Systemx INSTITUT DE RECHERCHE TECHNOLOGIQUE

Accélérateur de la transformation numérique

GT TransForm

De l'approche MBSA-OpenAltaRica vers le MBSE

14-12-2017

Michel BATTEUX

www.irt-systemx.fr

Analyses (probabilistes) du risque de système complexes (critiques)

Obligatoire dans tous systèmes industriels critiques

http://fr.wikipedia.org/wiki/Airbus_A380

http://fr.wikipedia.org/wiki/TGV

https://group.renault.com

http://energie.edf.com

http://fr.dcnsgroup.com

- ✓ raisons environnementales, sociales et économiques
- ✓ codifiée par autorités de régulation au travers de standards (IEC 61508, DO 178B, IEC 62279, ISO 26262, IEC 61513, etc.)

Analyses (probabilistes) du risque de système complexes (critiques)

De quoi parle-t-on ?

Analyses (probabilistes) du risque de système complexes (critiques)

De quoi parle-t-on ?

- Analyses (probabilistes) du risque
  - Fiabilité
  - Disponibilité
  - Maintenabilité
  - Sureté (safety)
  - Niveau d'intégrité de sécurité (SIL Safety Integrity Level)
  - Assurance/garantie de production, disponibilité de production
  - Etc.

i.e. tous types d'indicateurs (probabilistes) du risque/performance de systèmes sujets à des pannes, des défauts, des erreurs humaines, des conditions environnementales dégradées, etc.

Analyses (probabilistes) du risque de système complexes (critiques)

De quoi parle-t-on ?

- Analyses (probabilistes) du risque
- Systèmes (de systèmes) complexes
  - (INCOSE) « un système est la combinaison d'éléments interagissant ensemble et organisés pour assurer un ou plusieurs objectifs établis ».
  - Interconnexions et interactions (fortes) entre 'parties'/'composants' de différentes natures (matériel, logiciel, humain)
  - Phénomène d'émergence ('comportement')
  - Architecture pouvant évoluer au cours du temps
  - Suivant un/des objectifs (qui peuvent être en opposition)

Analyses (probabilistes) du risque de système complexes (critiques)

De quoi parle-t-on ?

- Analyses (probabilistes) du risque
- Systèmes (de systèmes) complexes critiques
  - Défaillances dépendantes ou en cascade,
  - Redondances (froides) et/ou composants de rechange,
  - Accès limités à certaines ressources,
  - Stratégies de reconfigurations et/ou maintenances,
  - Boucles de rétroaction, logique de contrôle/commande,
  - Disponibilités de production sous incertitudes,
  - Etc.

i.e. des systèmes pour lesquels l'analyse probabiliste du risque, au moyen de formalismes classiques (AdD ou équivalents), est généralement très dure et fournie des résultats 'grossiers' (trop pessimistes) à cause des dépendances entre événements de base.

Analyses (probabilistes) du risque de système complexes (critiques)

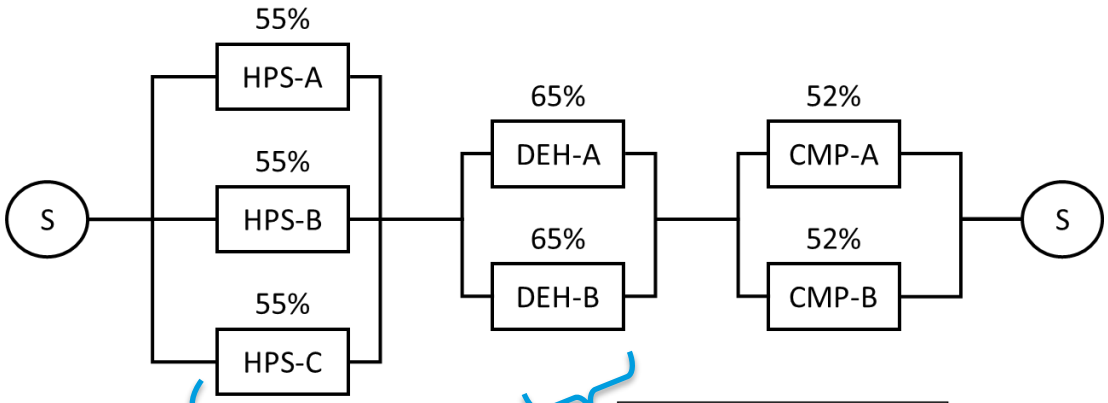
De quoi parle-t-on ?

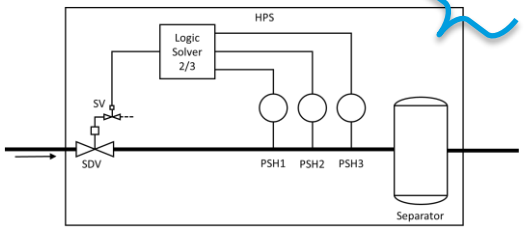
- Analyses (probabilistes) du risque
- Systèmes (de systèmes) complexes critiques

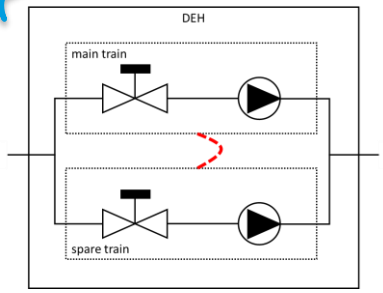
Problématiques adressées

- Complexité de calculs des indicateurs du risque/performance
- Niveau approprié d'abstraction
- Maintient des modèles en phases de conception et exploitation
- Réutilisation des modèles (ou parties)
- Synchronisation/mise en cohérence des modèles (sûreté – architecture)

Disponibilité de production (exemple)







