Journée Thématique “Validation des architectures de Système via les modèles MBSE-MBSA”

“Le projet S2C : *System & Safety Continuity – Continuité Numérique entre la définition des systèmes et les analyses safety*”

http://afis.community/jt-afis-validation-architectures-systeme-par-utilisation-des-modeles-mbse-mbsa/

Présentateurs

Patrick Farail responsable projet S2C, Anouk Dubois coordinateur S2C System X, Estelle SAEZ Spécialiste Safety

Le 19/06/2019

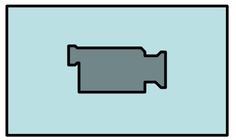
CONTINUITÉ NUMÉRIQUE ENTRE LA DÉFINITION DES SYSTÈMES ET LES ANALYSES SAFETY

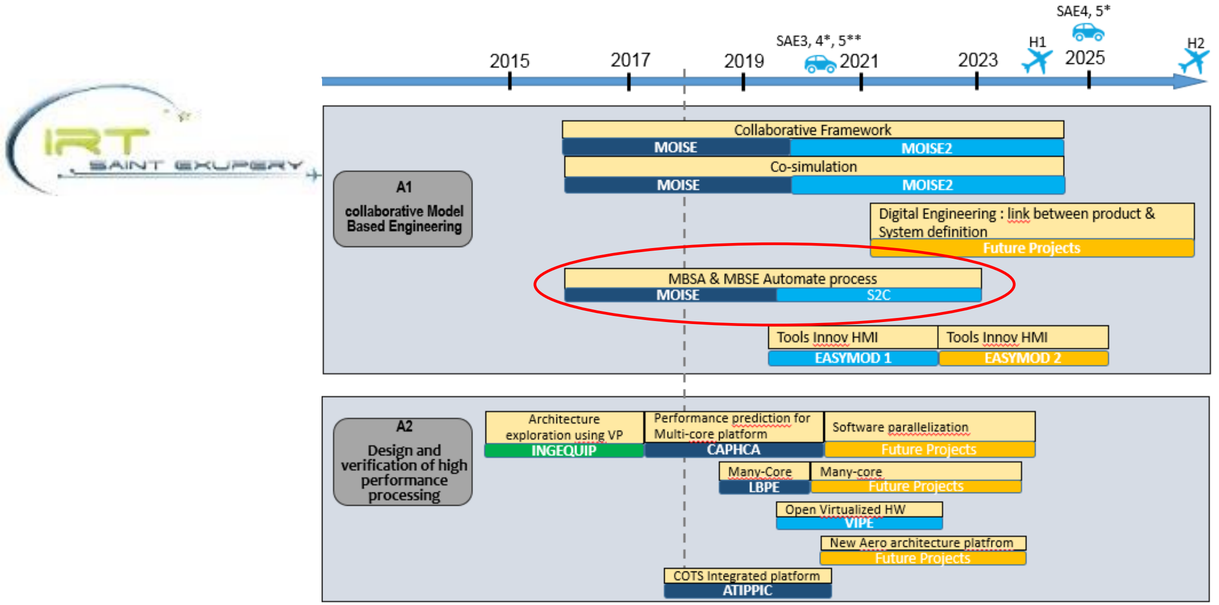
S2C : « SYSTEM AND SAFETY CONTINUITY »

Un projet qui s'inscrit dans la continuité de…

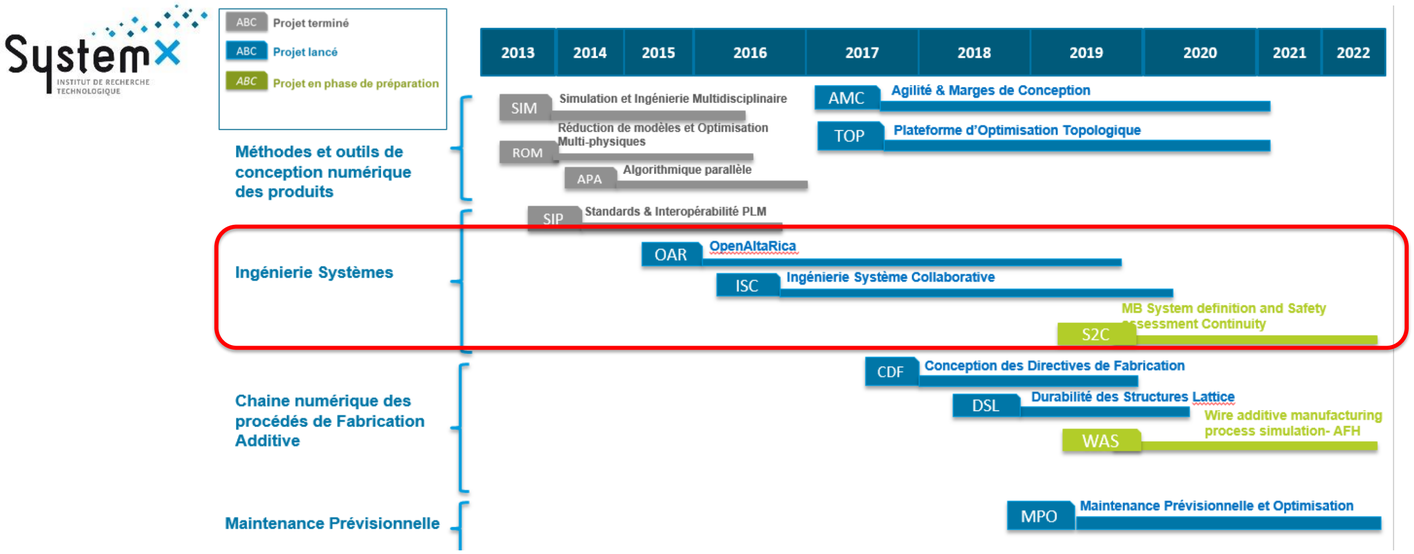
- du projet MOISE côté Saint Exupéry

Venez découvrir le projet MOISE (Lien sur la chaîne Youtube de l'IRT Saint Exupéry) :





