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

“Présentation des objectifs du CTSV2S et du GP MBSA

-

Intégration des Analyses Safety dès les Phases Amont de Conception Système(Trade-Off Analysis) à l’aide des modèles MBSA”

Présentateur

Tony HUTINET (CIMPA),

Co-Leader du CT SV2S (Sûreté, Validation et Soutien des Systèmes)

Présentation du CT SV2S

❑ Contexte et enjeux

- Tous les systèmes complexes* actuels et futurs (Défense, Transport, Energie, Observation, Services …) sont assortis d'enjeux de sûreté, de disponibilité du service et de sécurité des utilisateurs.
- La conception de ces systèmes doit les doter de capacités de reconfiguration, de testabilité, de réparation, de prévention, de survivabilité, de résilience, etc.
- Ces capacités doivent être tenues tout au long de la vie du système.
- Ces enjeux imposent une anticipation croissante et un contrôle généralisé des risques techniques lors de la conception et lors de l'exploitation des systèmes.

** Il s'agit bien des systèmes nécessitant plusieurs disciplines et non des matériels seulement ;*

ces systèmes incluent matériels, logiciels, humains ou encore des produits, services, organisations.

Ils sont dit complexes de part l'hétérogénéité, de nombreuses composantes, des échelles différentes, des rétroactions temporelles ou entre niveaux d'échelle.

Présentation du CT SV2S

❑ Finalité du CT SV2S (Sûreté, Validation et Soutien des Systèmes)

- ➢ Promouvoir, améliorer les connaissances et compétences des acteurs sur les activités :
  - ✓de Sûreté de Fonctionnement (FMDS/RAMS),
  - ✓d'Intégration, de Vérification, de Transition, de Validation et de Qualification,
  - ✓de Maîtrise des Risques Sociotechniques,
  - ✓de Maintien en Condition Opérationnelle.

❑ Mission du CT SV2S

- ➢ Développer ou adapter l'existant en termes de concepts, principes, définitions, processus, activités, méthodes et techniques de modélisation, d'analyse, d'évaluation et de mesure associées aux processus d'ingénierie système.

Présentation du CT SV2S

❑ Domaines et thèmes ciblés

➢ Prévision et prévention des défaillances en développement

✓Obtention des propriétés et capacités de Sûreté, Disponibilité, Fiabilité, Testabilité, Maintenabilité, Survivabilité, Résilience, Sécurité, Cyber-sécurité, ...

✓Etudes de vulnérabilité des architectures

➢ Vérification & Validation

✓Etablissement des éléments de preuves de la conformité du système à l'ensemble des exigences

✓Détection et élimination des défauts de conception

➢ Emploi des systèmes

✓Surveillance/Supervision, Test, Diagnostic, Pronostic, Maintenance, etc.

✓Prévision et prévention des risques en matière de sécurité, de cyber-sécurité,

Organisation du CT SV2S

❑ Animateurs

➢Christophe Ducamp (Airbus DS), Tony Hutinet (CIMPA)

❑ Groupes de Projet

➢**GP MBSA** Animateurs : Tony Hutinet (CIMPA), Agnès Lanusse (CEA LIST)

➢**GP IVTV** Animateurs : Vincent Chapurlat (Ecole des Mines d'Ales), Jean-Louis Sennegon (Nexter)

➢**GP SLI** Animateurs : Christophe Ducamp (Airbus DS), Eric Levrat (Université de Lorraine)

❑ Groupe d'Investigation en cours

➢**GT AFIS - BNAE** autour de la Qualification

➢**GT AFIS - IMdR** autour de l'Ingénierie des Systèmes Complexes

➢**GT sur L'IVVQ** à coût et délais optimisés

➢**GT sur les Cyber-Physical Systems**

❑ Nombre de membres :

➢**52 Inscrits** (30 Sociétés, 5 Universités/Ecoles d'ingénieurs) dont **environ 20 membres contributeurs**.

