Rapprocher Ingénierie système et sûreté de fonctionnement

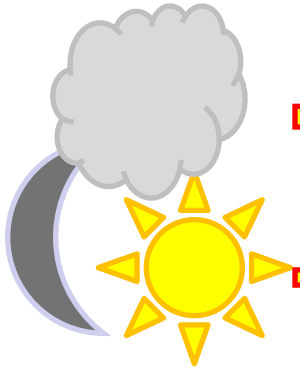
V. IDASIAK, F. KRATZ

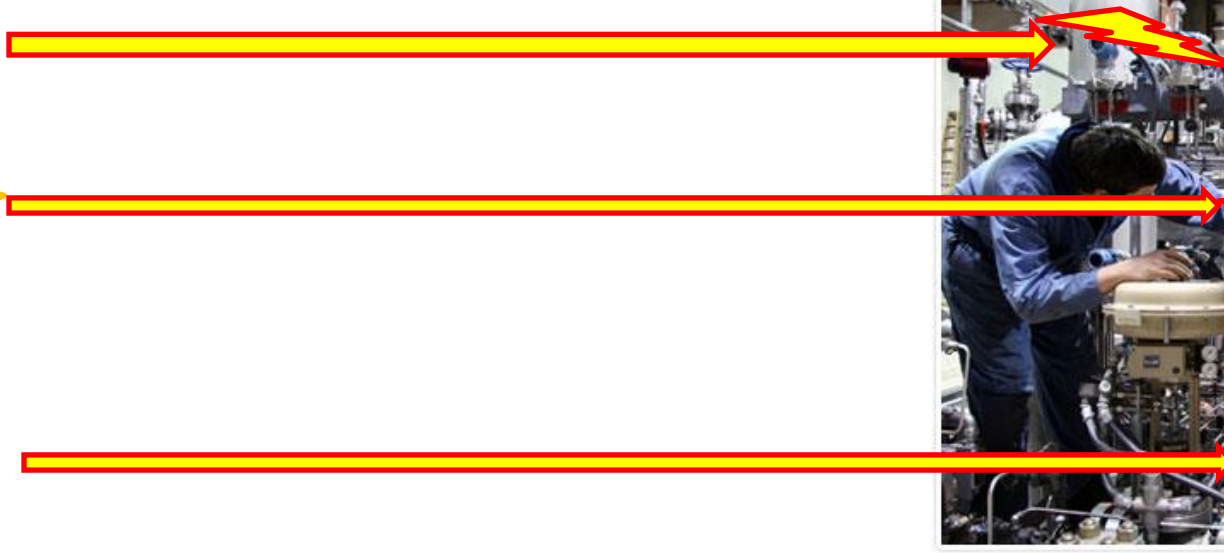
$$ISS_u = \min_{\Delta t} \int_{IS_y(t;t+\Delta t)} SdF$$

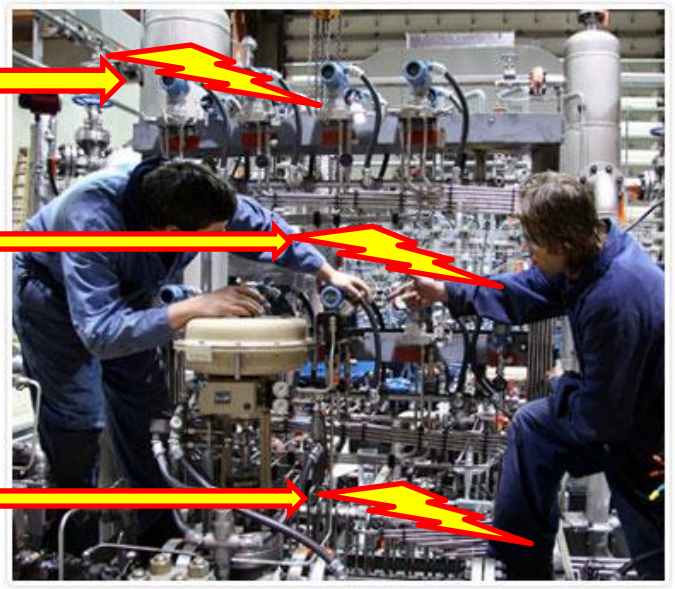
Plan

- Notre problématique
- De l’Ingénierie Système à la S.D.F
- MéDISIS
- Retour d’expérience / projet LEA- Dispatmo
- Conclusion

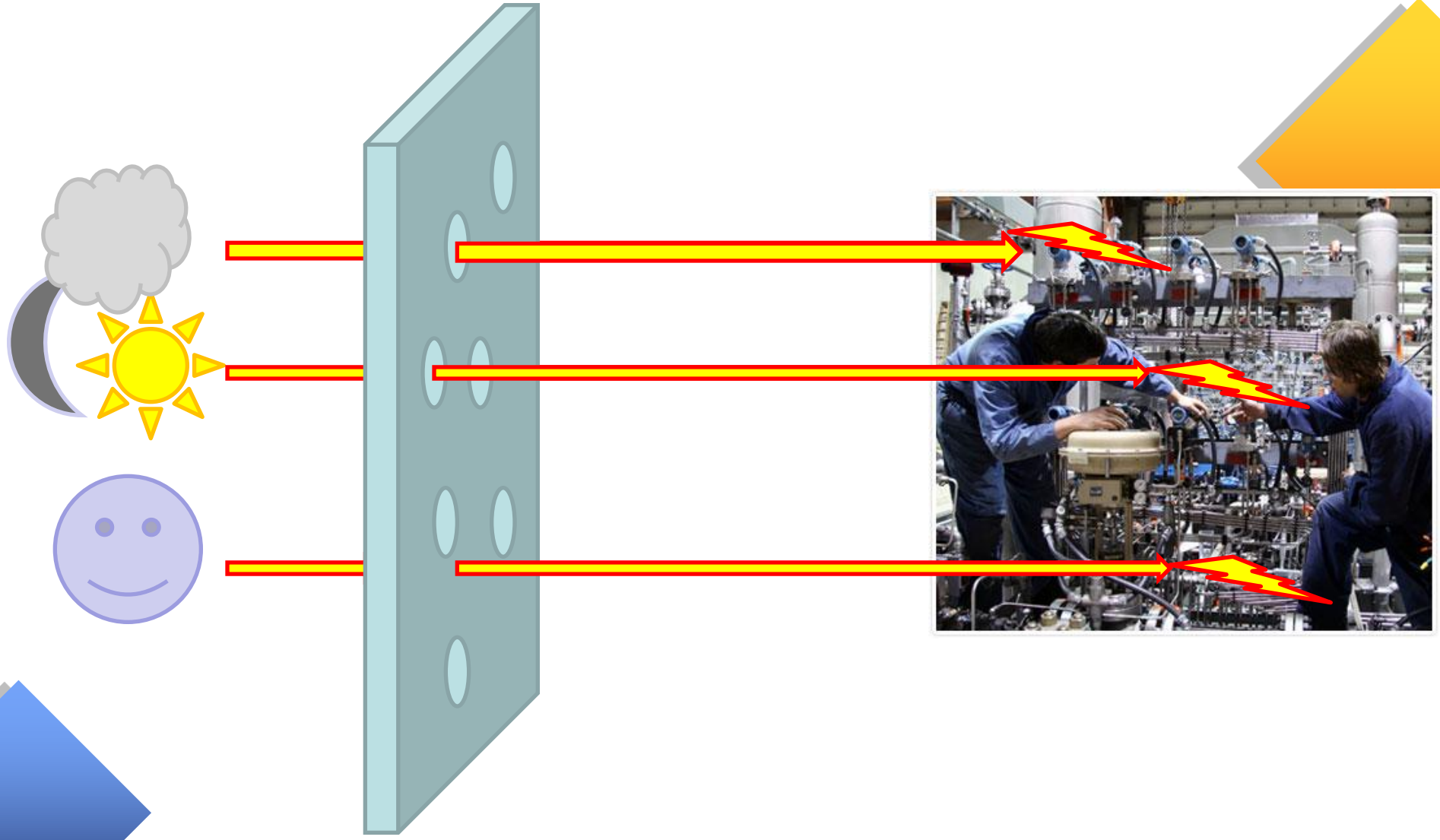
Notre problématique : les sources de danger