- des projets ISC « Ingénierie Système Collaborative des Système Complexes » et OAR « OpenAltarica » côté SystemX



Projet S2C - Model Based system definition and safety assessment continuity

Le 1er projet de collaboration en Ingénierie des Systèmes entre l'IRT Saint Exupéry de Toulouse et l'IRT SystemX de Palaiseau

Ecosystème pour l'instant très centré aéronautique civile mais souhait SystemX d'élargir à d'autres filières

ENJEUX

- Mieux gérer la complexité des systèmes
- Réduire le nombre d'itération de développement, limiter les risques de re-design, et réduire les coûts et délais de développement en conséquence
- Améliorer la confiance dans les analyses safety
- Contribuer à la promotion du MBSA au sein de l'écosystème aéro notamment
- Mieux répondre aux exigences des organismes de certification

Développement de nouveaux process de co-ingénierie Système/Safety en entreprise étendue en contexte d'ingénierie système basée sur les modèles

Organisation inter IRTs

S2C

Un même projet collaboratif

Un Accord de collaboration IRTs-DGA-TA

Des accords projets par IRT

THALES
(Corporate)

DASSAULT AVIATION

ALL4TEC

supméca

SystemX
INSTITUT DE RECHERCHE TECHNOLOGIQUE

DGA

IRT SAINT EXUPERY

Des accords projets par IRT

SAMARES ENGINEERING
Accelerate Systems Design

SAFRAN
(Tech, HE, LS, AS)

THALES
(AVS)

