Journée Thématique : “Validation au plus tôt des choix d’architectures Système par l’utilisation des modèles MBSE/MBSA”

Table ronde interactive : « *De quelle manière peut-on assurer la synchronisation des modèles utilisés en phase de conception (System Definition) et ceux utilisés pour les analyses de Sûreté de Fonctionnement (FMDS) ?* »

avec les représentants des CTs MBSE et SV2S/MBSA de l’AFIS, d’Airbus, de la DGA, de Nexter Systems et de l’IRT St Exupéry

Plan

- Présentation du sujet
- Présentation des participants
- Règles de déroulement
- Conclusion/restitution

LE SUJET

Introduction du sujet

❑ Rationnel (Enjeux ?)

- ➢ Avoir les modèles SA (Safety Analysis/Assessment) au début de la modélisation des architectures permet de faire une validation des choix d'Architecture au plus tôt.
- ➢ Partager les données communes aux deux types de modèles MBSE/MBSA permet de gagner en efficacité et en coût.

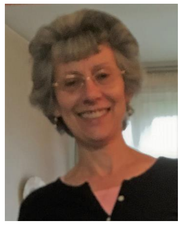
❑ Sujet (Méthode ?)

- ➢ De quelle manière peut-on assurer la synchronisation et la cohérence des modèles utilisés en phase de conception (System Definition) et ceux utilisés pour les analyses de Sûreté de Fonctionnement (FMDS) ?

LES PARTICIPANTS, LES RÈGLES

Présentation des participants

❑ Facilitation, Animation



- ➢ Lalitha Abhaya (CT MBSE, Airbus DS) anime la table ronde
- ➢ Avec le support de :
  - ✓ Anne Sigogne (Mission JTs AFIS) surveille le bon « timing »
  - ✓ Fabien Bouffaron (Airbus DS) pour prendre les notes et la restitution

❑ Débat

- ➢ Rémi Boutemy (CT MBSE, Nexter Systems)
- ➢ Tony Hutinet (CT SV2S/MBSA & MBSE, CIMPA)
- ➢ Estelle Saez (IRT Saint Exupéry, Liebherr)
- ➢ Cédric Morin (Nexter)
- ➢ Christophe Frazza (DGA TA)
- ➢ Jean-Luc Marty (Airbus DS)

Règles de déroulement

- **Tour de table pour se présenter : 1 min/participant**
  - Nom
  - Entreprise et fonction (une description court des activités)
  - Implication dans les travaux AFIS/INCOSE

- Chaque participant exprime **sa vision : 2 min/participant**

7

Noter : A n'importe quel moment l'assistance peut intervenir pour poser des questions/donner sa vision : **5 min**/pour une intervention au cours de débat

Rémi BOUTEMY

Vision CT MBSE - Co-organisateur de la JT

Présentation Rémi Boutemy

- Rémy est le Responsable du pôle MBSE chez NEXTER,
  - Expert en modélisation système au sein de la direction de l'ingénierie système de NEXTER.
  - Responsable des activités de modélisation système mises en place sur nos produits et de leur déploiement dans les équipes d'ingénierie système de NEXTER.
- Il est Co-leader du CT MBSE à l'AFIS et Co animateur du GT Méta modèle IS.
- Il participe à ce table ronde pour :
  - Apporter son RETEX côté MBSE sur la réutilisation de modèle système dans les analyses Safety
  - Connaitre les initiatives des autres industriels et académiques ainsi que les éventuelles difficultés rencontrées