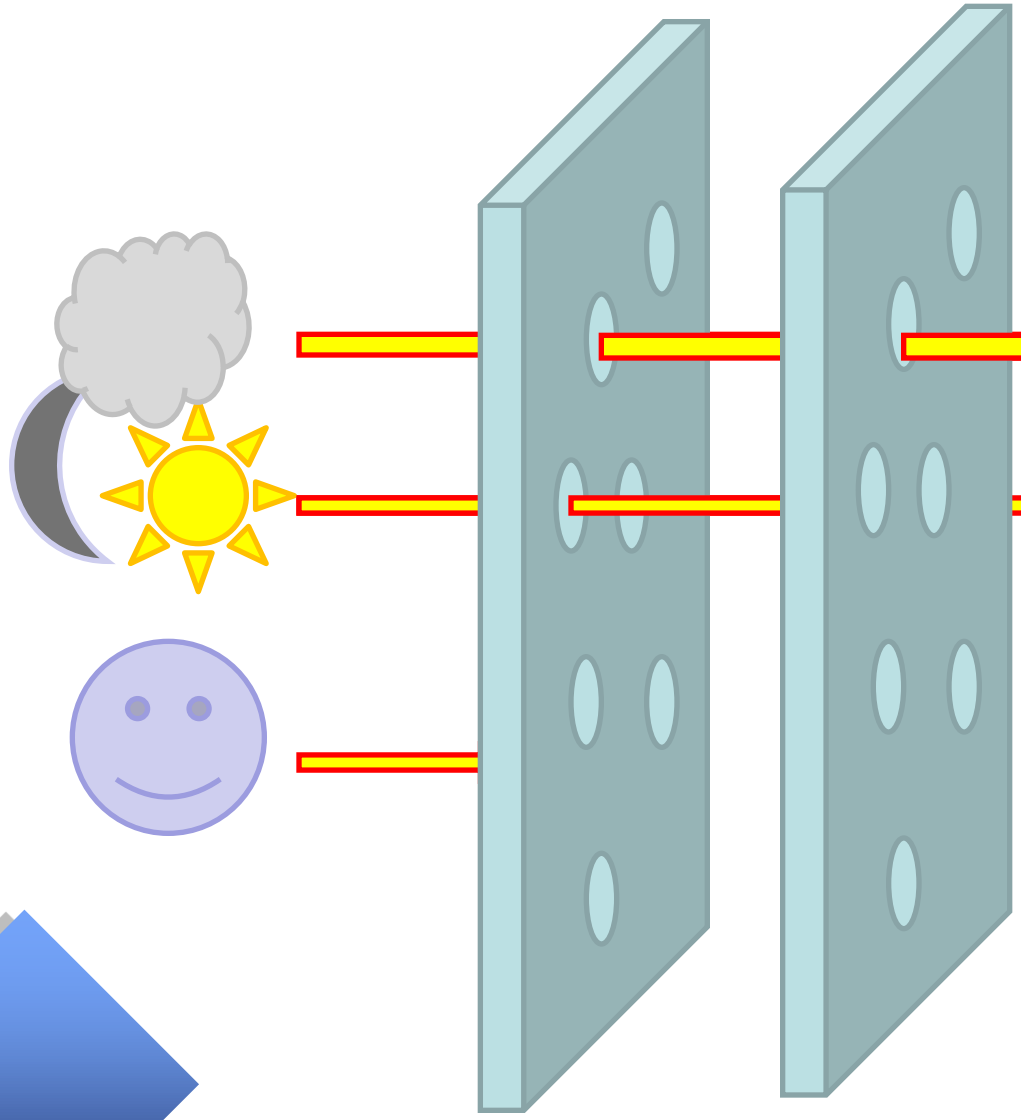


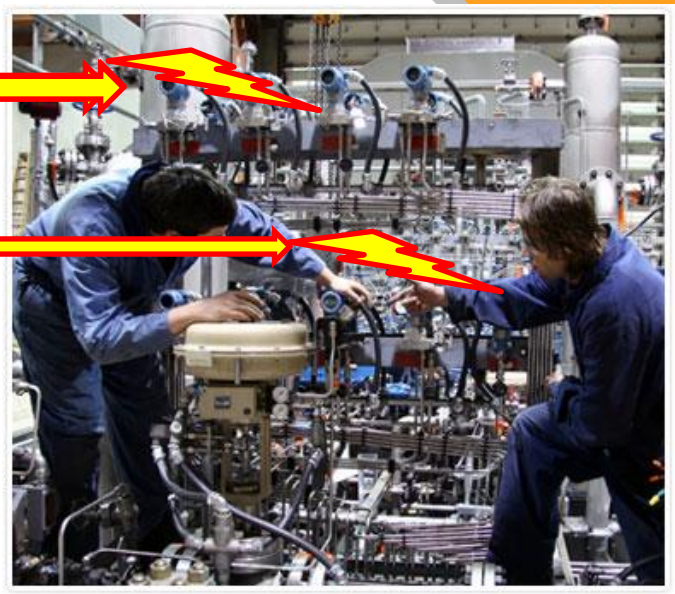


Notre problématique : efficacité des mesures de protection ?



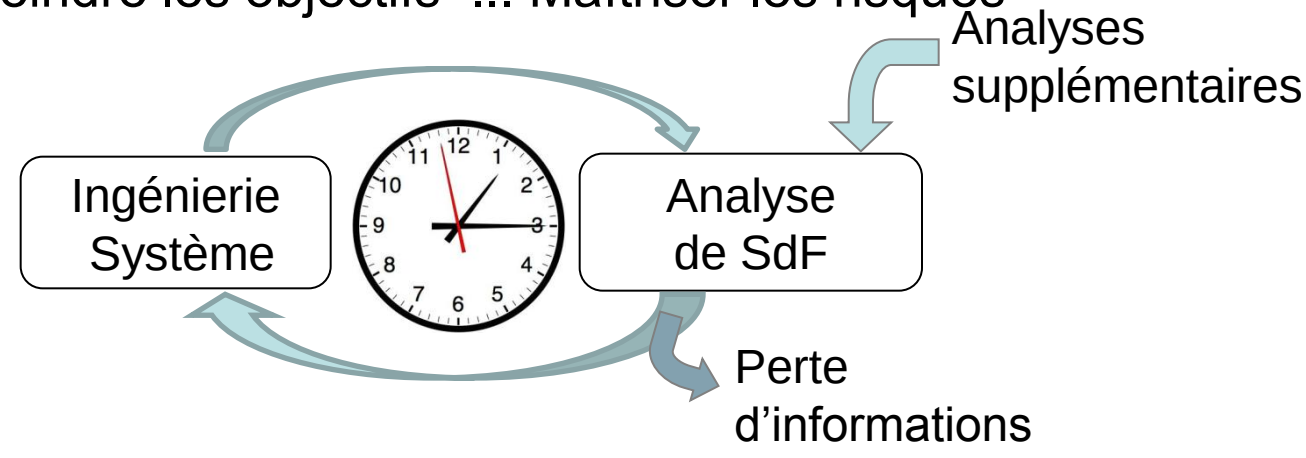
Notre problématique : efficacité économique des mesures de protection ?





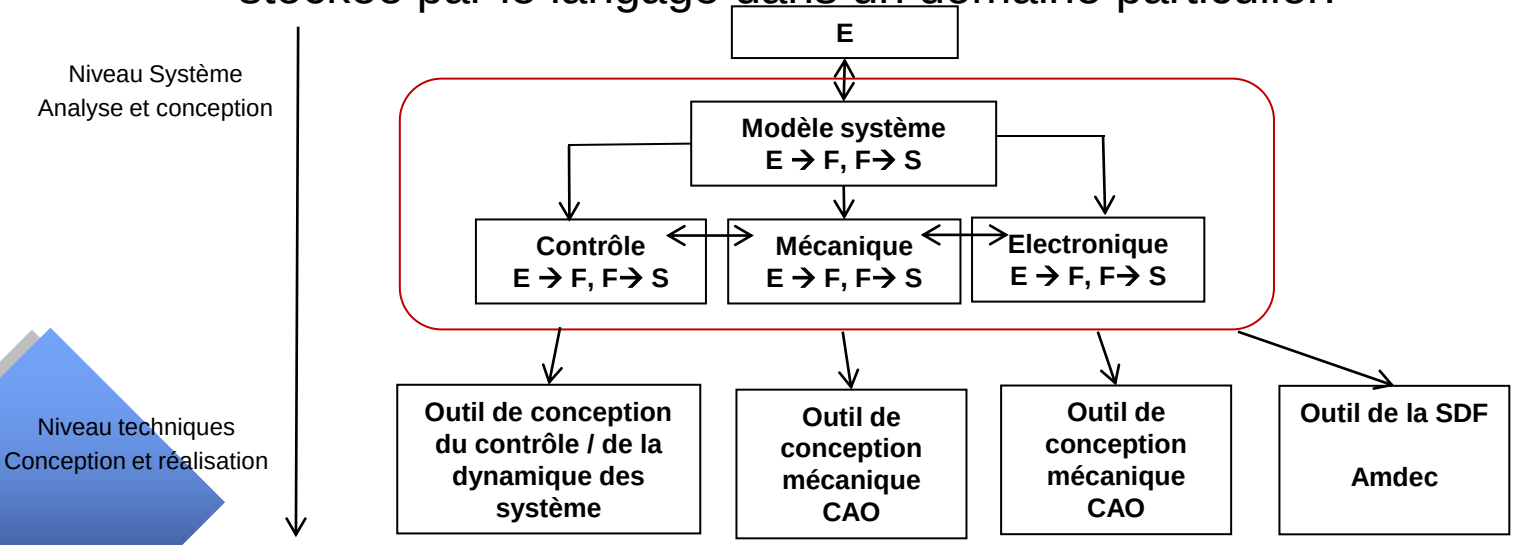
Notre problématique

- IS : Décrire un système en utilisant un formalisme
  - ✓ fonctions, états, comportement,…
  - ✓ ….maîtriser la complexité
- SdF : Analyser cette description à l'aide d'outils appropriés
  - ✓ Déterminer les scenarii de défaillance,
  - ✓ Calculer les taux de défaillance,
  - ✓ Estimer les composants critiques,
  - ✓ … maîtriser les coûts .
- Modifier le système en conséquence et réitérer les activités (IS, SdF) jusqu'à atteindre les objectifs ... Maîtriser les risques



Limites de l'IS

- Limites naturelles du langage système (LS) (ingénieur) généraliste [Qamar 2009]
- Pér : périmètre de description système qui défini le type d'informations stockées par un langage
  - ✓ Informations fonctionnelles, dysfonctionnelles,
  - ✓ Propriétés physiques, temporelles ou architecturales,
  - ✓ Comportements dynamiques…
- Pré : précision de description système qui définit la qualité de l'information stockée par le langage dans un domaine particulier.