AIRBUS DEFENCE & SPACE

LIEBHERR

APSYS
ICONIC PLACES

LGM

LAAS CNRS

ONERA
THE FRENCH AEROSPACE LAB

IRIT

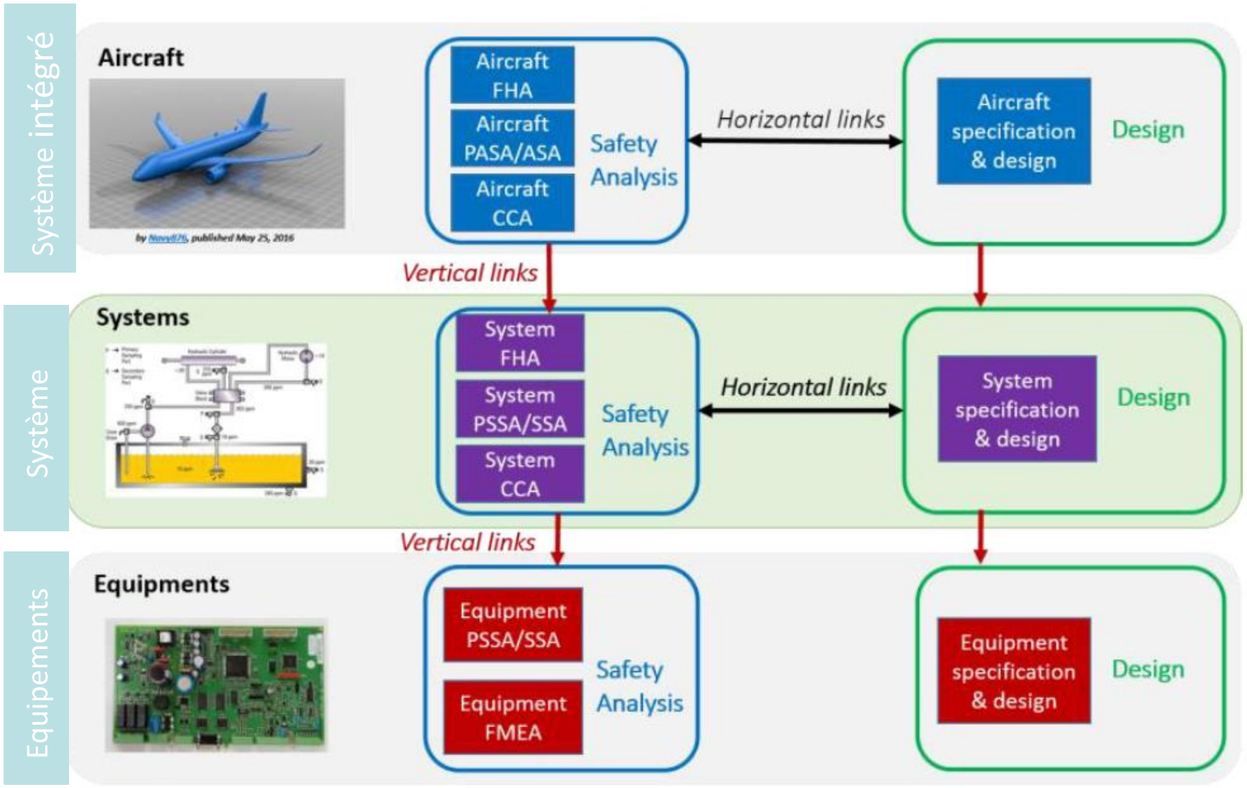
1er Avril Démarrage du projet

Fin projet 31/03/2023

2019	2020	2021	2022	2023

Objectifs du projet

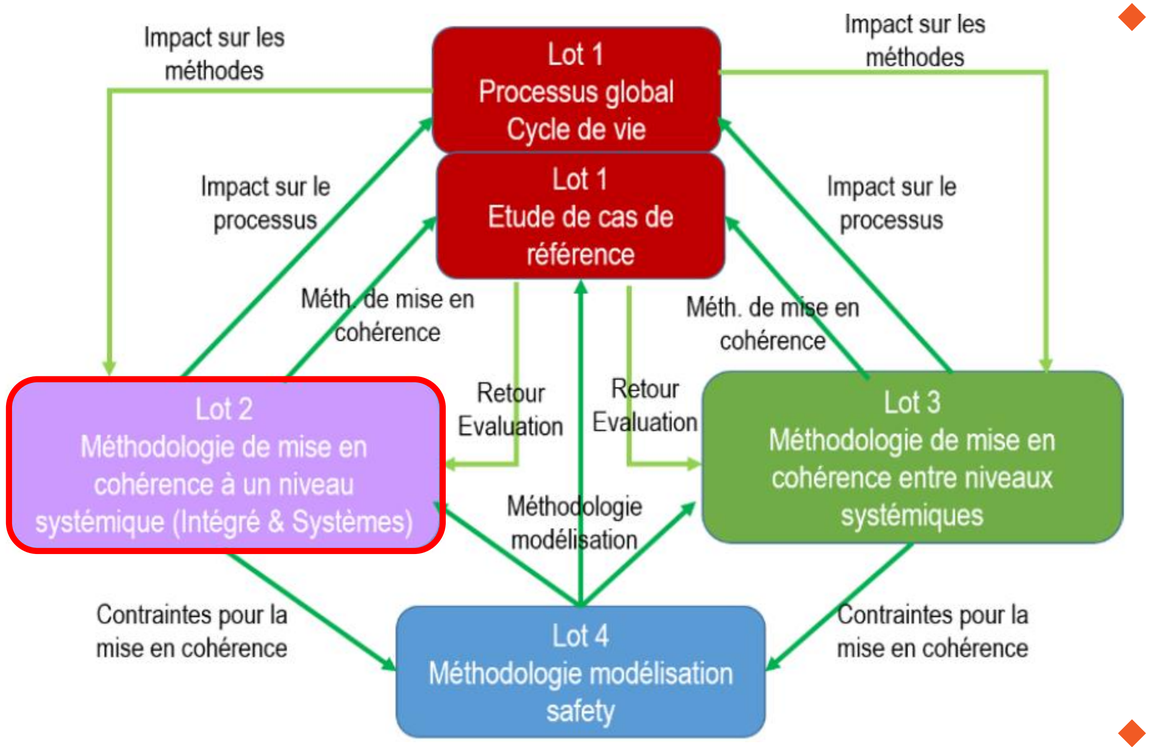
Définir les **processus, méthodes et outils** permettant de garantir la **cohérence** entre les **analyses safety** et la modélisation du système par l'architecte système (**MBSE**), dans un contexte de continuité numérique, **tout au long des cycles itératifs de développement** des produits et systèmes, et en répondant aux **contraintes de certification**



Principaux résultats attendus :

- Mise en cohérence entre modèles système/safety au niveau système intégré et système (liens horizontaux).
- Mise en cohérence entre les différents niveaux systémiques safety (liens verticaux).
- La traçabilité et la mise en forme des informations en vue de la constitution du dossier de certification
- Les moyens de diffusion et de maîtrise des méthodes de modélisation MBSA, notamment en vue de la synchronisation système/safety.

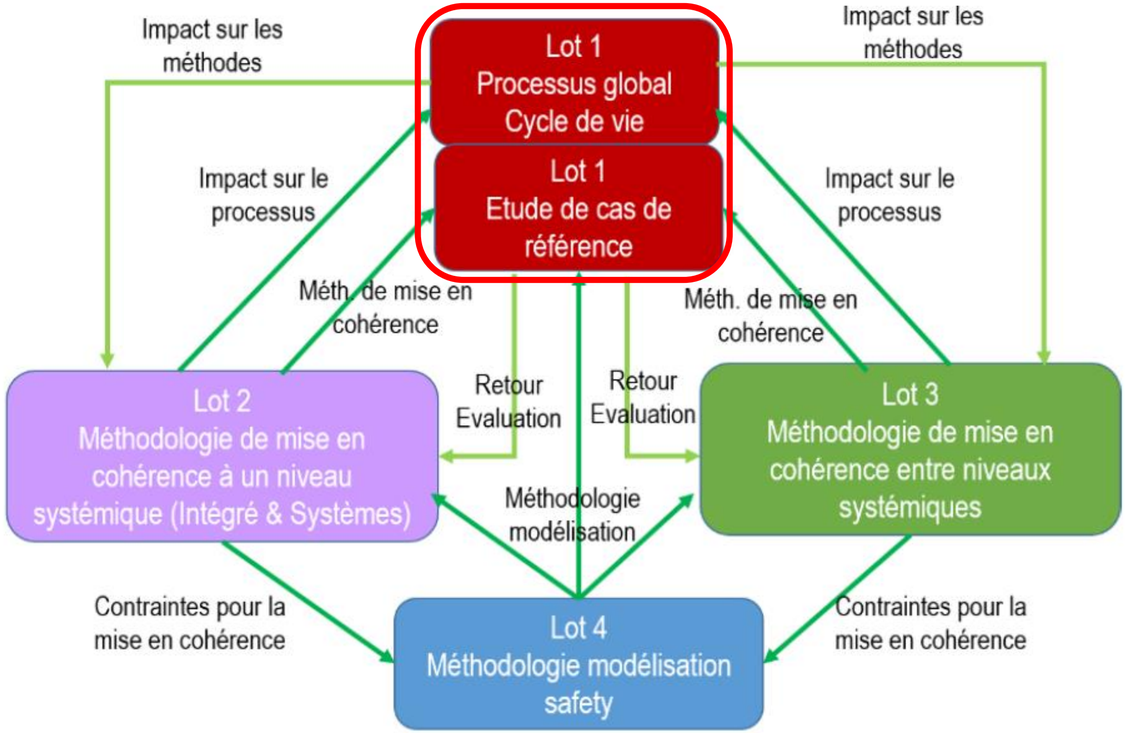
4 Lots d'activité / 2 thèses



- **Thèse Airbus D&S avec l'ONERA, l'IRIT ou LAAS CNRS**
  - **Approche multi-modèle pour l'optimisation des architectures systèmes en vue du diagnostic en opérations.** Mise en place d'une approche méthodologique permettant de caractériser l'optimisation d'une solution d'architecture système à partir de l'interopérabilité de méta-modèles définis par l MBSE- MBSA (orienté maintenabilité)- MBO (Model Based Operation).