Tony HUTINET

Vision MBSA (CT SV2S) - Co-organisateur de la JT

Présentation Tony Hutinet

- Tony, Manager du Centre de Compétences en Ingénierie Système de la société CIMPA (Groupe SOPRA-STERIA) possède une double expertise :
  - Expert en Evaluation des Architectures Système dans le cadre des études SSA (System Safety Assessment) tant dans le domaine Aéronautique (ARP 4754A-4761) qu'automobile (ISO26262 / SOTIF). Il a été en charge entre autre du développement de l'Atelier de Sûreté de Fonctionnement CECILIA OCAS de Dassault Aviation autour du Langage AltaRica.
  - Expert en PLM Systems (intégration des process d'ingénierie Système au sein du PLM) en autre au sein de la 3DX Platform (Dassault Systèmes).
- En tant que Co-Leader du CT SV2S, Tony apporte sa vision sur la « Validation au plus tôt des Choix d'Architectures Système par l'utilisation des modèles MBSE/MBSA » et de l'importance de mettre en avant le Design to X (X=Safey) lors des phases de Trade-Off Analysis en tenant compte du point de vue de la Discipline Métier Safety.
- Dans le cadre de la Digital Continuity, Tony précisera les différentes voies possibles pour assure la continuité des données partagées par l'ensemble des disciplines concernées et les moyens de contrôle pour évaluer les propositions d'évolutions des architectures Système (Traceability, Impact Analysis, …).

Estelle SAEZ

Ingénieure de Recherche Safety - IRT Saint Exupéry

Présentation Estelle SAEZ

- Elle est détachée de Liebherr Aerospace au sein de l'IRT Saint Exupéry : chez Liebherr elle est Ingénieure Safety et à l'IRT Ingénieur de recherche Safety.
- Pour l'IRT Saint Exupéry Estelle a participé au projet MOISE (2015-2019) en tant que responsable du lot d'activité MBSE/MBSA. Elle est actuellement Ingénieur de recherche sur le projet S2C où elle est responsable du lot Méthodologie MBSA.
- Elle participe à cette table ronde pour partager l'expérience du projet MOISE sur le sujet et pour représenter le projet S2C qui démarre en collaboration avec l'IRT SystemX.

Christophe Frazza

Expert modélisation dysfonctionnelle (MBSA) - DGA

Présentation Christophe Frazza

- Il est Expert en modélisation dysfonctionnelle (MBSA)
- Ses activités sont :
  - Mise en place, application et évolution d'une méthodologie outillée pour réaliser des analyses de sécurité de systèmes basées sur les modèles ; domaines d'application variés (aéronautique, spatial, contrôle aérien, naval, terrestre, missile, installation d'essai...).
  - Réalisation de formations (interne DGA, écoles d'ingénieur, au profit des industriels)
- Il participe à cette table ronde dans le but de Disséminer les bonnes pratiques (industriels et académiques).
- Pour Christophe, c'est une problématique importante (notamment dans le cadre d'une certification aéronautique) : maintenir l'indépendance entre le Design et la Safety (d'où la nécessité d'avoir des modèles différents et d'où le besoin de les maintenir en cohérence, plus que de les synchroniser).

Jean-Luc MARTY

Airbus DS

Présentation Jean-Luc Marty

- Jean-Luc est un Ingénieur Système pour des systèmes satellites
  - Il est en charge de synthèse technique du projet DDMS@Sps-de dont l'objectif est de fournir les nouveaux moyens (méthodes & outils) pour la conception de satellites soutenu par un environnement digital
  - Il a effectué les PMT (processus, méthode et outils) définition et le déploiement pour les systèmes sol (de systèmes satellites).
- Depuis 10 ans, il travaille sur l'utilisation des connaissances en Ingénierie Système pour réaliser un diagnostic précis pour la détection et l'analyse des défaillances (FDIR).
- Dans l'objectif de réduire les coûts d'exploitation et d'augmenter la disponibilité du système, il est nécessaire d'avoir une connaissance sur les défaillances du système qui pourrait être obtenu par l'analyse *de Sûreté de Fonctionnement (FMDS)*. Il est donc nécessaire que le modèle FMDS soit cohérant avec la définition fonctionnelle et le Design du système.
- Jean-Luc participe à ce table ronde pour contribuer à trouver une solution pour assurer cette cohérence

Mathieu COLLUMEAU

NEXTER Systems

Présentation Mathieu Collumeau

- Mathieu est architecte système dans le domaine de l'artillerie terrestre
  - En charge de la spécification et de la validation d'un véhicule complet
  - Egalement responsable de la cohérence des outils et méthodes IS sur un des sites Nexter
- Il participe à la table ronde en tant qu'utilisateur d'un outil passerelle entre les mondes MBSE et MBSA
- Il est intéressé par la thématique de cette journée de travail notamment pour l'aspect ingénierie simultanée