Quelques Questions/Sujets abordés

❑ Harmonisation des pratiques de SdF

- ➢ La tendance croissante à comparer et à harmoniser les pratiques de différentes branches industrielles (Nucléaire, Aéronautique, Ferroviaire, Pétrochimie ...) est-elle justifiée ?
- ➢ Exemple : déclinaison de la norme CEI 61508 (Functional Safety/Safety Integrity level) dans les autres secteurs (CEI 61511, CEI 60880, CEI 61513, ISO 26262, EN 50128, ….)

❑ Evaluation multidisciplinaire de la Sûreté

- ➢ MBDA (Model-Based Dependability Assessment) : Analyse dysfonctionnelle dirigée par les modèles dans une approche collaborative multidisciplinaire et couvrant l'ensemble du cycle de vie du système.
- ➢ Exemple : Peut-on et doit-on justifier certains compromis sur l'architecture de contrôle-commande pour mieux prendre en compte les contraintes imposées par les facteurs humains ?

❑ Extension de la prise en compte de la sûreté et de la résilience aux systèmes sociotechniques et organisationnels

- ➢ Maîtrise des risques fournisseurs, des propriétés émergentes, des incertitudes, de la décision opérationnelle, etc.

.

Quelques Questions/sujets abordés

❑ Utilisation des COTS (Components Off The Shelf) et contraintes de SdF

- ➢Certains systèmes s'appuient sur des composants qui n'ont pas été conçus pour de très hauts niveaux de sûreté de fonctionnement. Comment les évaluer de façon efficace (avec ou sans coopération des fournisseurs) ?
- ➢Quel niveau de vérification doit être obtenu pour l'intégration d'un COTS dans un système ?
- ➢Comment utiliser des produits "incertains" pour néanmoins obtenir un ensemble sûr ? Comment prévoir leur remplacement lorsqu'ils ne seront plus disponibles ?

❑ Confiance dans la sûreté et son coût d'obtention

- ➢Quelle stratégie ou quel compromis entre les différentes approches et techniques de vérification, validation à utiliser (test, simulation, vérification formelle, etc.) pour la meilleure confiance à moindre coût ?
- ➢Comment optimiser les opérations de vérification en production série en relation avec les process d'obtention ?
- ➢Comment assurer le maintien de la validation de la définition d'un système, lors d'évolutions des process de production série ?

Quelques Questions/sujets abordés

❑ Maintenabilité et Maintenance

- ➢Stratégie de conception simultanée du système principal (opérant) et de son système de soutien
- ➢Quelle stratégie de validation des performances du système soutenu ?

❑ La maintenance du futur

- ➢La maintenance préventive et curative (à conception constante dans un environnement d'exploitation spécifié),
- ➢La maintenance évolutive (évolution de la conception pour prendre en compte les modifications de l'environnement d'exploitation ou réglementaire, dues à de nouveaux besoins, à l'obsolescence des composants, à l'évolution de l'organisation assurant la maintenance).
- ➢La maintenance « On Condition », la maintenance prédictive

Focus sur le GP MBSA (Model-Based Safety Analysis/Assessment

"Working Groups AFIS/INCOSE & Groupes d'Investigation

WG4 commun CT MBSE & SV2S/GP MBSA « La Simulation de Modèles comme moyen de V&V »

- **1ère Phase : « Simulation de Modélisation Fonctionnelle au plus tôt »** :
  - L'objectif du WG4 est d'explorer les différentes techniques de simulation pour **valider au plus tôt les exigences fonctionnelles et le comportement « haut niveau » du système** dans son environnement opérationnel.
  - Dans un premier temps, **revue des mises en œuvre** au sein des sociétés suivantes : Airbus DS, CIL4Sys, Dassault Systèmes, Nexter Systems, Safran AE, Thales.
  - Le CT SV2S investigue les sujets suivants :
    - **Modélisation et Simulation du CONOPS** (CONcepts OPérationnelS),
    - **Modélisation et la Simulation Dysfonctionnelle pour le Trade-Off Analysis** Evaluation des Variantes d'Architectures dans le cadre des études SSA (System Safety Assessment) dans le cadre des ARP-4754A/4761(A) et de la DO178C.