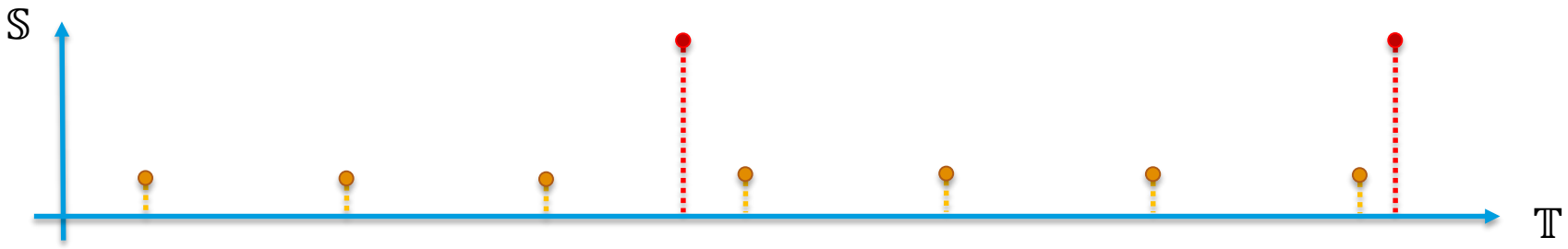
Production moyenne sur X années ? sachant que

- Composants peuvent **tomber en panne** et **être réparés**
- **Redondances** (froides) sur des (ensembles de) composants
- Défaillances de **causes communes**
- Composants avec « stratégies » de **détection** de mauvais fonctionnement
- Politiques de **maintenance** (corrective, préventive, prédictive) avec un **nombre limité** de **réparateurs partagés**

Analyses (probabilistes) du risque de système complexes (critiques)

Risque est de nature bidimensionnelle : analysé suivant deux axes

- sa fréquence
- sa sévérité

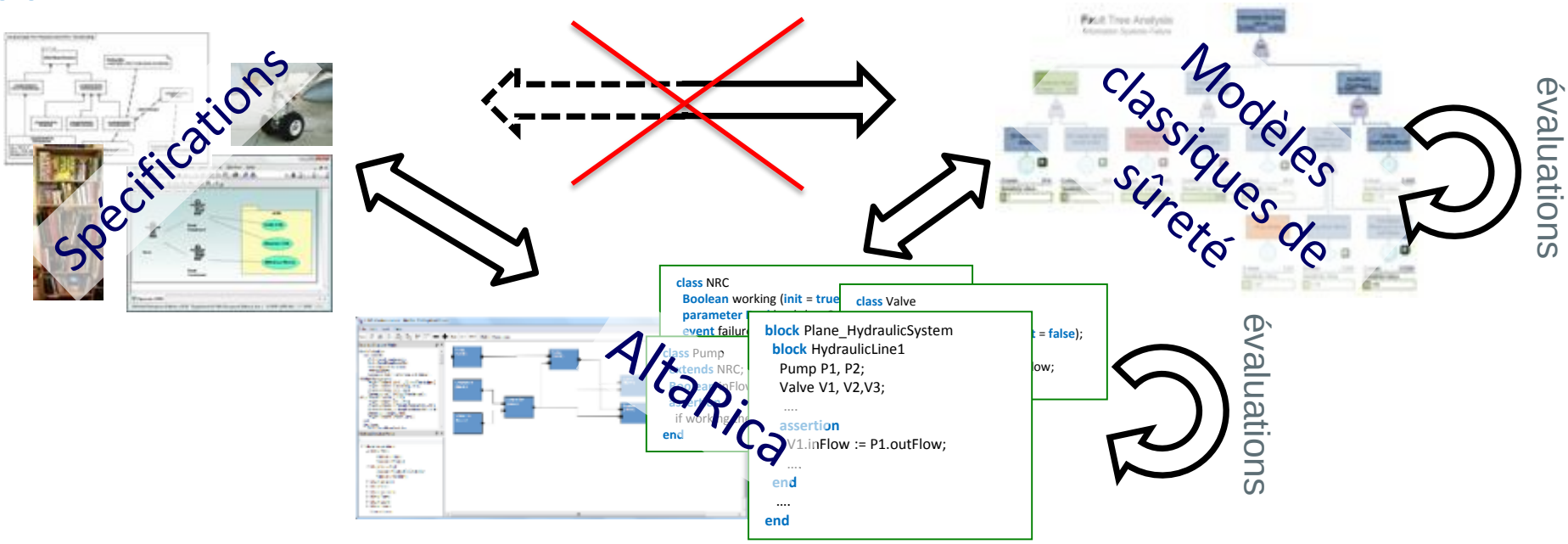


approche probabiliste d'évaluation

- ✓ déterminer les scénarios les plus fréquents
- ✓ déterminer les scénarios les plus graves

Risque inacceptable => cherche à l'atténuer, au moyen de mécanismes de sûreté, réduisant ou sa fréquence, ou sa sévérité, ou les deux.

Approche MBSA/AltaRica



Modéliser à plus haut niveau pour réduire la distance entre les spécifications et les modèles (sans augmenter la complexité des calculs)

