2. Outils
8.3. Bases de données / modèles existants

9. Réaliser le MBSA
9.1. Construction et mise à jour du modèle
9.2. Vérification du modèle
9.3. Validation du modèle
9.4. Simulation du modèle
9.5. Capitalisation
9.6. Documentation
10. Gestion en configuration
11. Données de sortie
12. Annexe : traitement d'un exemple
13. Bibliographie

Cette liste pourra être modifiée / complétée lors de la rédaction du cahier des charges ou au cours des travaux en fonction des besoins identifiés).

Tâche 3 : Mise en forme des résultats au format normatif IEC en français

Tâche 4 : Application démonstrative sur un exemple fourni par un (des) souscripteur(s).

Tâche 5 : Traduction du rapport en anglais (optionnel en fonction du nombre de souscripteurs)

Tâche 6 : Conclusions et perspectives

7. REFERENCES

[1] F. Milcent, M. Batteux, X. de Bossoreille, T. Prosvirnova. "MBSA: Increase trust in models", Congrès eSRel, panel session (2021), Angers, France
[2] ISO/IEC/IEEE 24641 Systems and Software engineering - Methods and tools for model-based systems and software engineering
[3] A. Joshi, M. P.E. Heimdahl, S. P. Miller, M. W. Whalen, "Model-Based Safety Analysis", 2006

8. DUREE

18 mois

9. MONTANT DE LA SOUSCRIPTION

Membres IMdR : 8 000 € HT (sur la base de 6 souscripteurs)

Non-membres IMdR : 8 000 € HT + prix de l'adhésion annuelle relative au collège souscripteur