- **Thèse SystemX avec SupMeca**
  - Contribution à la mise et au maintien en cohérence sémantique, structurelle et comportementale des modèles multi-niveau systèmes (MBSE) et sûreté de fonctionnement (MBSA) établis en vue d'un choix d'architecture, en s'appuyant sur **la théorie mathématique des catégories**

Définition d'un processus global

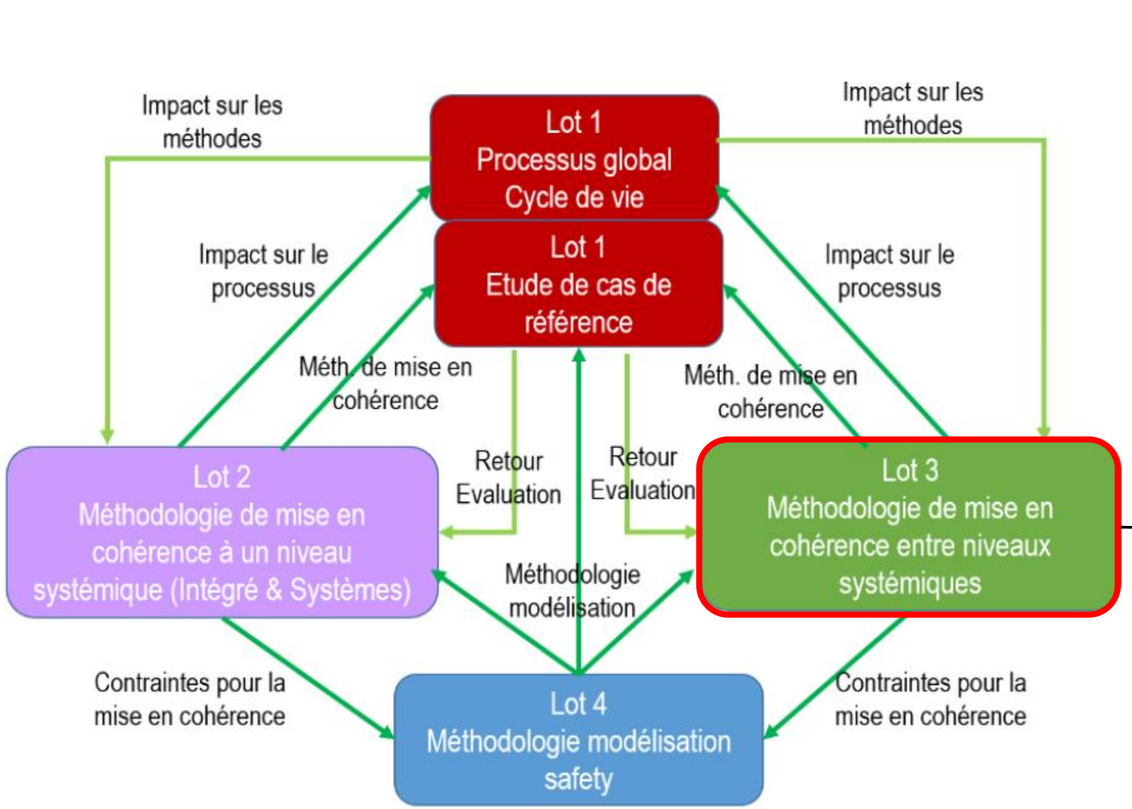


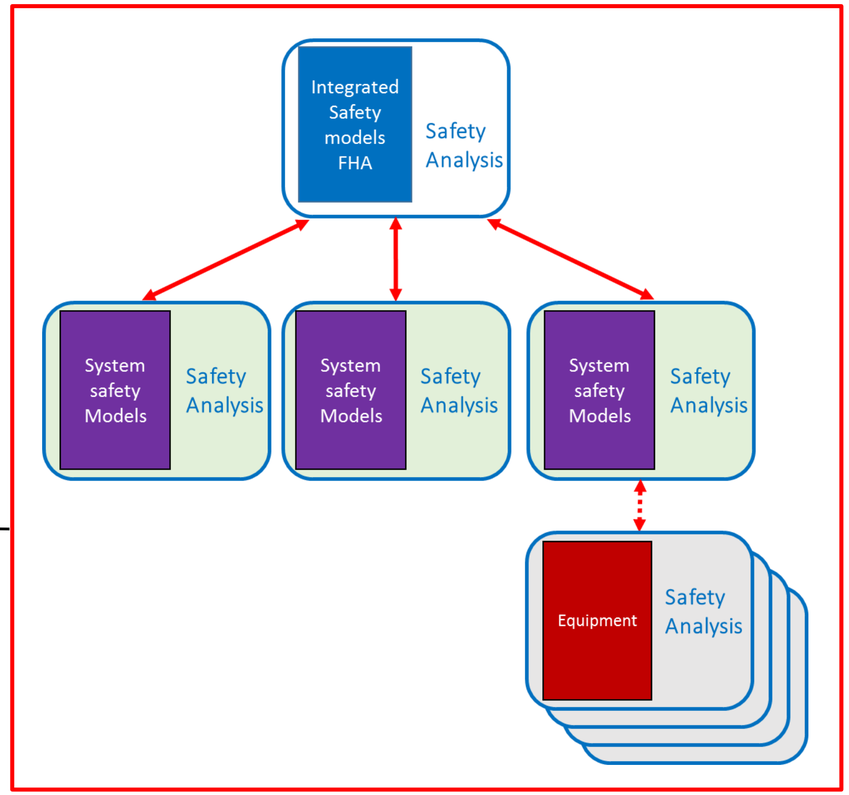
Objectifs et verrous :

- Proposer une méthodologie qui sera adaptée aux contraintes règlementaires
- Méthodologie générique pour maintenir et garantir la cohérence dans le temps des modèles à tous les niveaux
- Méthodologie pour assurer la traçabilité des objets