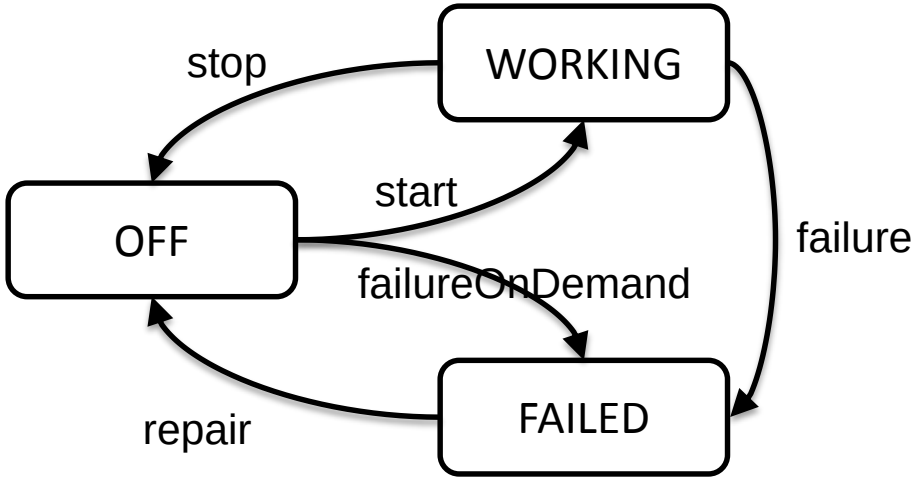
- **Animation/simulation** des modèles : faciliter **validation des modèles**, **discussions aves parties prenantes**.
- Un modèle, plusieurs événements redoutés : faciliter gestion **version**, **configuration**, **changements**
- Un modèle, plusieurs outils d'évaluation : **polyvalence** des évaluations, **assurance qualité** des résultats
- Analyse plus fine : **éviter** les **résultats pessimistes**

Langage de modélisation AltaRica 3.0 – Partie comportementale

1. Description centrée événements

Le système peut être dans un certain nombre d'**états** et les changements d'états se font suivant des occurrences d'**événements**.

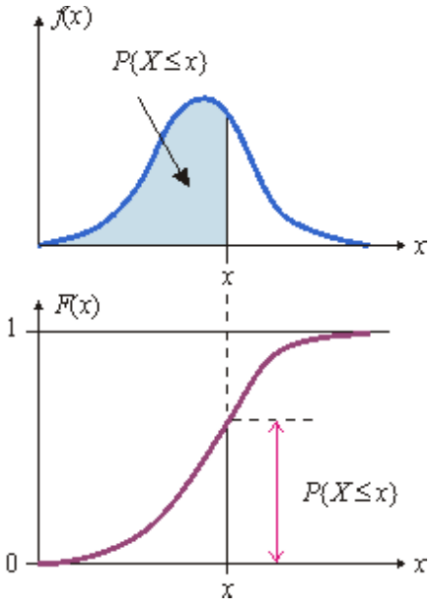
L'état du système est décrit au moyen de variables (une ou plusieurs)

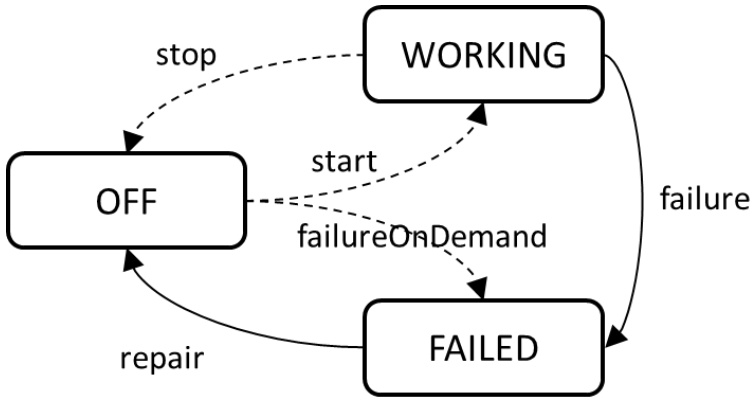


Langage de modélisation AltaRica 3.0 – Partie comportementale

1. **Description centrée événements**
2. **Description stochastique**

Les événements sont associés à des **délais stochastiques** ou **déterministes** et/ou des **probabilités** (**poids**)





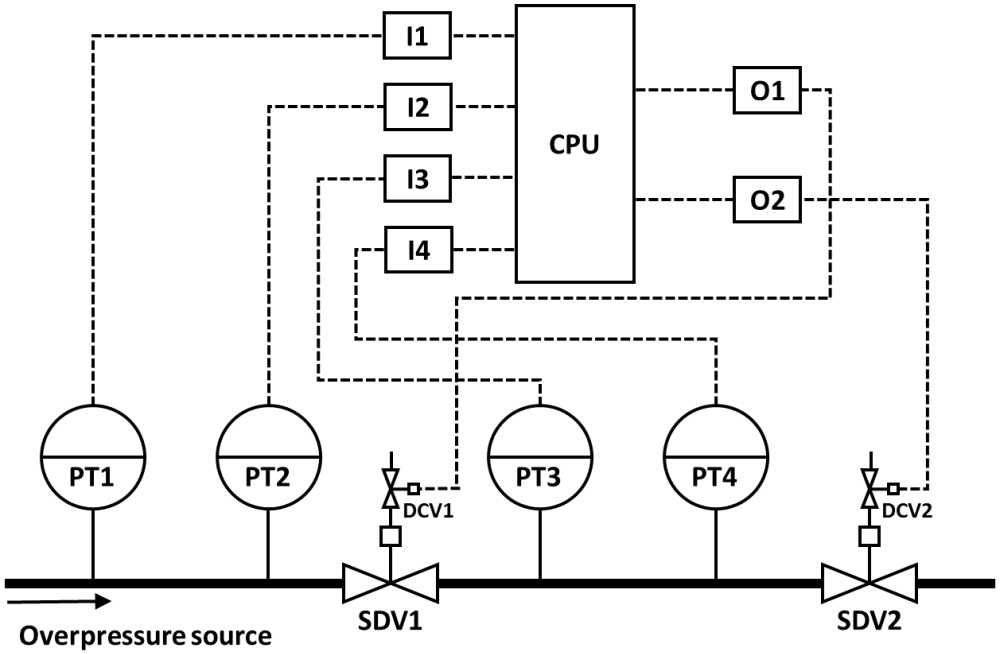
Event	Rate	Probability
failure	λ	
repair	μ	
start		$1-\gamma$
failureOnDemand		γ
stop		1

Langage de modélisation AltaRica 3.0 – Partie comportementale

1. **Description centrée événements**
2. **Description stochastique**
3. **Compositionnel et représentation implicite**

Le modèle du système s'obtient en **composant** des modèles de sous-systèmes et composants.