WG6 commun CT MBSE & SV2/GP MBSA
Méta-Modèles IS & échanges de Modèles

- Lancement prévu en septembre 2019 dans le prolongement du WG 3 Méta Modèles en Ingénierie Système (livrable prévu en Sepetembre).
- Elargir le Meta-model V1, défini au sein du WG3 couvrant les processus techniques IS aux autres spécialités d'IS (Safety Analysis, Sécurité, Maintenance, …)
- Propositions de CS
  - Comparaison Méta-modèle IS (WG3) avec méta-modèles du marché
    - ✓Dans la suite du WG3, confronter le méta-modèle défini avec les méta-modèles des ateliers du marché (par exemple UPDM, SysML, Arcadia), UAF et NAF
  - Passage de méta-modèle à un autre
    - ✓Dans un objectif d'échange de modèles entre partenaires ne disposant pas forcément des mêmes solutions de modélisation, proposition d'un projet visant à étudier la problématique de passage d'un méta-modèle à un autre (notion de Bridge),
- Pilotes: Lalitha Abhaya (Airbus DS), Rémi Boutemy (Nexter Group).

Candidatures pour participation toujours ouvertes !
=> ctmbse@afis.fr

WG7 commun CT MBSE & SV2/GP MBSA
Jumeau Numérique (Hybride)

- Par « Jumeau Numérique », il faut ici comprendre « Jumeau Numérique en phase opérationnelle ».

  Le sujet est au cœur de l'actualité dans de nombreuses entreprises industrielles. Qu'elles produisent des installations uniques ou des objets en série, la capacité à rejouer avec un Double Digital (Digital Twin) des situations « vécues » par l'objet réel trouve de nombreuses applications à forte valeur ajoutée.

- La question qu'il est proposé d'ouvrir : « le MBSE, un incontournable pour développer simultanément un produit et son jumeau numérique ? »

- Démarche proposée :
  - Préparation d'un cadre d'interviews
  - Réalisation d'interviews chez des membres de l'AFIS engagés dans cette démarche.
  - Synthèse « état de l'art ».
  - Perspectives apportées par le MBSE et le MBSA (Jumeau Numérique Hybride).

- Pilotes : Philippe Gicquel (Cil4Sys), Tony Hutinet (CIMPA)

Candidatures pour participation toujours ouvertes!
=> ctmbse@afis.fr

Axes d'investigation du CT SV2S

❑ Groupe de Travail commun AFIS-GIFAS (Commission GIFAS R&D IS & SdF)

➢ 2 thématiques portées pour le GT SV2S et le GT MBSE :

- Prise en Compte **des aspects non-Fonctionnels du système** tout au long de son cycle de vie en tenant compte des systèmes de soutien (MCO, KPI : Disponibilité Opérationnelle).
- **Virtualisation & Continuité interdisciplinaire de la représentation numérique du SOI** dans un environnement collaboratif (statique et dynamique) sur l'ensemble du cycle de vie.

❑ Contributions du CT SV2S à la Vision AFIS 2030+

➢ **Jumeau Numérique Hybride** : intégration des modèles de simulation (dont les modèles de dérives) et tenant compte des systèmes de soutien sur l'ensemble du cycle de vie. Virtualisation Hybride intégrant les simulations prédictives de la vie du SOI (Vieillissement, Défaillance, Obsolescence, …) et les systèmes de monitoring et de soutien (HUMS/Health Monitoring, Predictive Maintenance, …).

➢ **Design to Value** (intégrant l'ensemble des contraintes durant les phases du cycle de vie : System Design, Manufacturing & Support. Les entreprises sont désormais guidées vers le « **Design to values** » et doivent optimiser le cycle de vie de leurs produits.