Nécessité de maintenir la cohérence entre les solutions de mise en cohérence SE/SA et SA/SA ainsi qu'avec la méthode de modélisation

Mise en cohérence entre niveaux systémiques

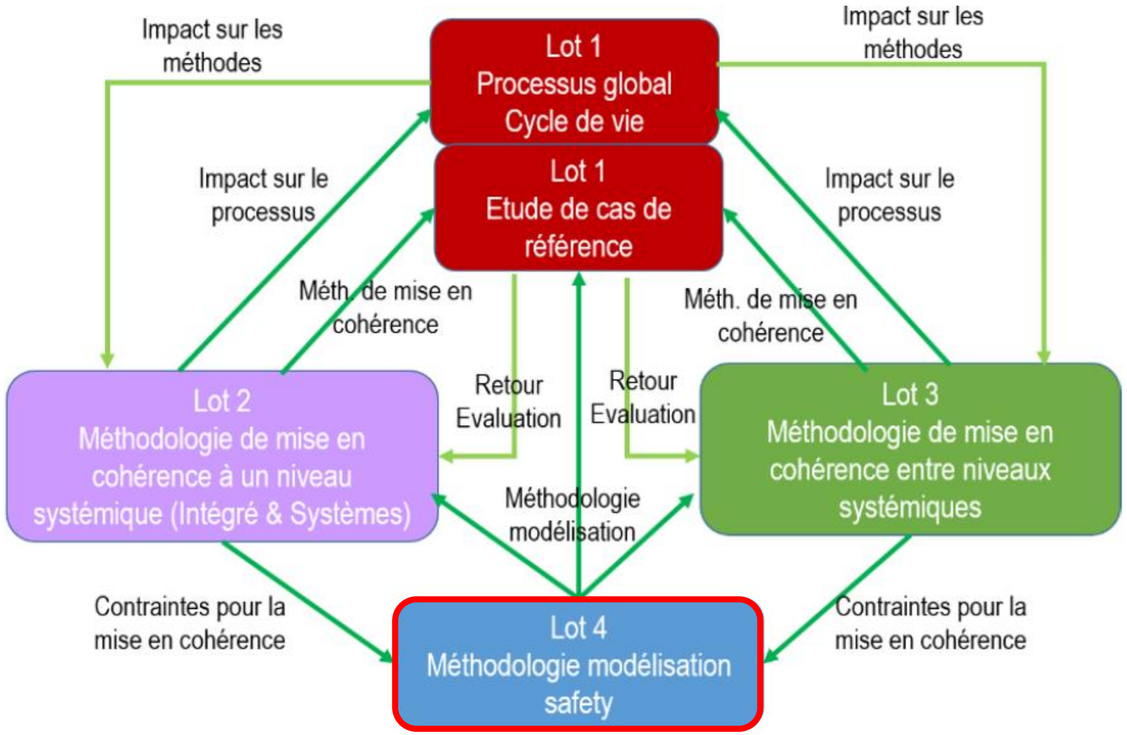




Objectifs et verrous :

- Prise en compte les contraintes issues des processus réels déployés dans les entreprises
- Conciliation de la différence des niveaux d'abstraction et de détails des modèles et analyses SA
- Conciliation de la différence de maturité au cours du temps entre les différents systèmes
- Intégration de modèles FTA et de modèles MBSA

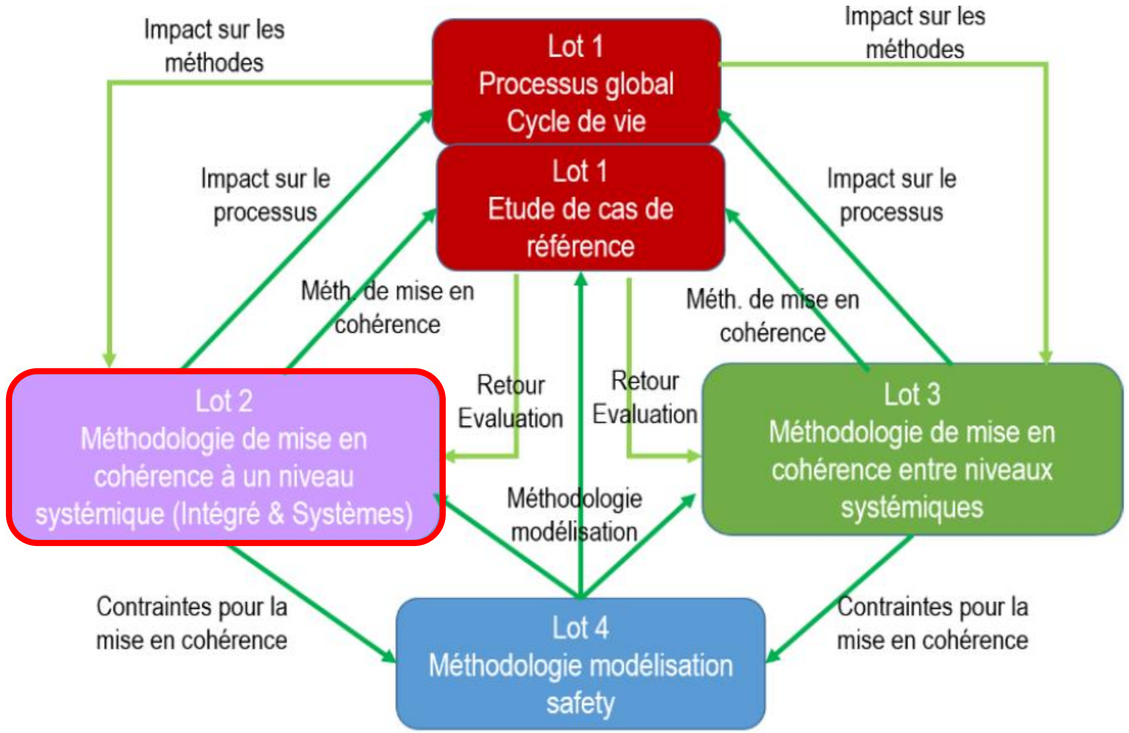
Mise en cohérence entre niveaux systémiques



Objectifs et verrous

- Définition d'une méthodologie partagée
- Diffusion auprès de la communauté des spécialistes safety
- Evaluation et démonstration de l'intérêt industriel

Cohérence entre la définition du système et les analyses safety



Objectifs

- Faciliter la communication entre SE et SA, la validation des analyses safety
- Aider à la mise en cohérence et au maintien de la cohérence des modèles MBSE et MBSA
- Faciliter la traçabilité et la capitalisation des informations échangées

Verrous

- Différence sémantique entre des artefacts système et safety due aux disparités entre concepts métiers, entre formalismes, et entre logiques les soutenant.