Questions pour (re)lancer les débats

- Quels sont les modèles SE/SA ?
- Quels sont les éléments communs pour ces deux types de modèles ? Comment connecter la modélisation Système et la modélisation pour la Safety ? Ne peut-on pas s'appuyer sur cette base pour connecter la Security ?
- Est-ce que l'on peut générer automatiquement le modèle dysfonctionnel à partir d'un modèle fonctionnel ? Si non pourquoi ? Pourquoi ne peut-on pas utiliser les techniques de transformation de modèles pour cela ?
- Pensez-vous que l'on puisse générer automatiquement les Analyses FTA ou FMECA à partir de modèles de design ?
- Pour une modélisation, un langage est-il nécessaire ? et la modélisation d'un système complexe ne peut pas être simple (sinon impossible d'adresser la complexité sans perdre les informations), donc besoin de structurer, gérer, documenter,…
  - Quelles sont les langages les mieux adaptés ?
  - Comment gérer les versions et les configurations des modèles SE et SA tout au long de cycle de vie d'un système ?
- Quelles sont les bonnes approches/méthodes ?
- On utilise des AF dans la phase d'Architecture. Y-a-t-il des Frameworks « spécifique SA »
- Quelles sont les outils (chaines d'outils) les mieux adaptés actuellement (continuité numérique) ?

Table Ronde

Synthèse / Conclusions

Synthèse Table Ronde (1/5)

- La question posé est : **De quelle manière peut-on assurer la synchronisation et la cohérence des modèles utilisés en phase de conception (System Définition) et ceux utilisés pour les analyses de Sûreté de Fonctionnement (FMDS) ?**
- Participants ont contribué par leur Expertise MBSE, MBSA et Retour Expérience dans différents domaines (avec une intervention très active de la salle)
- Différentes approches sont proposées pour un besoin commun **: Mise en cohérence des modèles MBSE / MBSA**
- Point de vue CT MBSE & CT SV2/MBSA (suite aux groupes de Travail & Workshop EMEA INCOSE 2015 IVTV - MBSA)
  - Pour certains, on doit avoir un seul modèle en privilégiant le « Co-design » : Aligner les modèles MBSE/ MBSA 100% Conformes avec le modèle fonctionnel, intégration des mécanismes dysfonctionnels (propagation des pannes) au sein du modèle fonctionnel (Rhapsody, Simulink, Scade, …).
    - ✓Le point de vue Safety n'étant que l'un des points de vue devant être agrégé au sein du modèle Système (System Definition) pour entre-autre faire du Trade-Off Analysis.

Synthèse Table Ronde (2/5)

- Pour d'autres, on devrait avoir deux types de modèles distincts mis en cohérence pour tenir compte des différents contextes (niveaux d'abstraction différents) et des objectifs de validation spécifiques : Certification (Modèles séparés) / Beaucoup d'itérations (Besoins de lier les points de vues) / Besoins Différents (Safety, Coût, Maintenance, …).

➢ **Pour la synchronisation mise en cohérence des modèles MBSE/MBSA**

- ✓Pour **le secteur de l'Aéronautique** : pas de synchronisation dynamique des modèles mais une mise en cohérence lors des **Jalon de maturité** ….)
- ✓De plus tenir compte de l'Evolution du marché : On vend dorénavant plus un produit seul mais des services, à savoir un produit avec les contrats MCO et le critère (KPI) de tenue du contrat est la Disponibilité Opérationnel (des pénalités sont définies si la disponibilité opérationnelle prévue n'est pas atteinte en condition opérationnelle)
- ✓Il faut donc aussi intégrer les aspects soutiens au modèles (Diagnostic, Maintenance, ..).