➢ **Cyber-Physical Systems** (IoT/IoS, Cybersécurité, IA Algorithms)

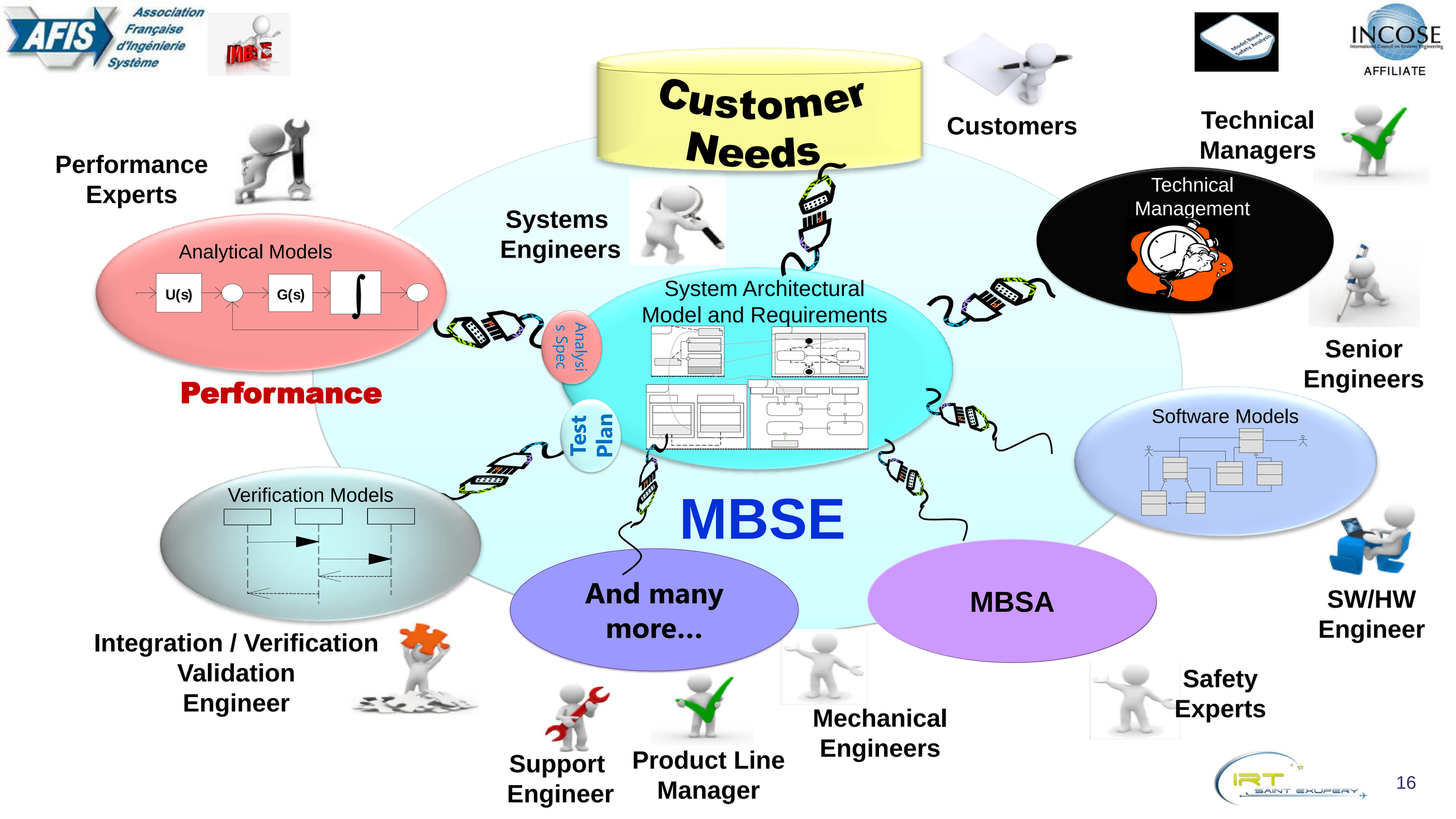
Questions?