- Différence structurelle des éléments se trouvant dans des structurations hétérogènes

Cohérence entre la définition du système et les analyses safety

Approche proposée

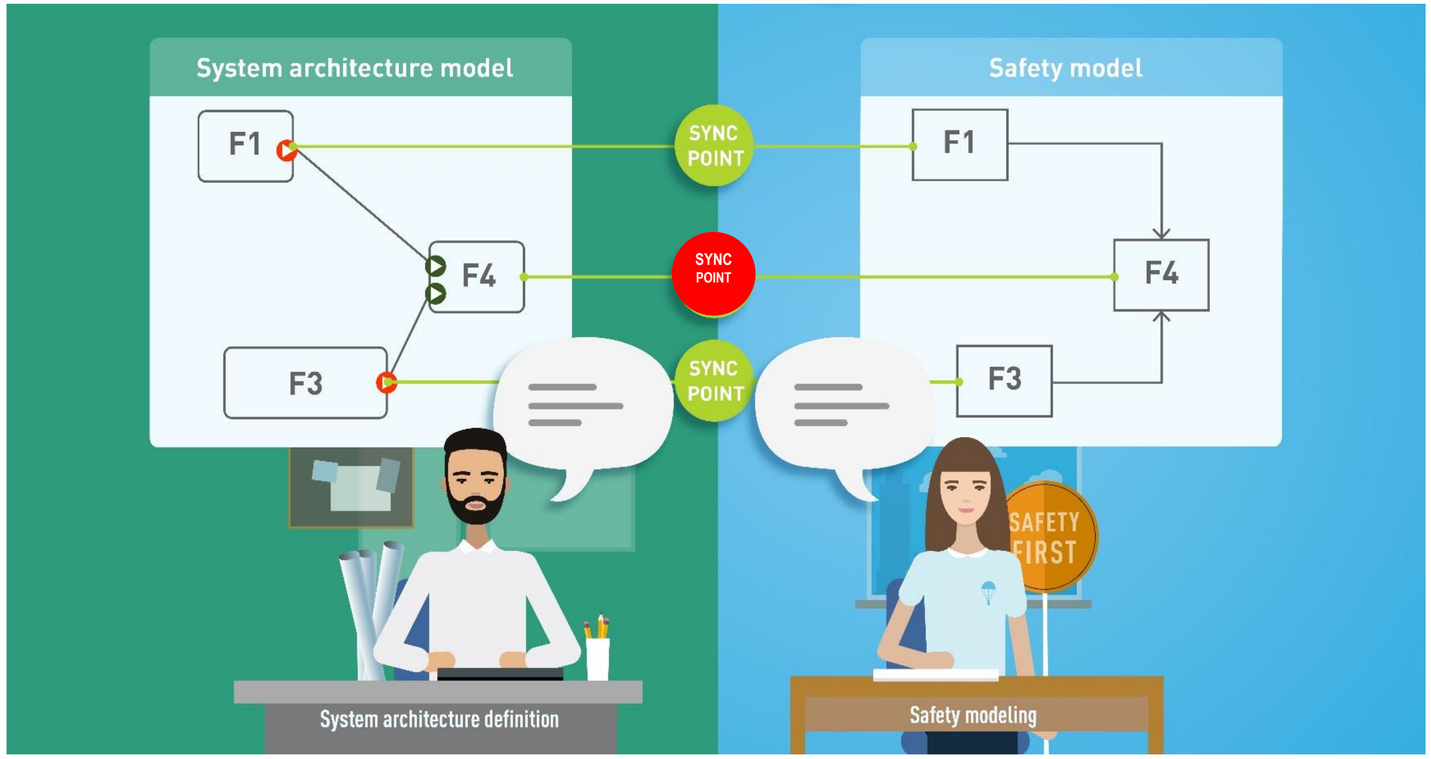
- Approche basée sur les modèles:
  - ✓Modèles MBSE pour la description des systèmes
  - ✓Modèles MBSA (au sens de l'ARP4761A) et Fault Tree pour la safety

- Choix de modèles distincts pour le MBSE et MBSA, en réponse aux besoins:
  - ✓ D'indépendance entre la conception et la validation (système critique)
  - ✓ De flexibilité pour travailler à des rythmes différents
  - ✓ De lisibilité et de gestion d'un modèle d'architecture commun
  - ✓ De flexibilité d'expression et d'appropriation dans les modèles safety :
    - Expression de chemin de propagation à des niveaux de granularité différents de ceux proposés dans la description système
    - Représentation d'éléments non présents dans la description du système (exemple : détails de systèmes externes)

  - ✓ Le projet propose des méthodes et des POC, il est donc important de pouvoir se baser sur des outils de modélisation performants.