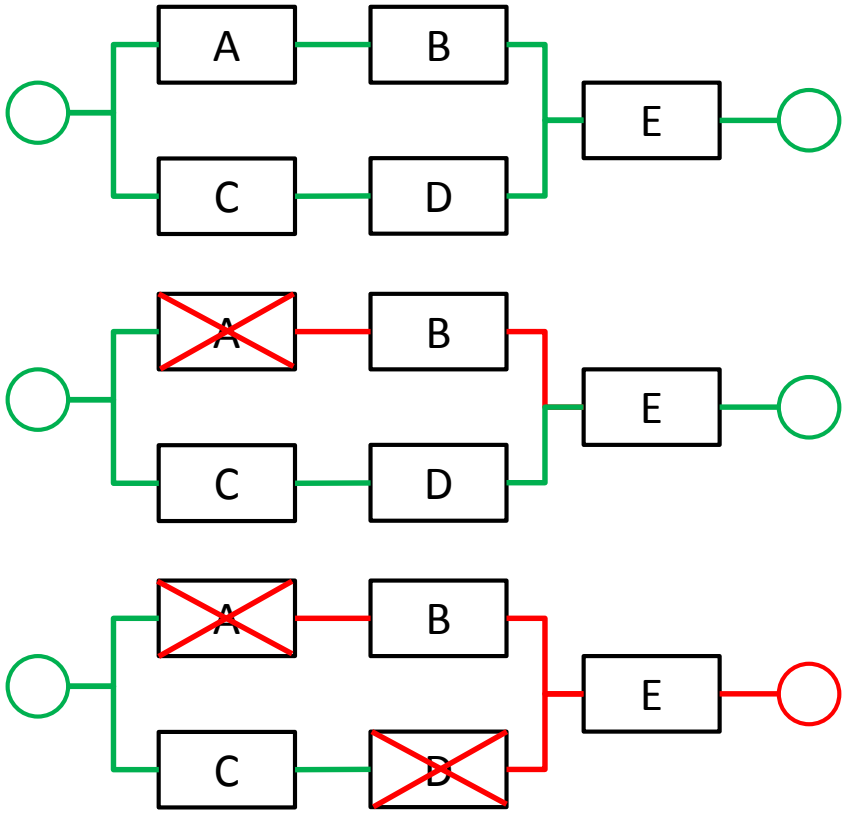
Cela signifie que le modèle est une **représentation implicite** de l'espace d'états (à l'inverse d'une représentation explicite comme les chaînes de Markov).



Langage de modélisation AltaRica 3.0 – Partie comportementale

1. **Description centrée événements**
2. **Description stochastique**
3. **Compositionnel et représentation implicite**
4. **Propagation des flux**

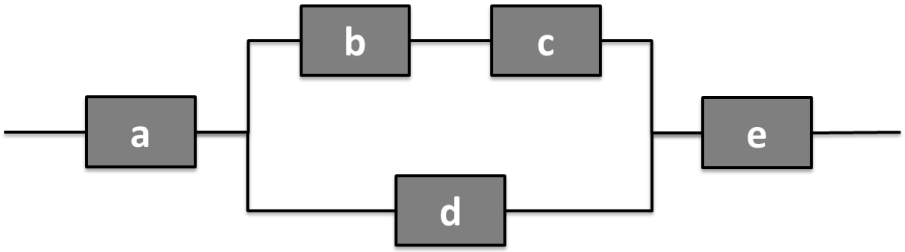
Après chaque **tirage** de transition, un mécanisme **propage** les changements d'états à travers le **réseau de composants**

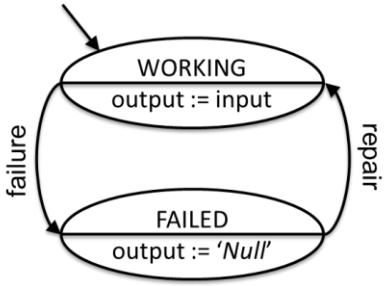


Les **flux** circulant à travers le réseau peuvent être de différents **types**

Langage de modélisation AltaRica 3.0 – Exemple

- 5 composants identiques
- Chacun peut tomber en panne et être réparé






```
class Component
    Boolean _state (init = true);
    Boolean input, output (reset = false);
    parameter Real lambda = 1.0e-5;
    parameter Real mu = 1.0e-2;
    event failure (delay = exponential(lambda));
    event repair (delay = exponential(mu));
    transition
        failure: _state -> _state := false;
        repair: not _state -> _state := true;
    assertion
        output := if _state then input else false;
end
```

```
block Artefact
    Component a,d,e (lambda = 1.0e-6);
    Component b,c;
    observer Boolean oOut = e.output;

    parameter Real lambdaCCF = 1.0e-6;
    event CCF (delay = exponential(lambdaCCF));
    transition
        CCF: ?b.failure & ?c.failure;

    assertion
        a.input := true;
        b.input := a.output;
        c.input := b.output;
        d.input := a.output;
        e.input := c.output or d.output;
end
```

Langage de modélisation AltaRica 3.0 – Définition formelle

Un GTS est un uplet <V,E,T,A,i> tel que :

- V est un ensemble de variables (V = S Ů F)
- E est un ensemble d'événements
- T est un ensemble de transitions, i.e. de triplets <e,G,P> où e est une événement, G est une expression Booléenne sur V (garde) et P est une instruction sur les variables de S.
- A est une assertion, i.e. une instruction sur les variables de F.
- i est l'affectation initiale des variables de V.