Pour intégrer le CT SV2S ou pour toutes informations:

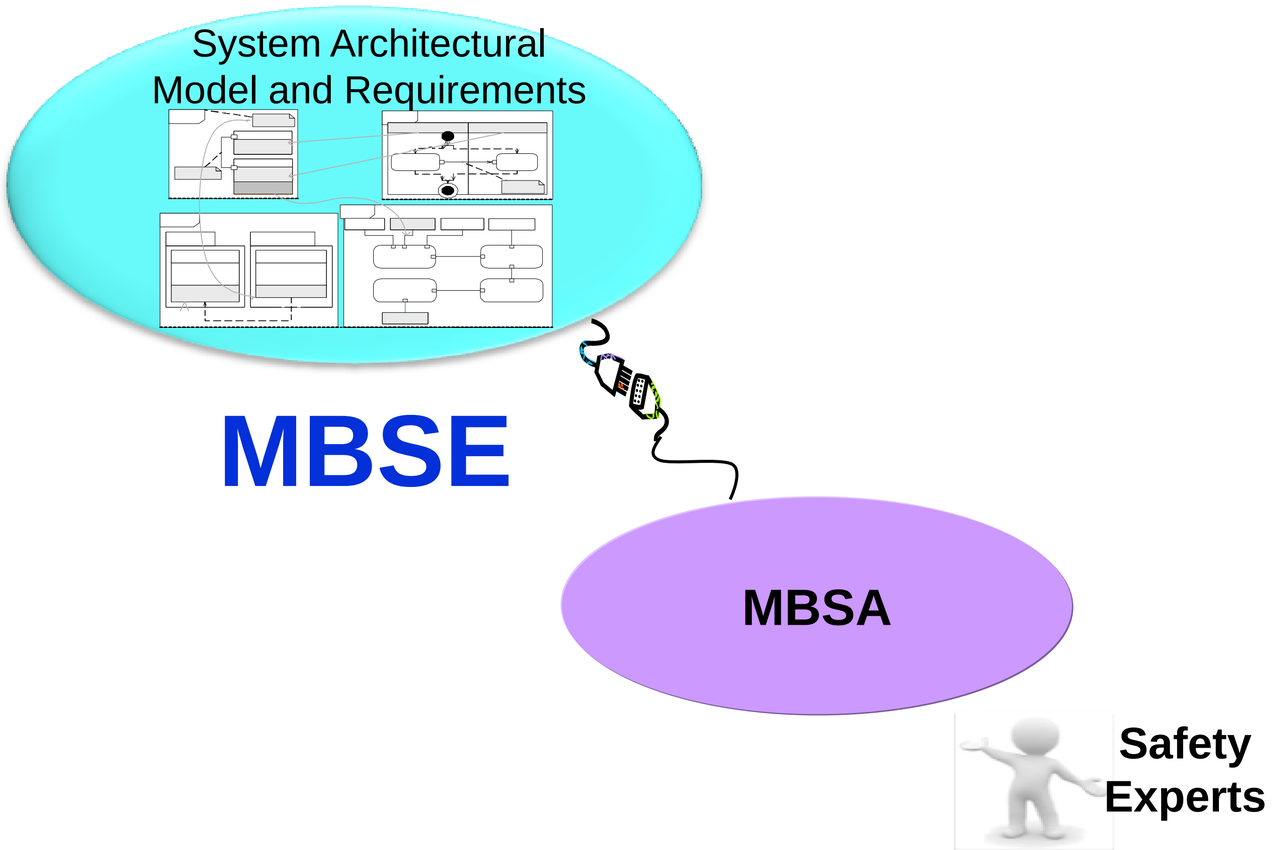
ctsv2s@afis.fr

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

“Intégration des Analyses Safety dès les Phases Amont de Conception Système (Trade-Off Analysis) à l’aide des modèles MBSA”


Customer Needs
Customers
Technical Managers
Performance Experts
Systems Engineers
Technical Management
Analytical Models
U(s)
G(s)
Senior Engineers
System Architectural Model and Requirements
Analysis Spec
Test Plan
Performance
Software Models
MBSE
Verification Models
And many more...
MBSA
SW/HW Engineer
Integration / Verification Validation Engineer
Safety Experts
Support Engineer
Product Line Manager
Mechanical Engineers