- Sysml
- DSL

[Qamar 2009] A. Qamar, C. During, J. Wikander, Designing Mechatronic Systems, a Model-based Perspective, an Attempt to Acheive SysML-Matlab/Simulink Model Intergration, IEEE/ASME Conference on Advanced Intelligent Mechatronics, Singapore, Juiller 2009

Caractérisation d'un processus DSL

- Le langage cible du DSL présente un intérêt s'il : [cressent 2011]
  - ✓ Étend le périmètre du langage source
    - $Pér_{Cible} \not\subset Pér_{Source}$
  - ✓ Raffine les informations dans un domaine particulier
    - $Pré_{Cible}(D) > Pré_{Source}(D)$, où D est un domaine quelconque

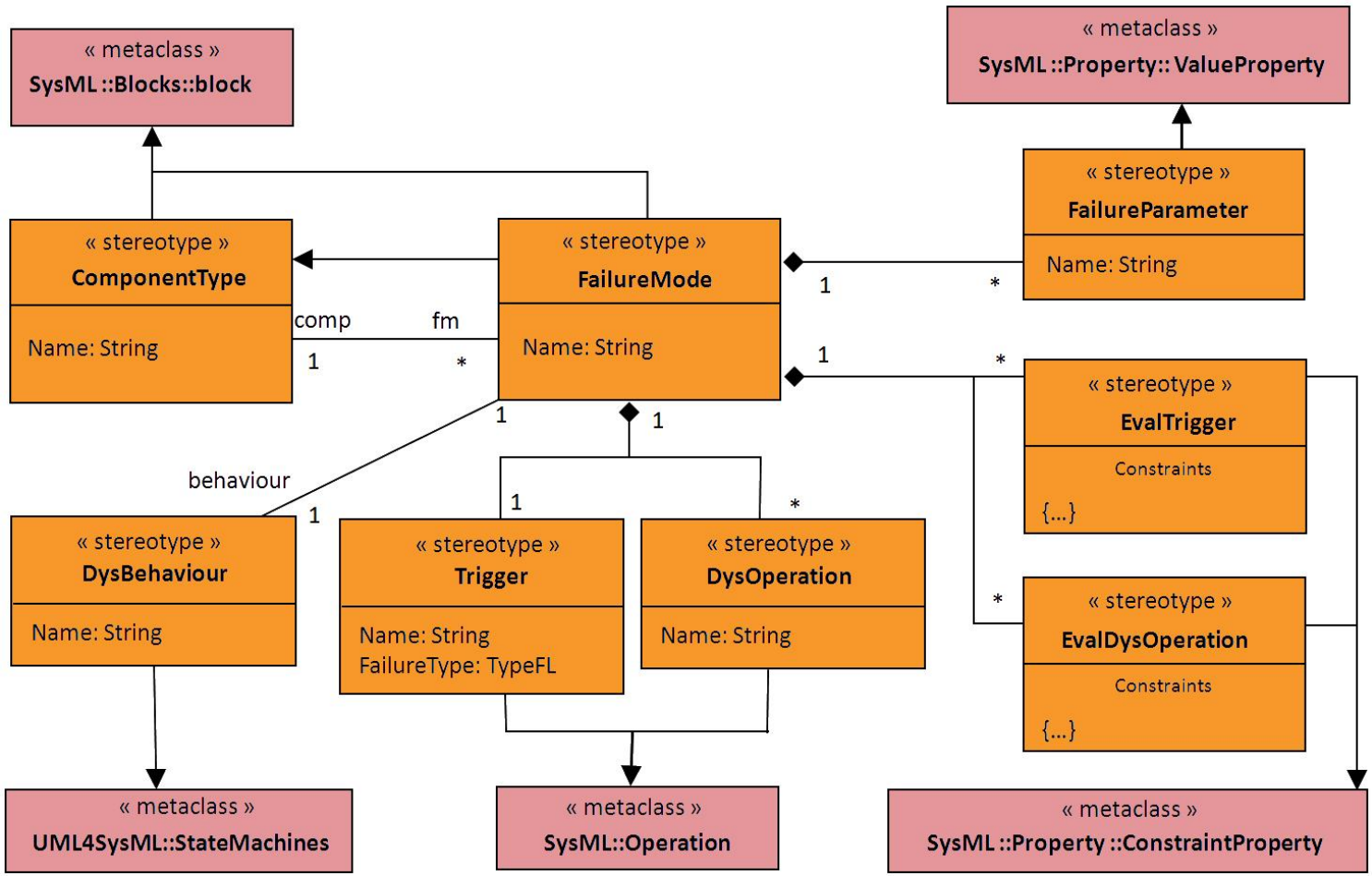
- Principe du processus
  - ✓ Identifier ($Pér(E_i)$, $Pré(E_i)$) - niveau de décomposition (LS/ DSL)
    - Gestion de la cohérence LS grâce à :(stfby, reaby, Stfby *o* reaby)
  - ✓ Vérifier que $Pér_{dsl} - (Pér_{dsl} \cap Pér_{LS}) = \{F_i, S_i, E_i\}_{new}$ ➔ BDM

    Base De Donnée Métier
  - ✓ Identifier les transformations de $\{F_i, S_i, E_i\}_{sys} X \{F_i, S_i, E_i\}_{new}$ ➔ $\{F_i, S_i, E_i\}_{dsl}$

    [david 2010]

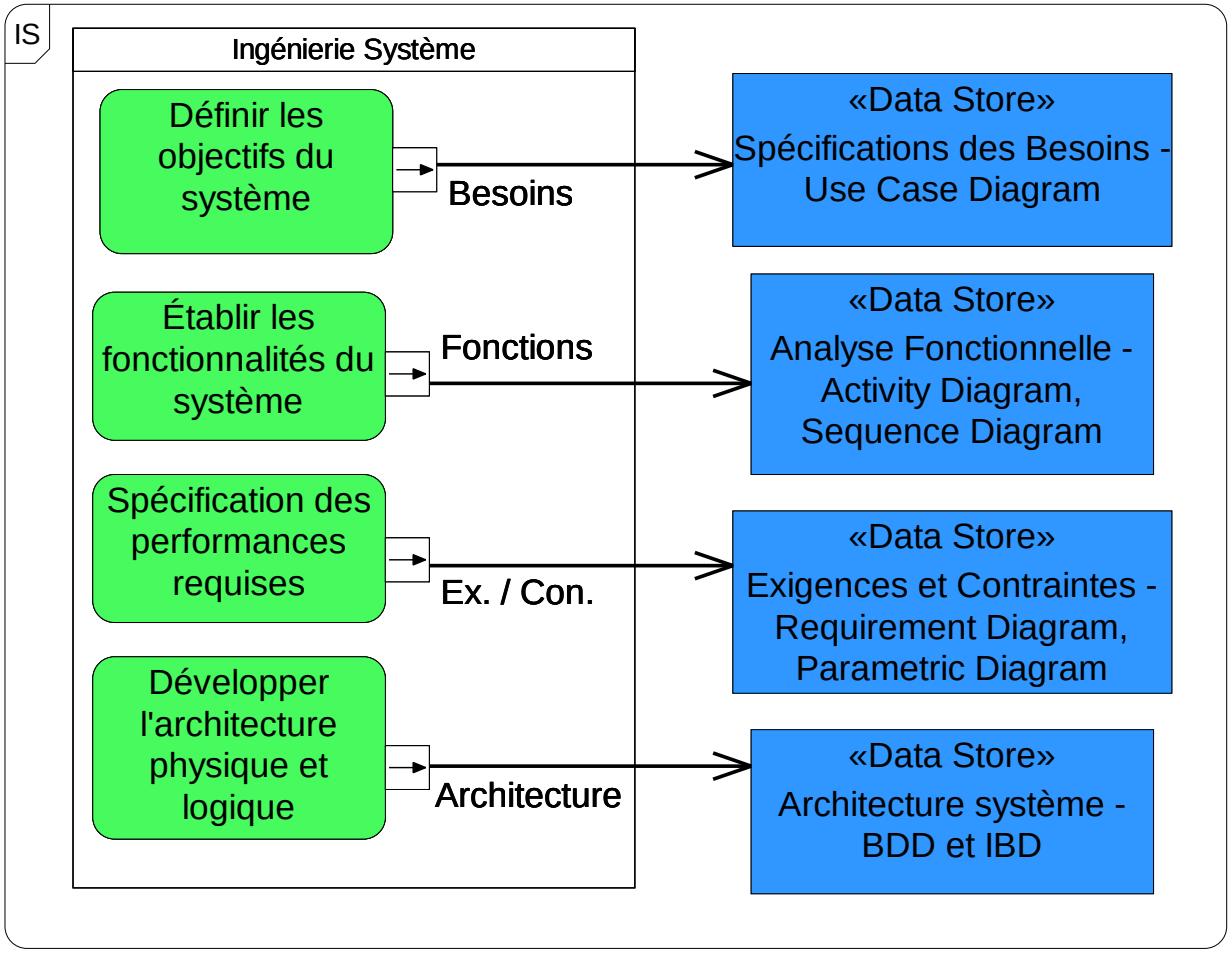
[Cressent 2011] R. Cressent, V. Idasiak, F. Kratz, Rapprocher les études de sûreté de fonctionnement de l'ingénierie système : retour d'expérience, *QUALITA 2011*, France (2011).
[David 2010] P. David, V. Idasiak, F. Kratz, Reliability study of complex physical systems using SysML, Reliability Engineering & System Safety, Vol. 95, pp. 431–450, 2010.