Cohérence entre la définition du système et les analyses safety

- On bénéficie de la méthodologies définie dans le projet MOISE (Model and Information Sharing in Extended Enterprise) de l'IRT Saint-Exupéry : **introduction du concept de points de cohérence**
  - ✓ pour l'enrichir et l'améliorer
  - ✓ pour aider à définir les besoins lorsque de nouvelles pistes seront explorées



Les points de cohérence

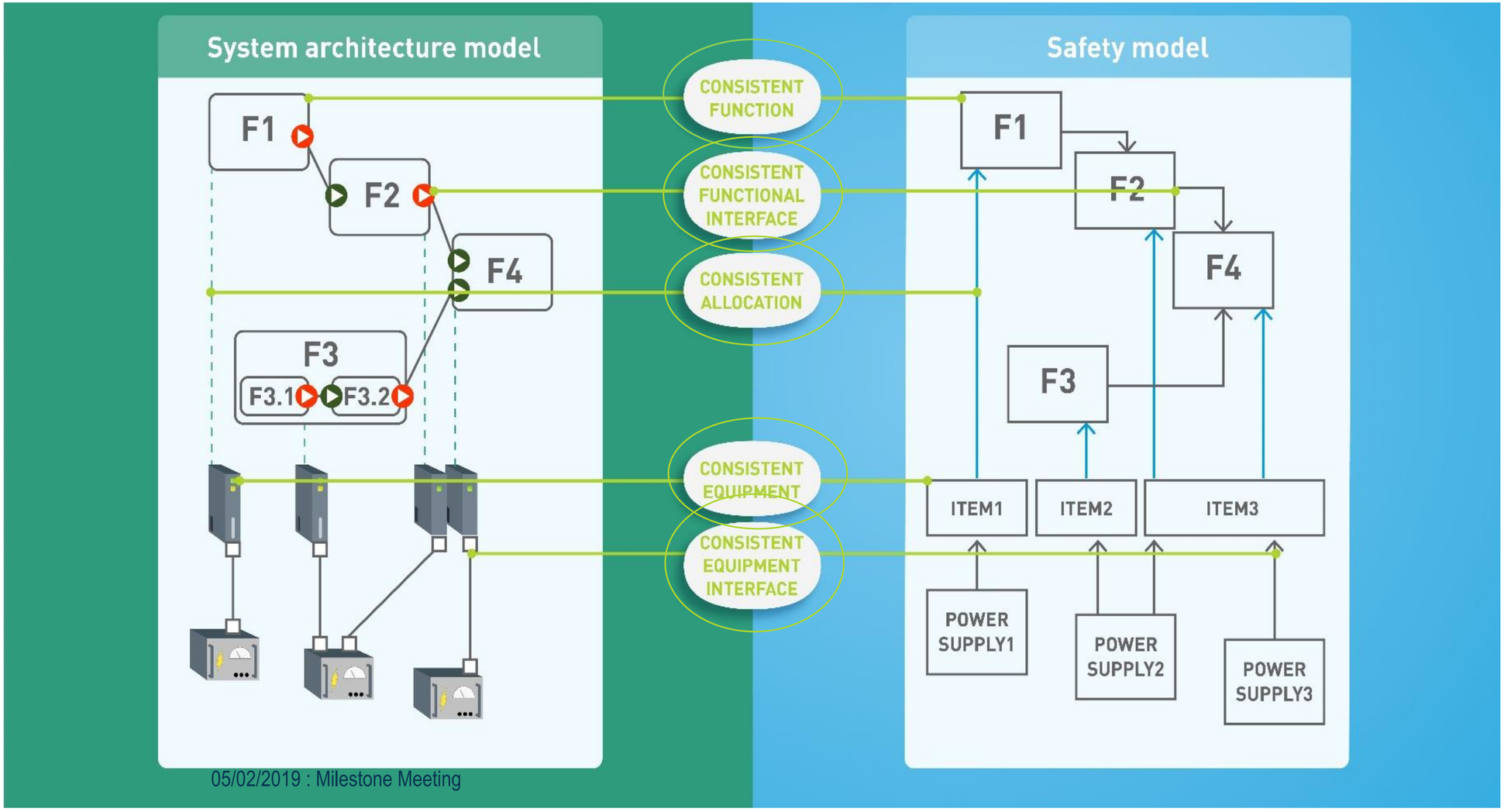
- Support de revue du modèle dysfonctionnel

- Formalisation des échanges dans le temps
- Traçabilité
- Suivi en version

- Suivi des changements dans le temps pour optimiser la revue

=> Revue « outillée »