Introduction à la JT MBSE MBSA



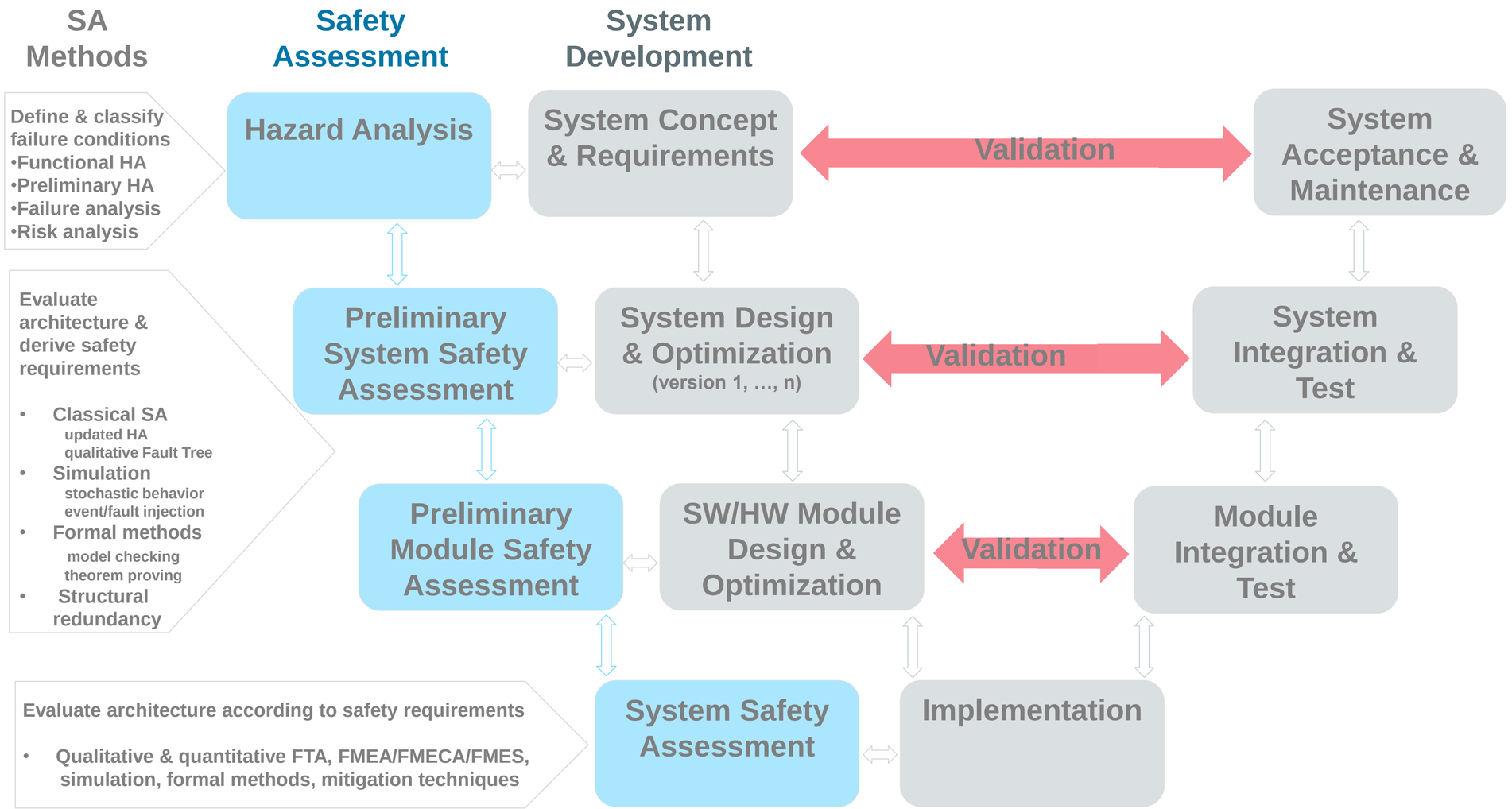
- Synchronisation des modèles système et des Analyses Safety au plus tôt ?
- Trade-off système prenant en compte les critères Safety ?
- Comment réutiliser les modèles système (fonctionnels) dans l'élaboration des modélisation Safety ?
- Quels sont les Langages, Méthodes et Outils utilisés actuellement et à venir ?