❑ *Evolution (Raffinement) des modèles MBSE / MBSA (Pourquoi, Contenu) selon les différentes phases de conception : Design / Vérification / Validation*

Synthèse Table Ronde (3/5)

- **<u>Modèle Commun MBSE / MBSA est en général Structurel (FBS & PBS) et défini en phase de Design et portant respectivement le point de vue fonctionnel et dysfonctionnel</u>**
- Safety est l'une des Conditions que l'installation doit supporter.
- Définition des besoins Safety dès les premières phases de conception du Système
- Du fait de l'évolution des Systèmes, l'évaluation de la Safety à l'aide de Modèles Statiques (FTA) est limitée voire impossible, il nous faut avoir recours à des modèles fonctionnels dynamiques (pour traduire entre-autres les dynamiques de reconfiguration sur défauts / ….)
- ➔ Concepts partagés communs : Exigences / Uses Cases / Scénarios / Fonctions
  (le point de vue Safety Raffine le modèles MBSE en tenant compte des mécanismes dysfonctionnels)
- <u>Le Représentant EDF indique qu'EDF n'a pas les mêmes besoins pour le MBSA (plus axés Sûreté avec une composant Nucléaire) ;</u>
  - La Vérification doit être indépendante ➔ et les Modèles utilisés sont souvent éloignés de la conception / Plutôt basé sur l'environnement (séisme, causes externes comme crash avion) / Modèles d'autres natures ….

Synthèse Table Ronde (4/5)

- **Mise en cohérence des différents Modèles MBSE / MBSA)**
  - **Analyse / Vérification/ Assesment (Validation)**
- Point de vue DGA / IRT / Airbus (Mises en œuvre)
  - Les équipes Safety et équipes Design sont différentes
    - ✓ Différents points de vues et abstractions entre MBSE / MBSA
    - ✓ Deux métiers différents avec différents PM&T, Modèle MBSA (avec propagation des fautes) : Permet de limiter les efforts pour la Safety (capitalisation des connaissances dysfonctionnelles au sein de bibliothèques) :

      A partir des Modèles MBSA, génération automatiques de modèles d'évaluation Safety : AMDEC, Arbre

      (Ex. Dassault Aviation a évalué 28 variantes du système de Commandes de Vols électriques du Falcon 7X en 2 mois (CECILIA OCAS - AltaRica) et a utilisé ces bibliothèques pour les autres versions de la gammes Falcon.
- **Justification :**
  - Requis dans les cas de certification : Lors des phases de design préliminaire, il est compliqué d'avoir la coexistence des 2 modèles (Abstraction, Niveau de granularité, choix d'architecture non encore défini de manière précise)
  - Par la suite lors des phases de raffinement, les Modèles ont de plus en plus la même structure, ce qui facilite la mise en cohérence.

Synthèse Table Ronde (5/5)

❑ Proposition :

- ➢ Premier squelette : Pour l'initialisation du modèle MBSA (pouvant s'appuyer sur le modèle structurel)
- ➢ Puis mise en cohérence du modèles MBSE en MBSA lors des phases de Raffinement
- ➢ Synchronisation MSBE / MBSA lors des Jalons de Maturité.

❑ Limites entrevues :

- ➢ Concernant la Cohérence des modèles : nécessité d'évaluer la complétitude/cohérence des modèles vis-à-vis du système réel : Erreur dans la modélisation ➔ Confiance dans le modèle (niveau de maturité)
- ➢ Pour les Jalons de Maturité, souvent des boucle longues (Maturité) ➔ Trouver une structure permettant l'information partagée + réconciliation ➔ Identifier les données (Tagguer les exigences dites sensibles)
- ➢ Description de la dynamique : Difficulté pour la Mise en cohérence des modèles / transformation
- ➢ Mise en cohérence : Attention à la duplication des objets : Deux Objets vs deux points de vues (MBSE/ MBSA), et la gestion des versions.
- ➢ Difficulté associée aux différents niveaux d'abstraction : Problèmes de réconciliation (la continuité des données nécessite qu'un même niveau d'abstraction soit partagé pour effectuer la synchroniser / la mise en cohérence au moins lors des jalons de Maturité pour une revue du Design.