BDM Base De Donnée Métier : SDF DBD/BCD

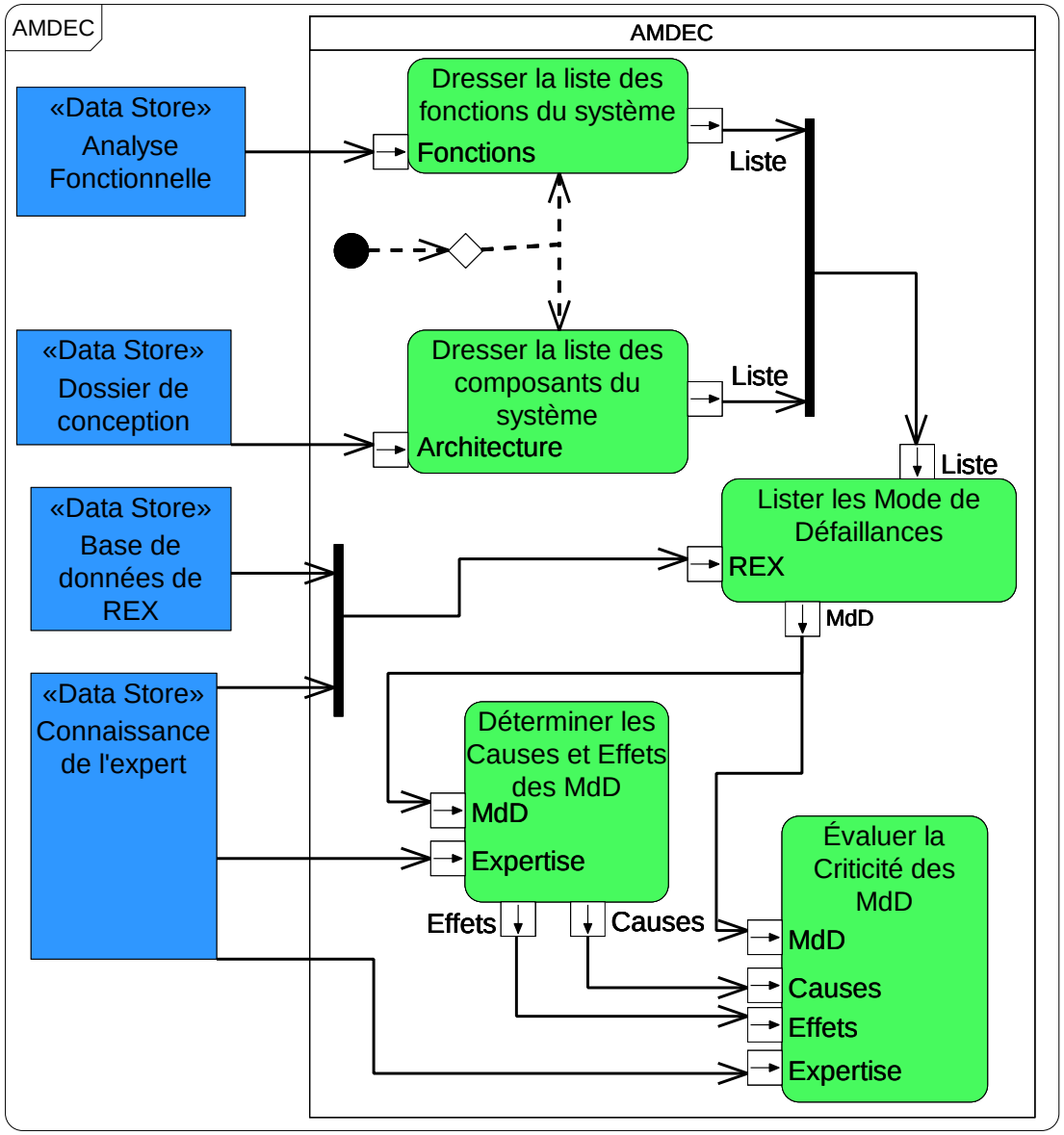


SL ←→DSL

Identifier les activités et processus – IS



Identifier les activités et processus – SdF