L'ensemble des instructions est le plus petit ensemble tel que :

- 'skip' est une instruction
- Si 'v' est une variable et 'E' une expression, alors 'v := E' est une instruction
- Si 'C' est une expression (Booléenne) et 'I' une instruction, alors 'if C then I' est une instruction
- Si 'I_1' et 'I_2' sont des instructions alors 'I_1 ; I_2' est une instruction.

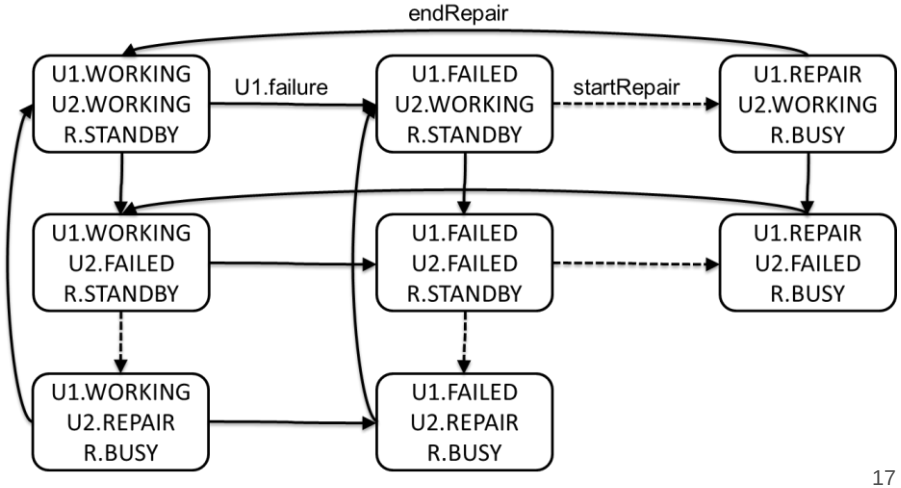
Langage de modélisation AltaRica 3.0 – Sémantique

Règles d'inférence pour les instructions (extrait)

S0: $\dfrac{}{\langle skip, \sigma, \tau\rangle \longrightarrow \tau}$	
S1: $\dfrac{\tau(v) = ?,\ \ \sigma(E) \in dom(v)}{\langle v \coloneqq E, \sigma, \tau\rangle \longrightarrow \tau[\sigma(E)/v]}$	S2: $\dfrac{\tau(v) = \ \sigma(E),\ \ \sigma(E) \in dom(v)}{\langle v \coloneqq E, \sigma, \tau\rangle \longrightarrow \tau}$
S3: $\dfrac{\sigma(E) = ERROR\ \ or\ \ \sigma(E) \notin dom(v)\ \ or\ \ \tau(v) \neq ?,\ \ \sigma(E) \neq \tau(v)}{\langle v \coloneqq E, \sigma, \tau\rangle \longrightarrow ERROR}$	
...	

GTS sont des représentations implicites de structures de Kripke

- Nœuds du graphe sont labélisés par des affectations des variables V
- Arcs du graphe sont labélisés par les événements

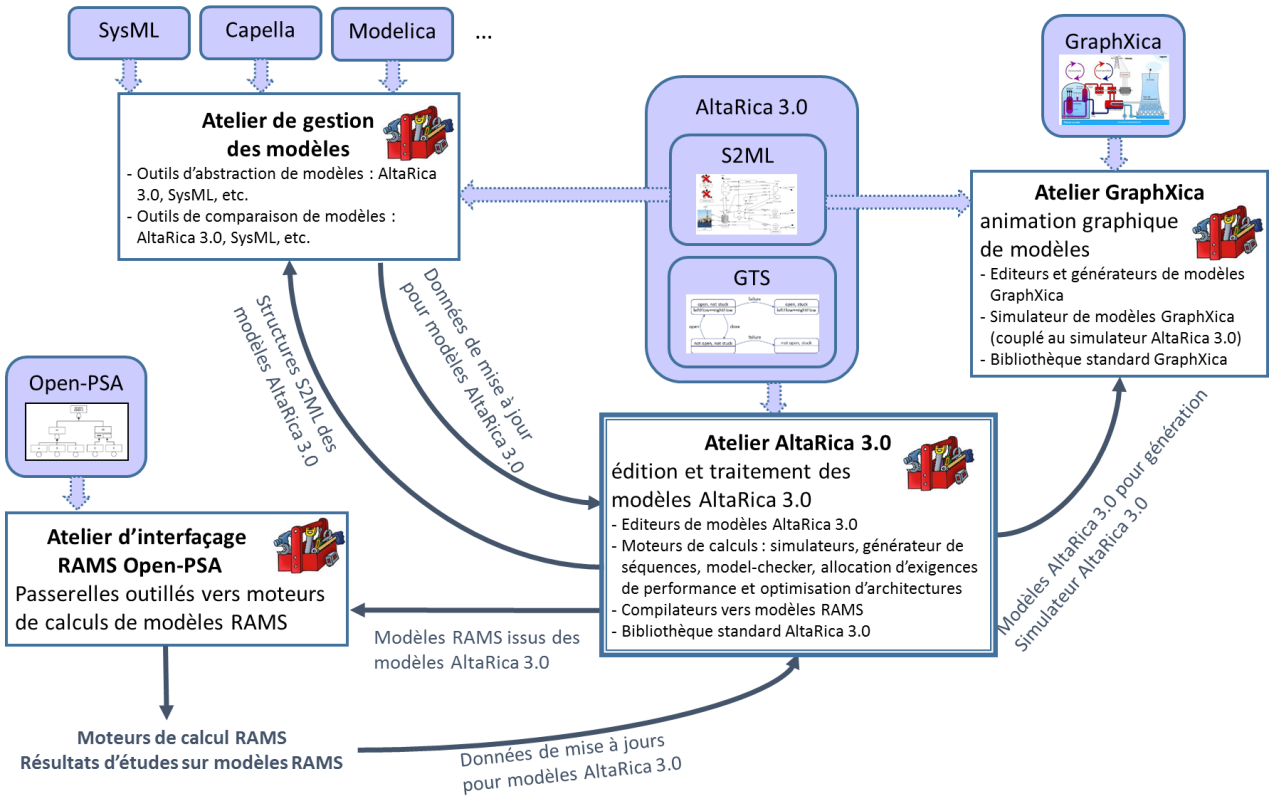


Spécification du langage

www.openaltarica.fr – partie 'docs & downloads'