Les points de cohérence définis dans le projet MOISE

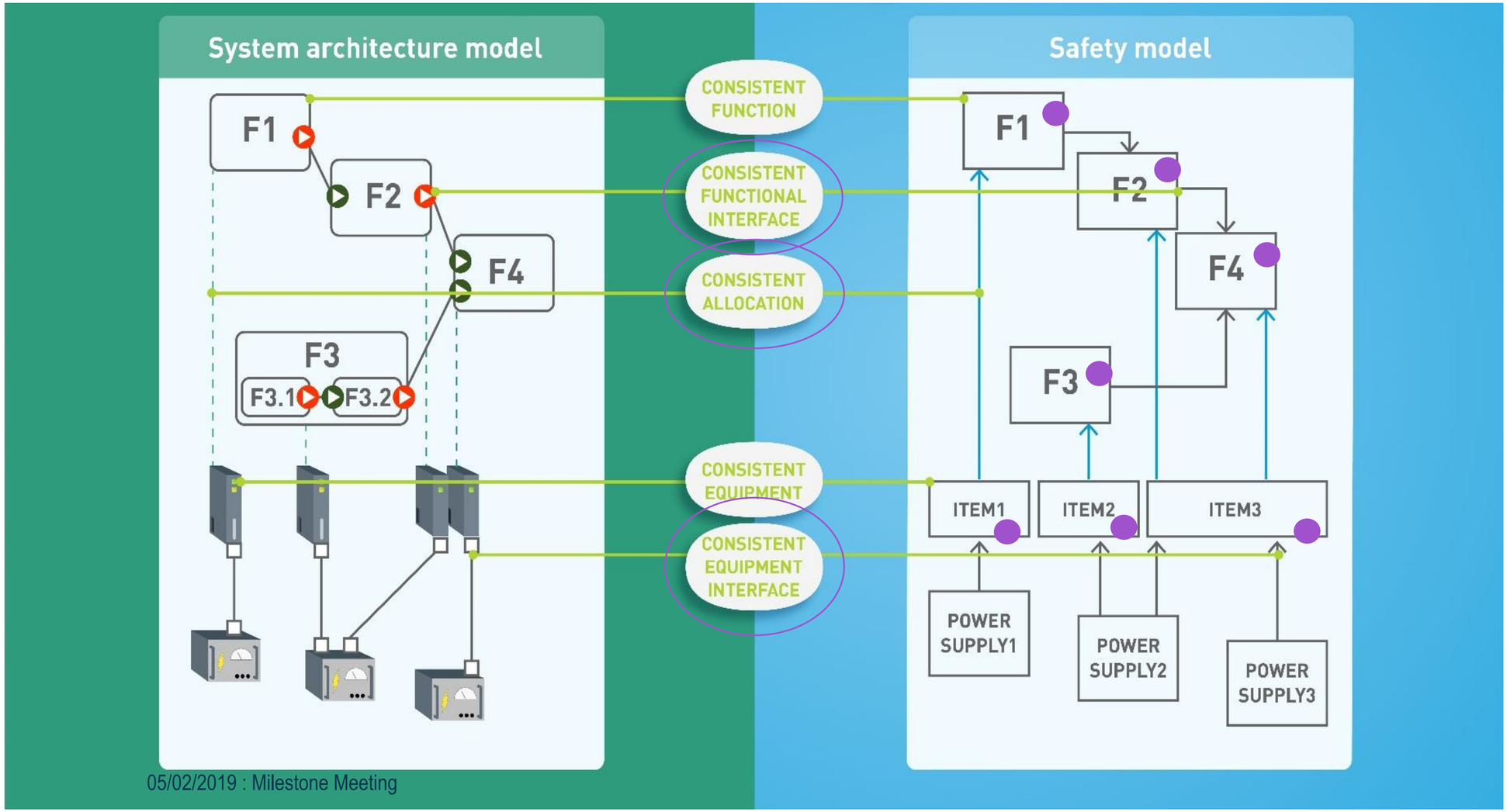


Les objets
mis en cohérence

- Fonctions
- Eléments Physiques
- Les flux
- Les Allocations

Traitement
de la hiérarchie
et de la complexité

Les points de cohérence définis dans le projet MOISE

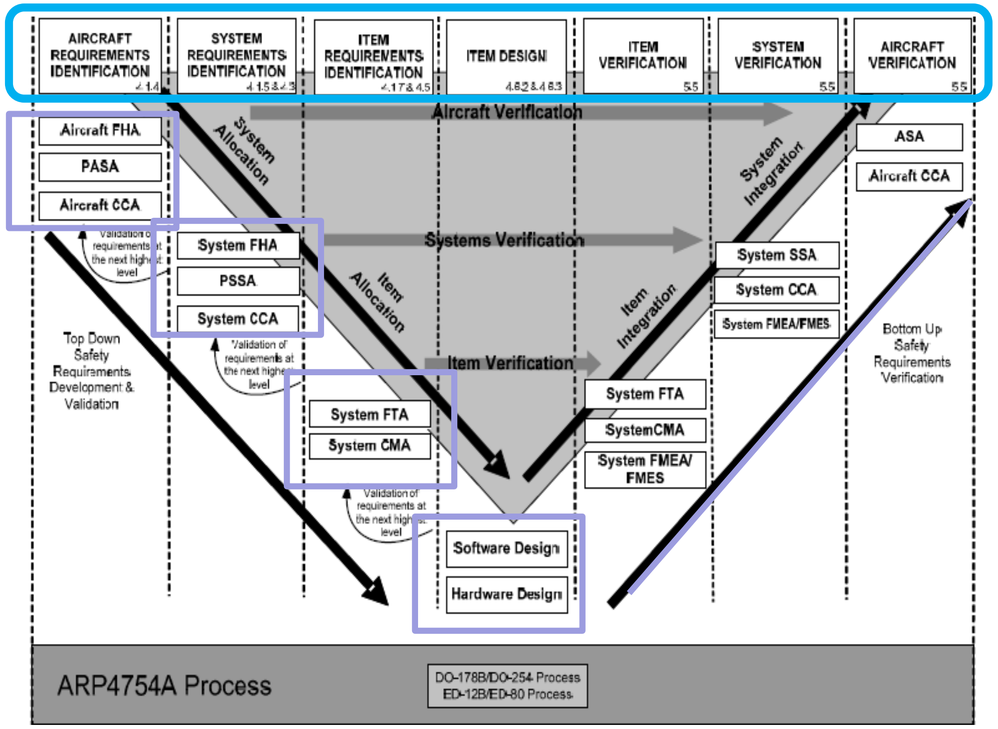


Traitement du Comportement partiel

Supporté par les points de cohérence

Cohérence entre la définition du système et les analyses safety

Le processus global en vue de la certification : lien MBSE/MBSA



Le projet S2C a pour objectif de répondre aux besoins des industriels en proposant des méthodes compatibles avec leur processus de certifications

Dans le monde aéronautique :

- Centré sur les exigences
- Besoin de gérer les évolution dans le temps: traçabilité et suivi configuration

Les exigences seront traitées indépendamment de leur format : textuel ou dans les modèles

Conclusion

Conclusion

- S2C a pour objectif d'assurer et de maintenir la cohérence entre SE et SA, tout en s'inscrivant dans un processus global, tout au long du développement

- Le projet reste ouvert aux nouveaux membres : rejoignez-nous!

- S2C est un projet ouvert sur l'extérieur et axé sur la communication:
  - ✓ Workshops, publications, etc.
  - ✓ Restons en contact !

Questions?

Contact:

estelle.saez@irt-saintexupery.com

anouk.dubois@irt-systemx.fr

patrick.farail@irt-saintexupery.com