Dép

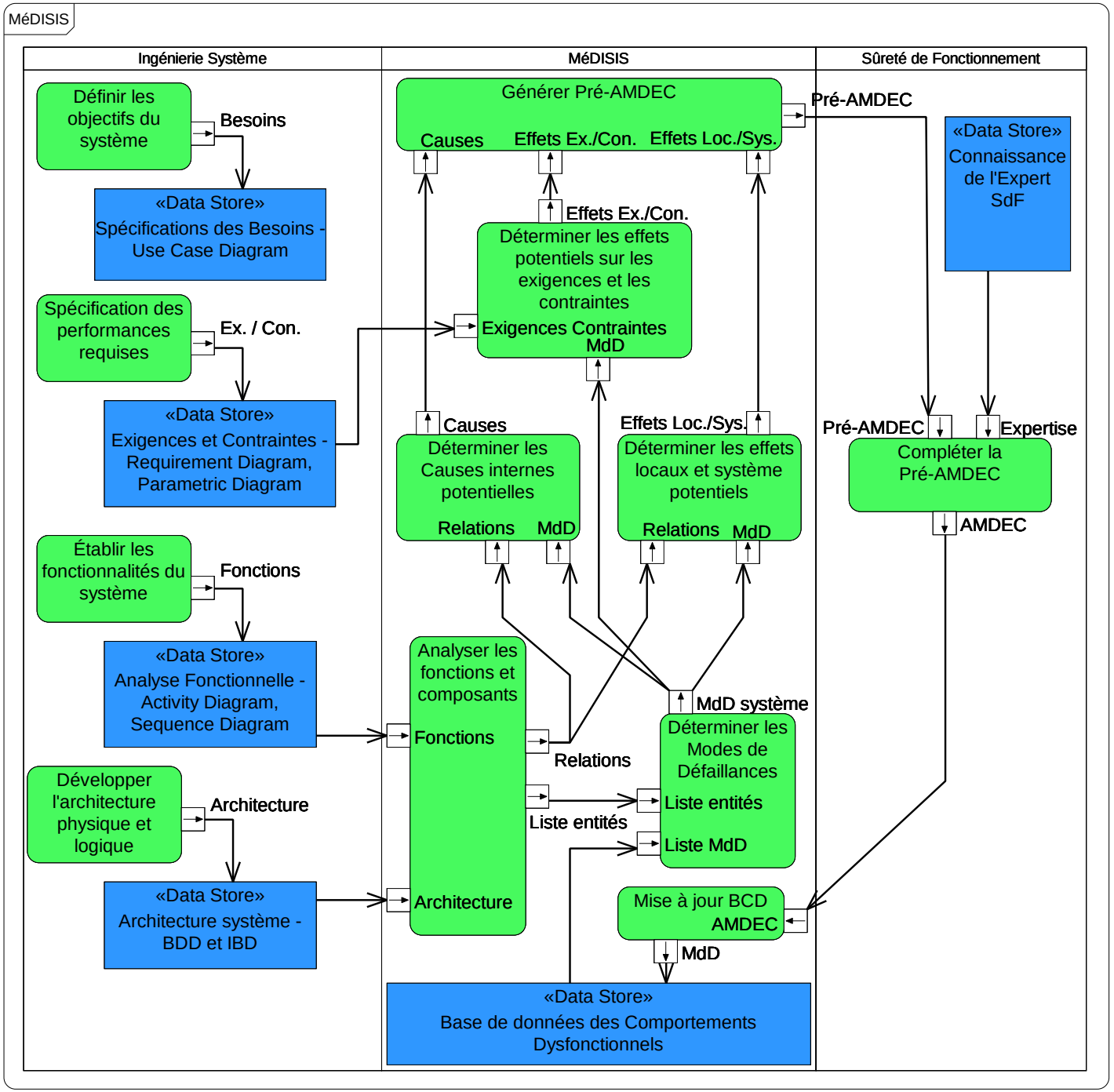
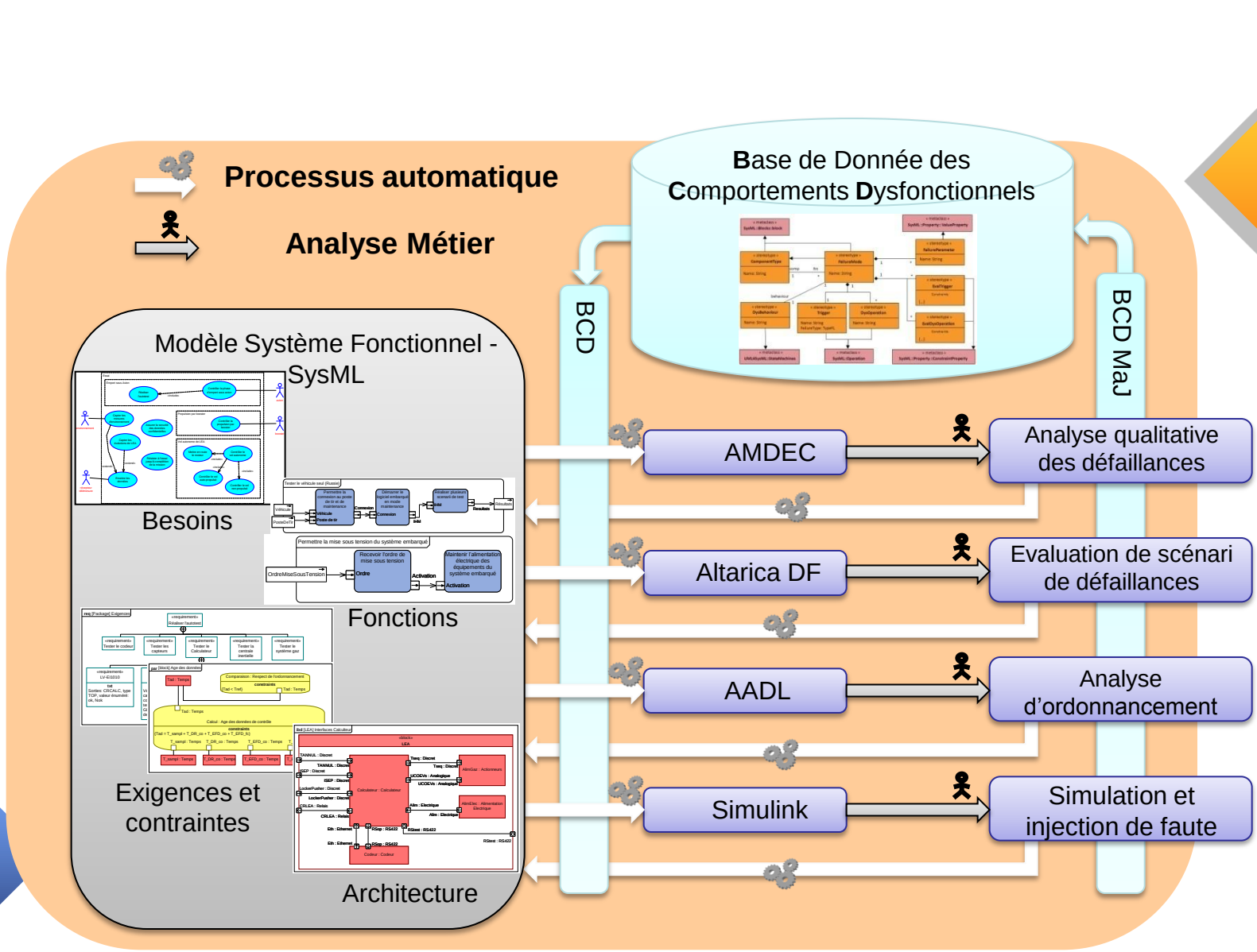
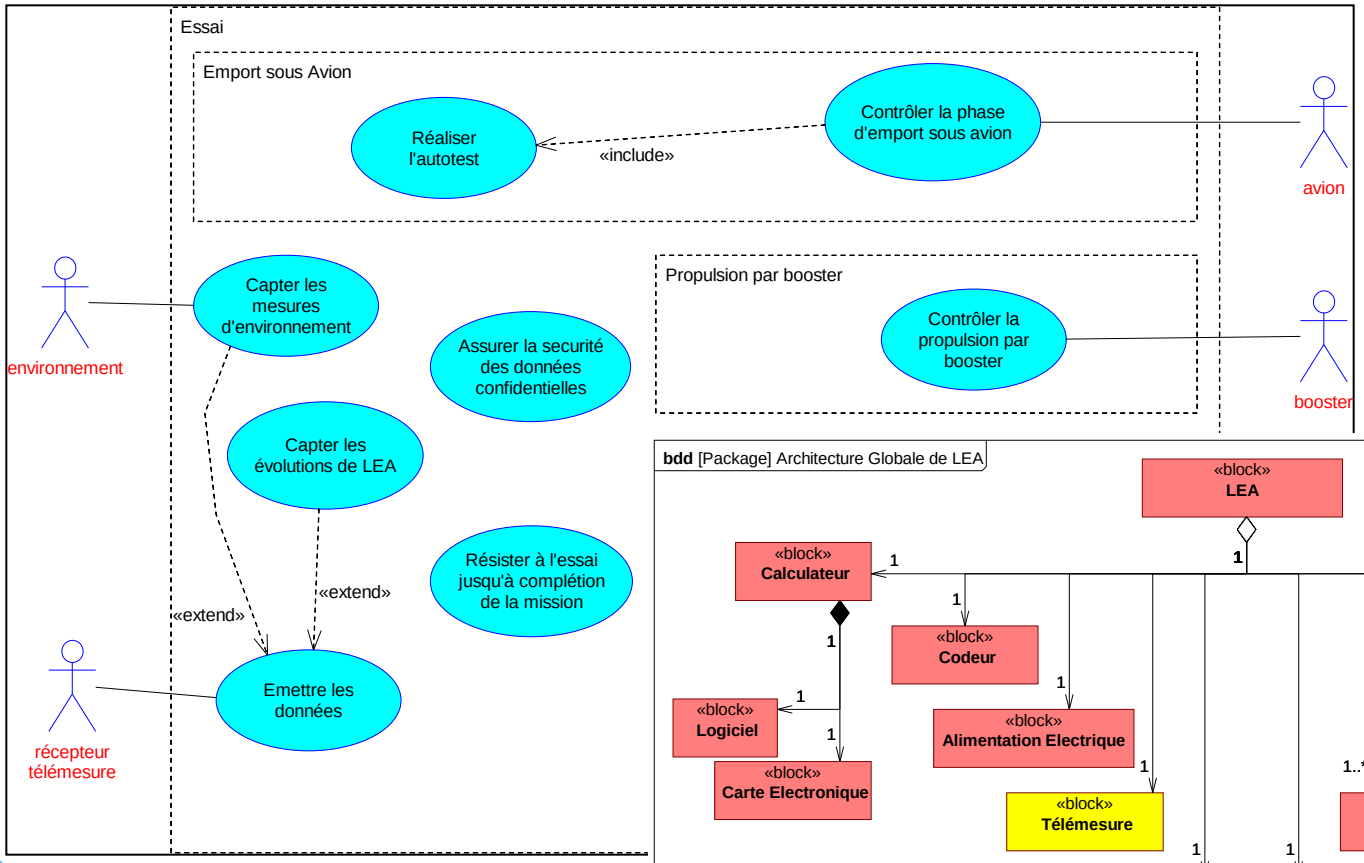
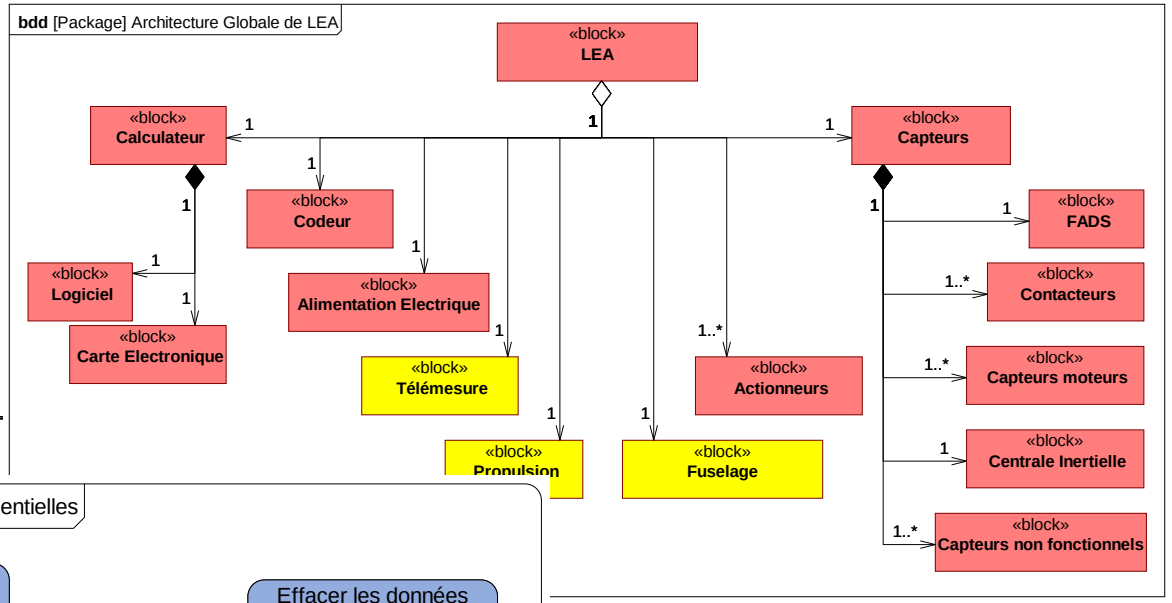