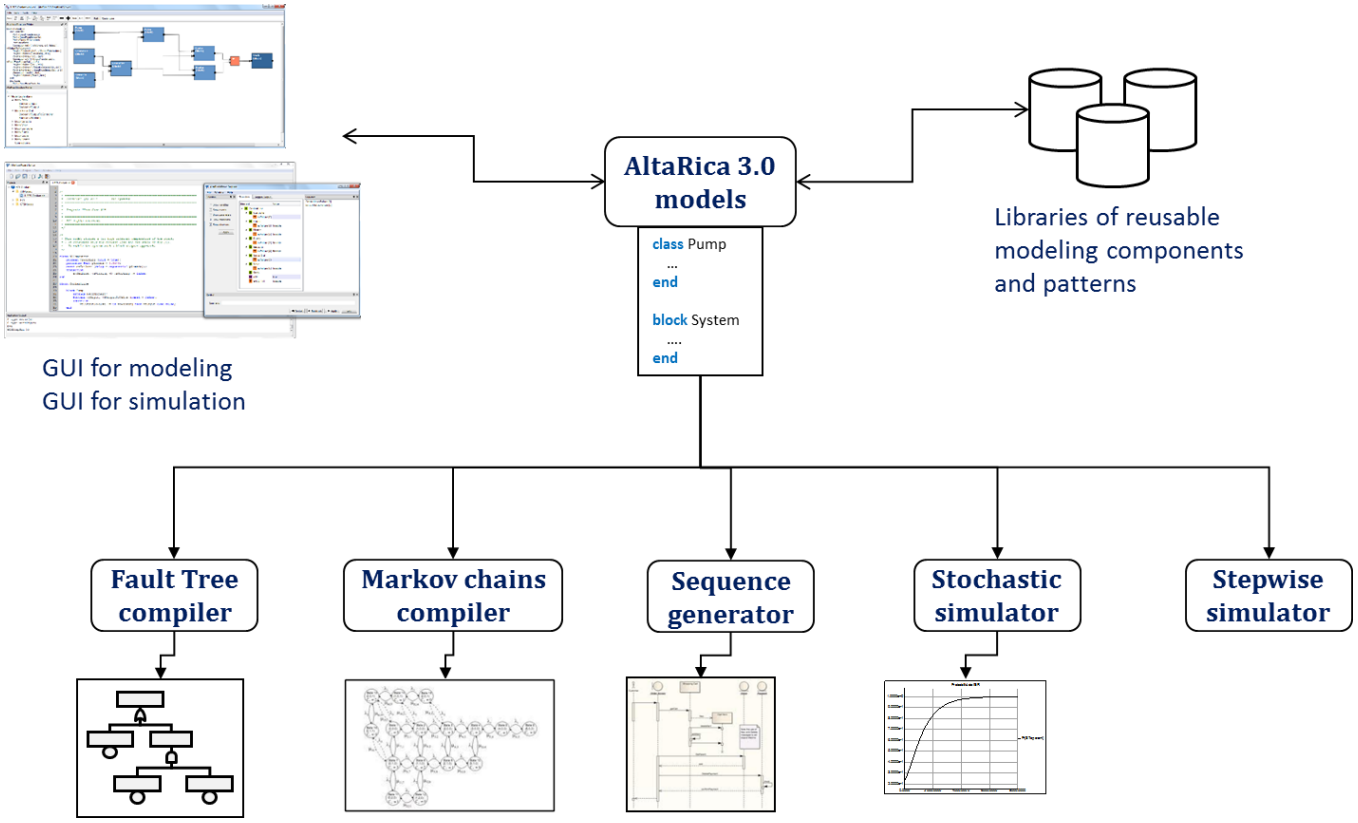
Le projet OpenAltaRica

Développer l'écosystème autour du langage AltaRica 3.0 pour l'analyse du risque de systèmes complexes



Partenaires

Plateforme OpenAltaRica (vision outils)



Téléchargement de la plateforme

www.openaltarica.fr – partie 'docs & downloads'

Démonstrations/Relations/Implications du projet OpenAltaRica

Apport de l'approche AltaRica par rapport à une étude par AdD

Système d'alimentation électrique - chaîne de traitement par arbres de défaillance et par simulation de séquences.

Vérification de propriétés de bon fonctionnement

Système train d'atterrissage d'un avion (commandes, contrôleur, vérins, vannes, capteurs, etc.) - chaîne de traitement par simulation stochastique

Validation amont d'architectures

Régulateur de vitesse intelligent (radar, contrôleur, bus-can) - chaîne de traitement par arbres de défaillance puis synthèse de coupes minimales

Projet SVA - Simulation pour la sécurité du véhicule autonome

Démontrer la sécurité du véhicule autonome. Complexité liée au grand nombre de situations, leur incertitude, les technologies embarquées.