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

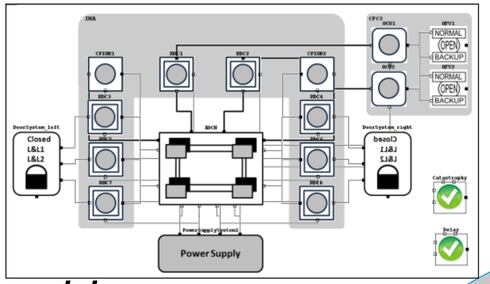
“Intégration des Analyses Safety dès les Phases Amont de Conception Système (Trade-Off Analysis) à l’aide des modèles MBSA”

Safety Assessment integrated development flow

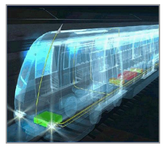
Parallel V-cycle

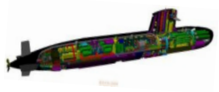


Model Based Safety Assessment for System Design



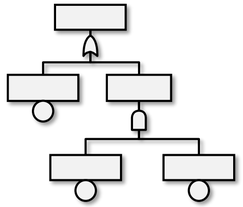
Safety model construction using library of reusable components





1. System Modeling

2. Safety Analysis

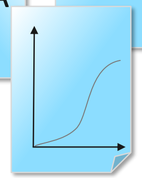


Fault Tree Generation

FMEA

MCS

CCA



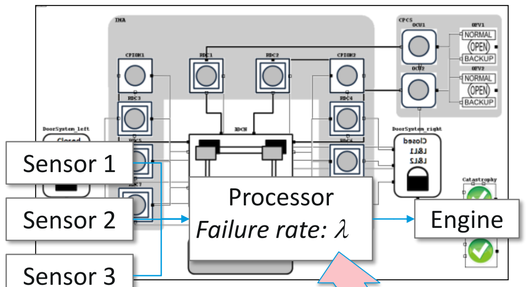
Processing the model and generating the results

3. Analyze results

Review

OK!

Safety Engineering



4. Update the system and safety model

Sensor 1
Sensor 2
Sensor 3
Processor
Failure rate: λ
Engine

Model Based Safety Assessment - Values

- **Allows to study more candidate architectures of the system**
  - The Automation of System Safety Analysis allows to perform more studies and more simulations on various candidate system architectures in order to select the “best one” vs Safety/Reliability requirements (Trade-off Analysis, Traceability from Safety Requirements to Safety Analysis Results)
- **Improves collaboration between designers and safety engineers**
  - MBSA provides a unique functional & dysfunctional view of the system from formal models that allows to perform Safety Analysis (Dysfunctional Simulation, Fault Tree Analysis, MCS, FMEA, MMEL, CCA, PRA, …) in the early phases of the system development
- **Standardization and capitalization**
  - MBSA allows to create reusable libraries of equipment/component that provide standardization, accelerate validation times and reduce the product costs. Standard component libraries can be shared by program suppliers
- **Openness**
  - The System modeling language used for Formal System model has to offer high capability of integration with the other System Engineering applications dedicated System Analysis

Model Based Safety Assessment rationales

- **Goals:**
  - Propose formal failure propagation models closer to design models
  - Develop tools to
    - Assist System model construction
    - Analyze automatically complex models
  - For various purposes
    - FTA, FMEA, Common Cause Analysis, Human Error Analysis, …

      since the earlier phases of the system development
- **2 possible approaches:**

Extend design models
(Scade Simulink, Modelica, SysML, AADL...)
with failure modes

↓

Transform into analyzable formalisms
(Boolean formulae, automata, ...)

Build dedicated failure
propagation models
(AltaRica, Figaro, Slim...)

↓

Develop specialized
Safety Analysis tools