MéDISIS
Ingénierie Système
MéDISIS
Sûreté de Fonctionnement
Définir les objectifs du système
Besoins
«Data Store» Spécifications des Besoins - Use Case Diagram
Spécification des performances requises
Ex. / Con.
«Data Store» Exigences et Contraintes - Requirement Diagram, Parametric Diagram
Établir les fonctionnalités du système
Fonctions
«Data Store» Analyse Fonctionnelle - Activity Diagram, Sequence Diagram
Développer l'architecture physique et logique
Architecture
«Data Store» Architecture système - BDD et IBD
Générer Pré-AMDEC
Causes
Effets Ex./Con.
Effets Loc./Sys.
Pré-AMDEC
Effets Ex./Con.
Déterminer les effets potentiels sur les exigences et les contraintes
Exigences Contraintes
MdD
Causes
Déterminer les Causes internes potentielles
Relations
MdD
Effets Loc./Sys.
Déterminer les effets locaux et système potentiels
Relations
MdD
Analyser les fonctions et composants
Fonctions
Architecture
Relations
Liste entités
MdD système
Déterminer les Modes de Défaillances
Liste entités
Liste MdD
Mise à jour BCD AMDEC
MdD
«Data Store» Base de données des Comportements Dysfonctionnels
«Data Store» Connaissance de l'Expert SdF
Pré-AMDEC
Expertise
Compléter la Pré-AMDEC
AMDEC

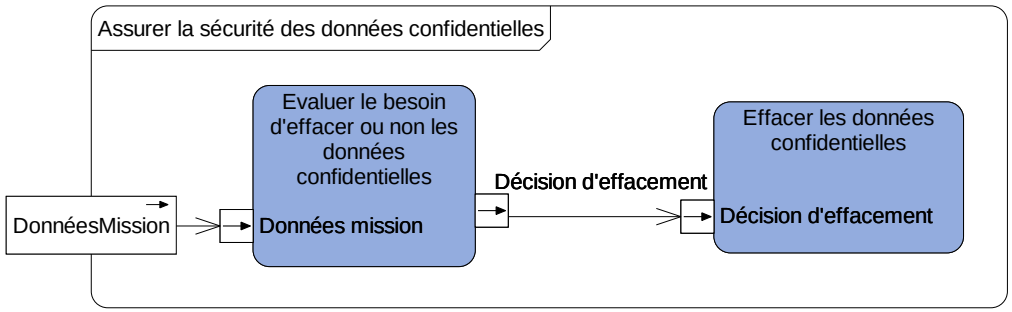
Plate-forme MéDISIS



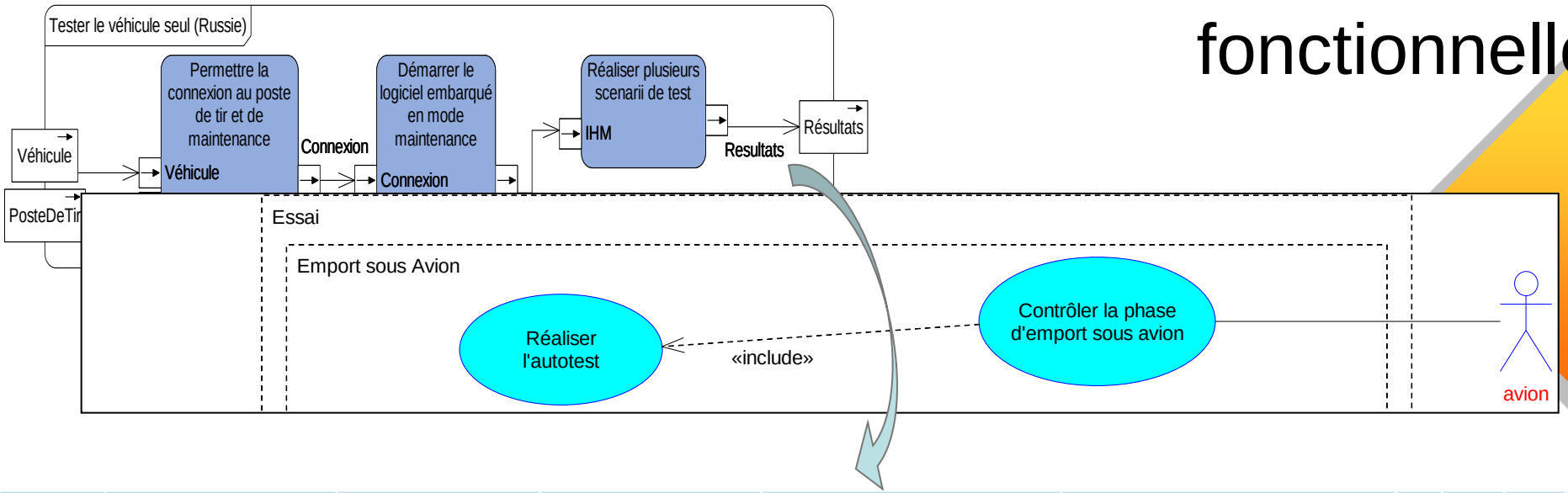
Modélisation système







A. M. D. E. C. fonctionnelle



ID	Fonction	Mode de défaillance	Cause	Effets Locaux	Fonctions principales impactées	Gravité	Fréquence	Criticité
Phase de vie: Emport sous avion KLEA sous tension								
FD-4	Autotest	Fonction Absente	Défaillance fonction: Mise sous tension / Avion	Fonction défaillante: Contrôler la phase d'emport sous avion	Contrôler la phase d'emport sous avion	4	3	12
FX-4	Détecter l'ordre d'annulation de mission	Fonction Absente	Non réception du signal: TANNUL	Fonction défaillante: Annuler la mission	Contrôler la phase d'emport sous avion, Capter les évolutions de mission (ISEP, TANNUL)	3	3	9

A.M.D.E.C. composant

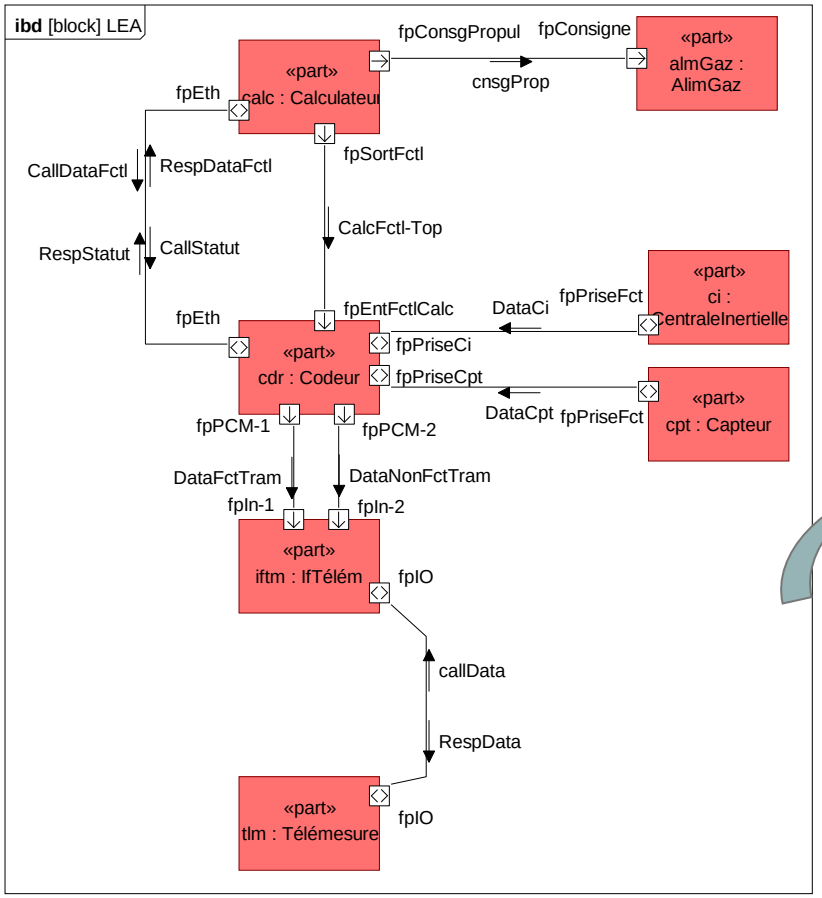
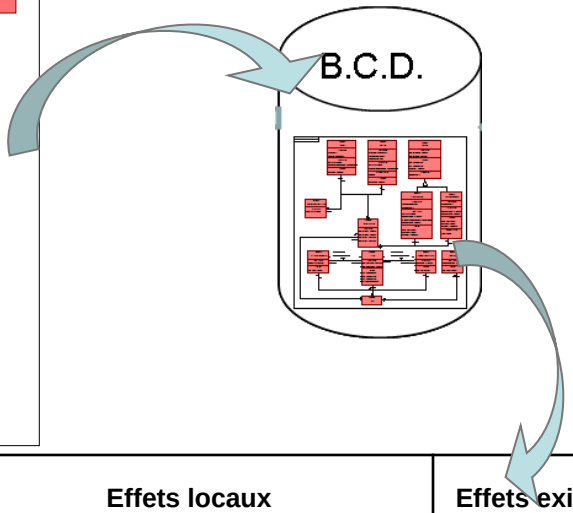