Autres (non diffusables)

Retour vers **nos Systèmes Complexes (Critiques)**

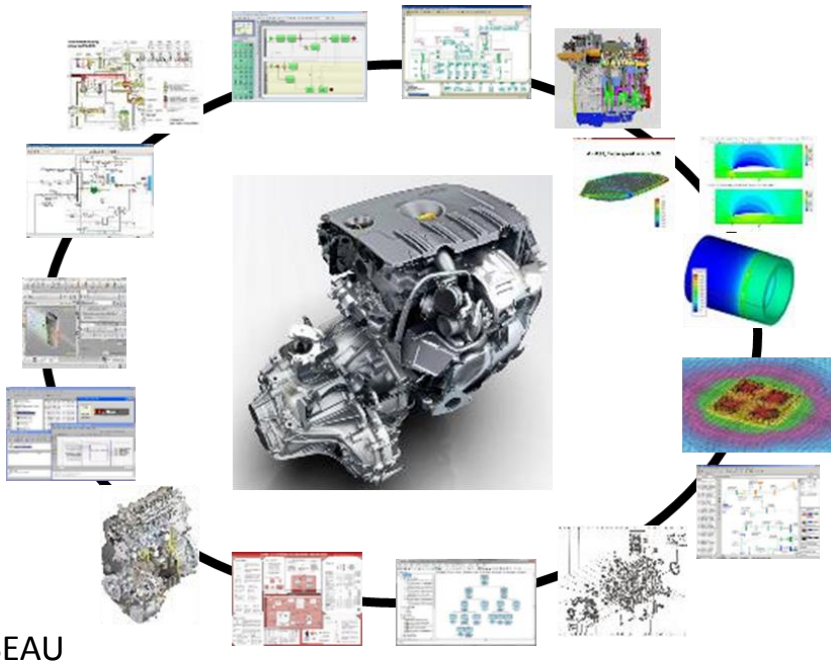
- **Systèmes** conçus par l'industrie sont de plus en plus **complexes** et **interconnectés**.
- Non seulement ces **produits** sont de plus en plus complexes, mais aussi les **processus** associés (qui les **conçoivent**, **produisent**, **opèrent**, **mettent hors service**), mais aussi les **organisations** qui implémentent ces processus.

L'ère de l'Ingénierie Système basée sur les modèles (MBSE)

Les différentes disciplines d'ingénierie (mécanique, hydraulique, électronique, informatique; architecture, etc.) **virtualisent** leurs contenus : **conception de modèles**. Les systèmes sont créés *in virtuo** ou *in silico** avant d'être effectivement réalisés

Tout système matériel et/ou logiciel et/ou humain vient (désormais) avec des centaines (voire des milliers) de modèles.

La science émergente des systèmes complexes est la science des modèles



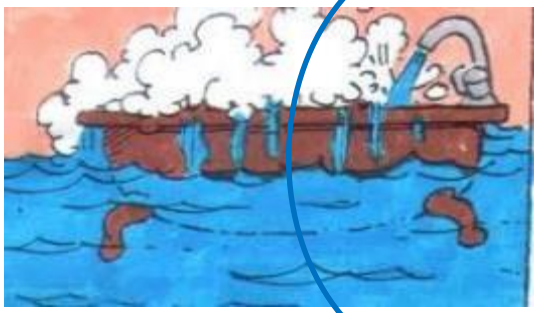
*In vivo, in vitro, in silico, in virtuo - Jacques TISSEAU

L'ère de l'Ingénierie Système basée sur les modèles (MBSE)

- Pour concevoir un modèle, on a besoin d'un **langage de modélisation** (pouvant être graphique) ; comme pour concevoir un programme, on a besoin d'un langage de programmation.
- Les modèles des systèmes complexes ne peuvent être simple, sinon ils ne peuvent capturer la complexité du système (perte d'information). Ils ont donc besoin d'être **structurés**, documentés, diriger ('manager'), etc., i.e. besoin d'une **ingénierie des modèles**

Objectifs spécifiques, modèles spécifiques

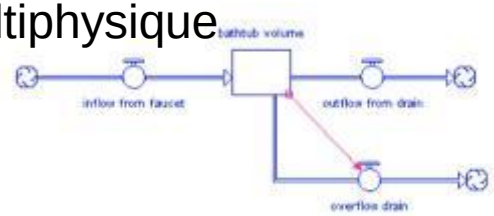
Le **contenu** et le **niveau d'abstraction** d'un modèle dépend de ce que l'on souhaite observer, i.e. les **expériences virtuelles** que l'on souhaite réaliser sur le modèle.



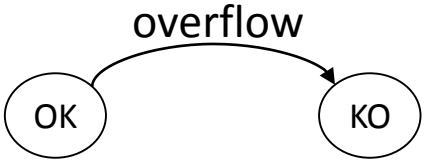
Mécanique de fluides

$$\frac{\partial \vec{v}}{\partial t} + \left(\vec{v} \cdot \vec{\nabla}\right) \vec{v} = -\frac{1}{\rho}\vec{\nabla} p + \nu \nabla^2 \vec{v} + \vec{f}$$

Simulation multiphysique



Sûreté de fonctionnement



Architecture System

Assurance

Region	Premium price (Winter 2013/14)	Premium price (Winter 2014/15)	Percentage decrease year on year
London North West (NW)	£182.04	£149.05	-18.1%
Hereford (HR)	£113.42	£97.57	-14%
London West (W)	£157.24	£135.68	-13.7%
Enfield (EN)	£154.31	£133.61	-13.4%
Manchester (M)	£137.45	£121.22	-11.8%
Cambridge (CB)	£118.16	£104.45	-11.6%
Liverpool (L)	£138.86	£123.41	-11.1%
Southend-on-sea (SS)	£150.17	£133.64	-11%
Harrogate (HG)	£122.63	£109.32	-10.9%
Huddersfield (HD)	£128.56	£114.65	-10.8%

Taxonomie des modèles de l'ingénierie

Les modèles sont conçus à différents niveaux d'abstraction, pour des objectifs/besoins différents et dans différents **formalismes de modélisation**.