Diagramme de bloc interne de LEA



Extrait de l'AMDEC de LEA

Nom	Modes de défaillances	Causes	Effets locaux	Effets exigences	Effets systèmes
Calculateur	Défaillance d'ordon-nancement	Flux Ethernet [Contrainte Env : vibration]>[Specif. Connecteur]	Consigne de propulsion [AlimGaz] / Sorties Fonctionnelles [Codeur]	Contraintes temps réelles non respectées	Perte de données capteurs non transmises au codeur destinées à la télémesure / Risque de mauvais fonctionnement du moteur si les consignes ne sont pas émises convenablement.
		Surcharge Interne	Consigne de propulsion [AlimGaz] / Sorties Fonctionnelles [Codeur]	Contraintes temps réelles non respectées	Perte de données

Analyse spécifique métier

Etude d'ordonnancement avec AADL

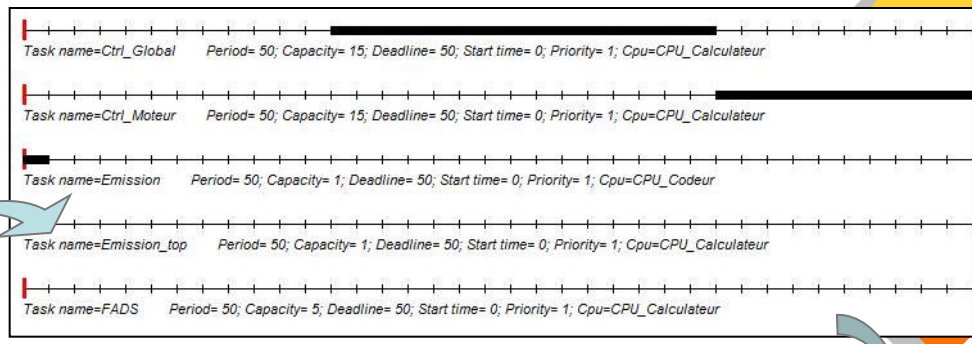
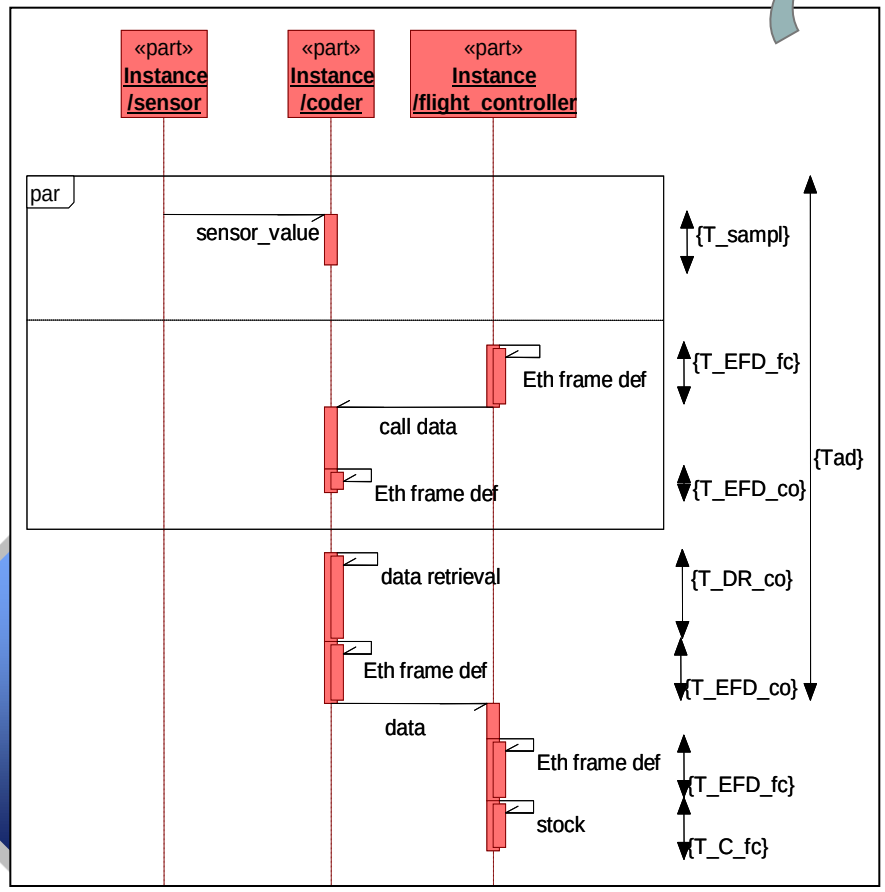
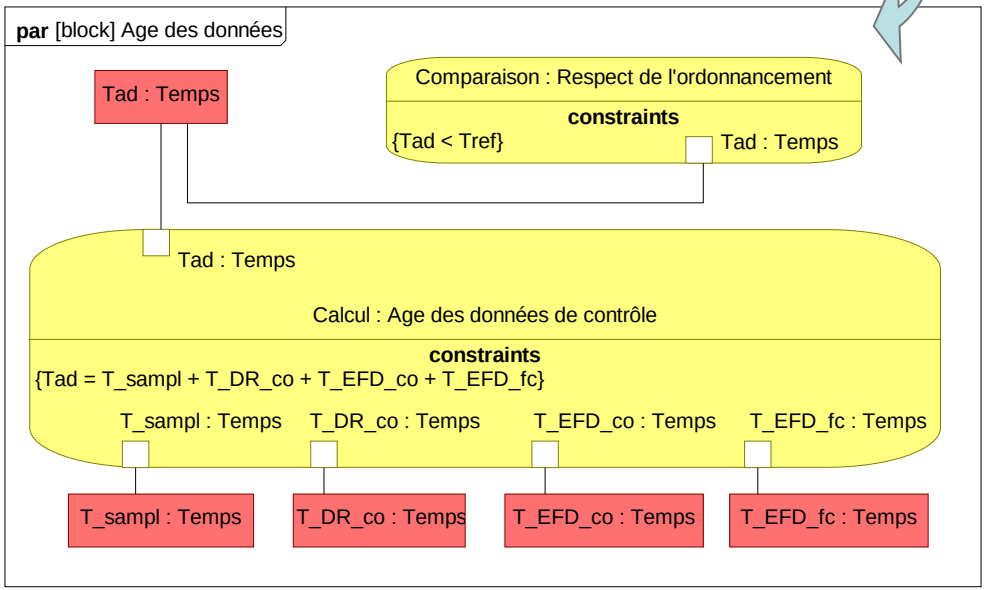


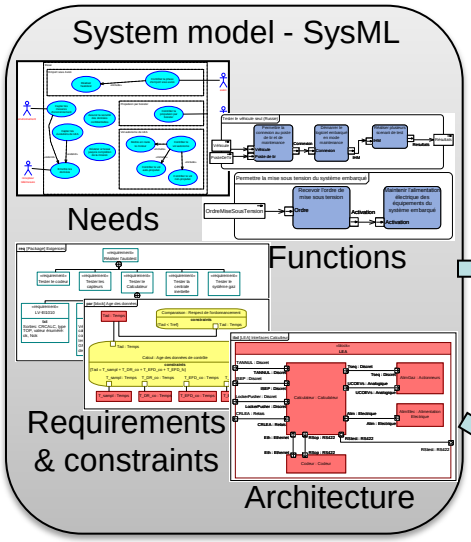
Diagramme de séquence de LEA

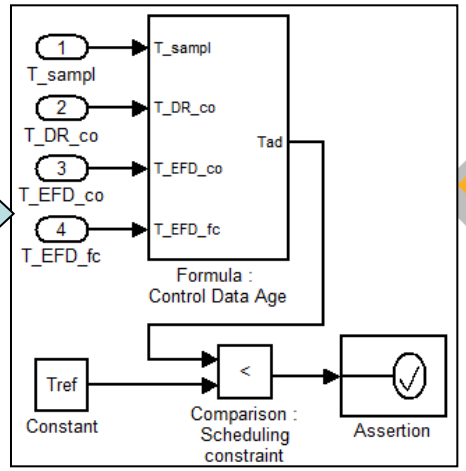


Retour d'informations au niveau système

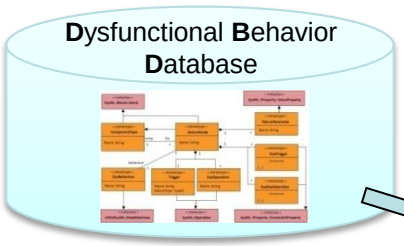


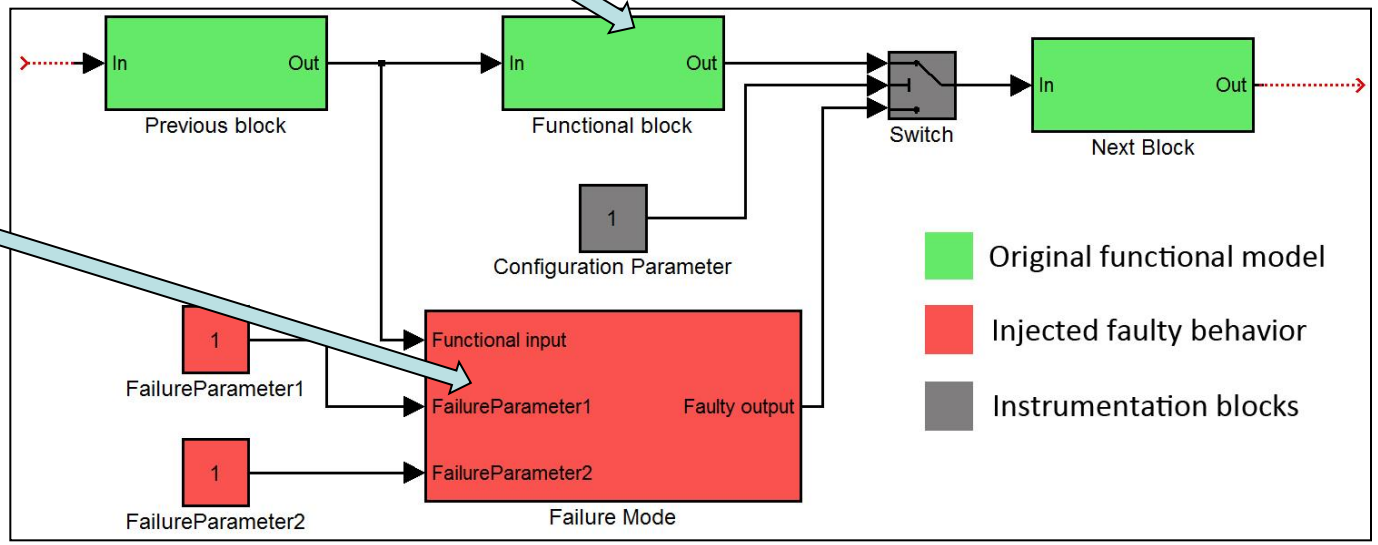
Injection de fautes avec simulink





Test avec les assertions Simulink





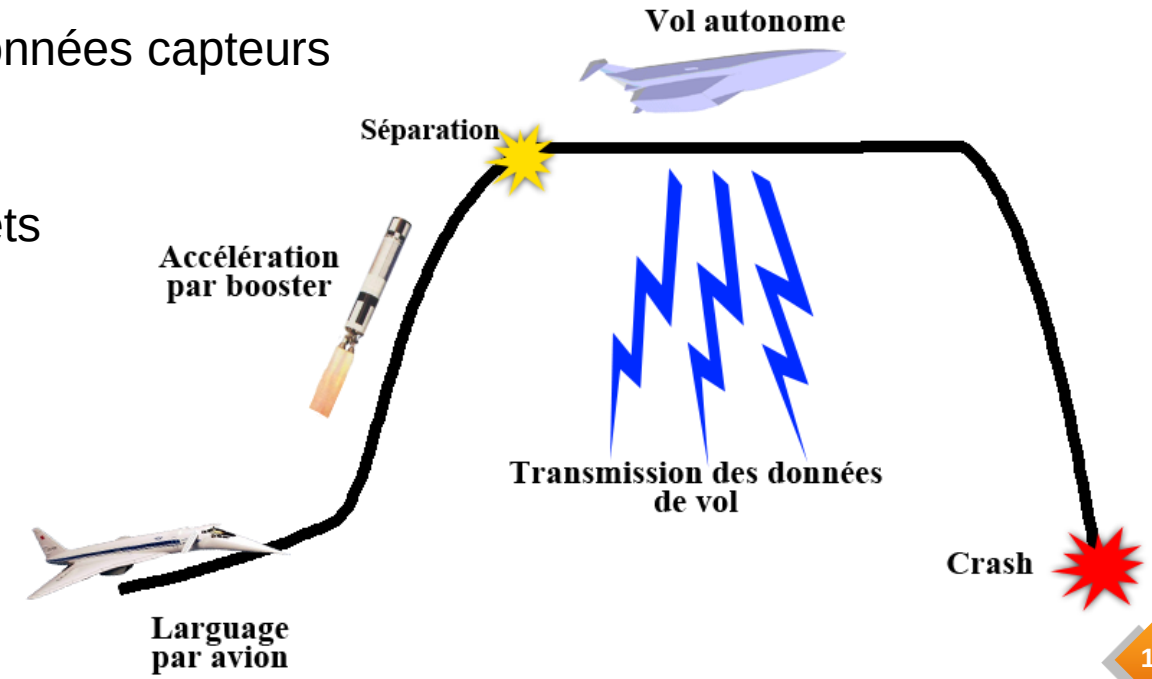
Injection de défaillance dans le modèle

Le projet LEA

(Lietaoutnii Experimentalnii Apparat)

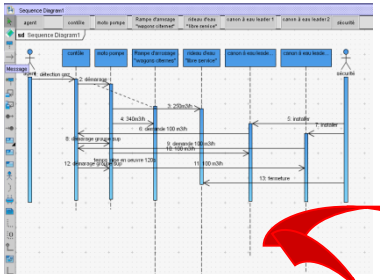
- Objectif : tester un stato-réacteur en conditions réelles de vol
- Le système embarqué contrôle la propulsion et gère l'intégrité des données et les fonctions de sécurité :
  - ✓ Allumage du moteur
  - ✓ Régulation des gaz
  - ✓ Test des équipements
  - ✓ Mise en forme des données capteurs

- Maitrise des risques projets et risques technologiques

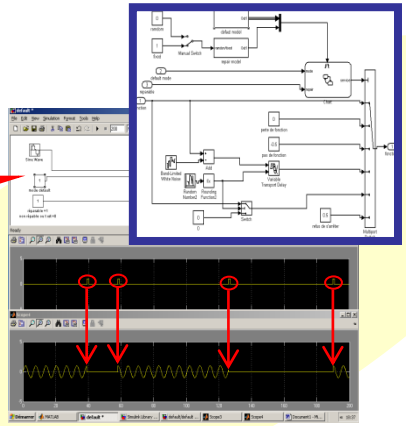


Les projets Virtual P.O.I.

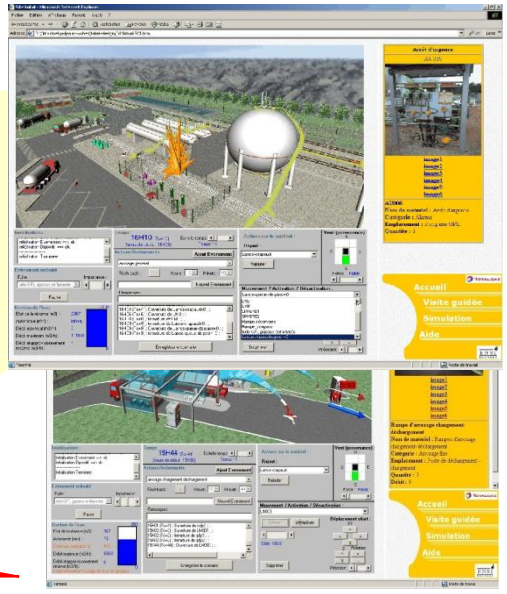
(Total-gaz 2006, Dispatmo 2012)

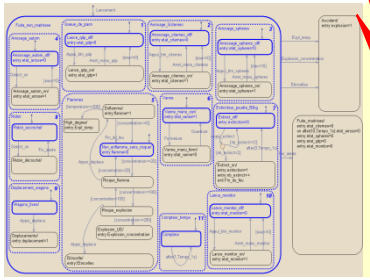


Modèle fonctionel



Modèle de défaillance





Model Dynamique
- **Statechart**

✓Prototype sous matlab, exécutable (java, vrml/ moteur 3D).
✓Modélisation et analyse des scénarios d'accidents (SysML).
✓Outil d'aide à la décision.

✓Maîtrise des risques technologiques et humains

Conclusion

- MéDISIS démarche généraliste systémique permet de faciliter :
  - ✓ Les échanges d'informations et de propriétés du système entres les différents modèles et domaines
  - ✓ Le retour d'information depuis les analyses spécifique métier vers le modèle système
- MéDISIS s'intègre efficacement dans une stratégie d'ingénierie système dirigée par les modèles

- Retour projets montre :
  - ✓ Démarrage des activités de SDF plus rapide
  - ✓ Resistance des études systèmes aux modifications
  - ✓ Meilleurs prise en compte des résultats des analyses de risque.

- Points d'amélioration et perspectives
  - ✓ Connexion au base de donnée métier (FIDES).
  - ✓ Prise en compte de nouveau Pus (HAZOP)

Merci de votre attention