Modèles pour communiquer
entre les parties-prenantes

Modèles pour calculer
indicateurs de performance

Modèles pour générer des artefacts (via la génération de code) ou des composants physiques (via la fabrication additive)

Notations standardisées, appelées parfois modèles *semi-formels.*

Modèles formels, qui essentiellement encodent ou organisent (un certain type) des équations mathématiques.

Comportement + Structure = Modèle*

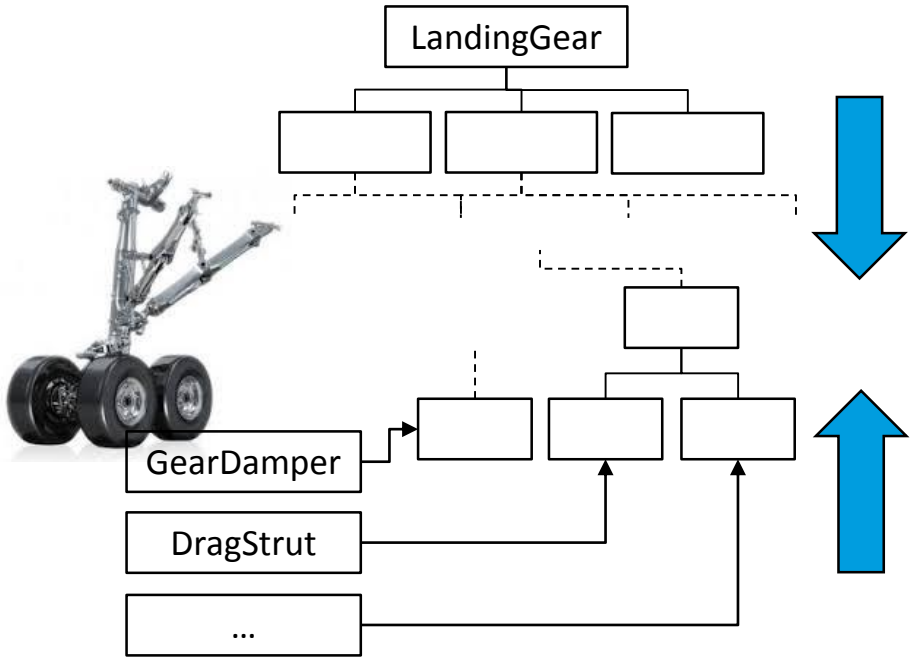
Tout langage de modélisation est la combinaison d'un **cadre mathématique**, pour décrire le comportement du système étudié, et d'un **paradigme de structuration** pour organiser le modèle.

- Le choix du **cadre mathématique approprié** dépend des aspects que l'on souhaite étudier du système.
- Le **paradigme de structuration** est, pour une large part, **indépendant** du cadre mathématique choisi. Il peut donc être considéré en lui-même.

* En référence au livre de Niklaus Wirth : « Algorithms + Data Structures = Programs »

S2ML : System Structure Modeling Language

- Un **paradigme de structuration** qui unifie les deux paradigmes (de structuration) dominants des langages de modélisation, i.e. l'**orienté objet** et l'**orienté prototype**.
- Un **langage de modélisation**, en lui-même, dédié aux descriptions d'architectures (des systèmes).



- Modélisation de « haut en bas »
- Vision au niveau système
- Réutilisation de schémas de modélisation
- Orienté prototype

system architecture

safety

- Modélisation de « bas en haut »
- Vision au niveau composant
- Réutilisation de composants de modélisation
- Orienté objet

MATLAB SIMULINK

MODELICA

Multiphysics simulation

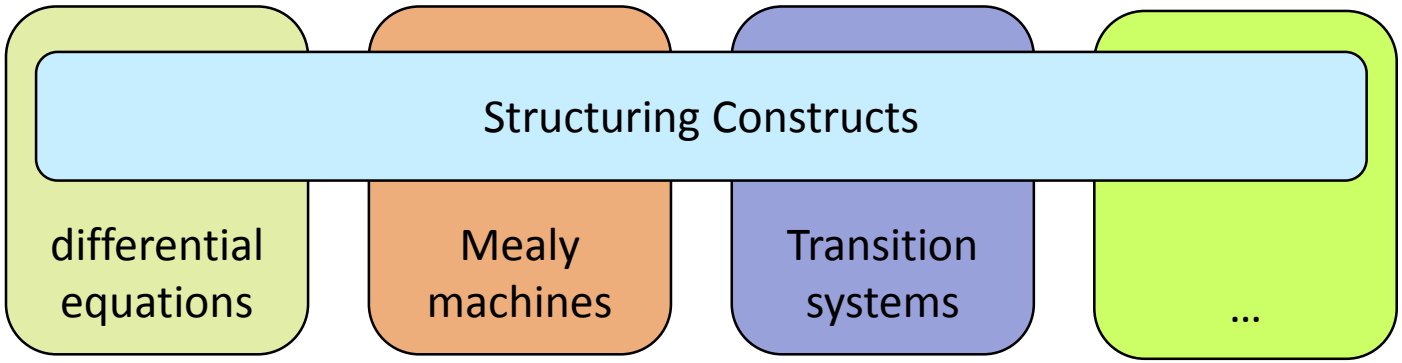
Spécification du langage (v1.0)
https://hal.archives-ouvertes.fr/hal-01234903

Alignement des modèles

Les modèles sont conçus par **différentes équipes**, dans différents langages, à **différents niveaux d'abstraction**, pour **différents objectifs**. Ils ont aussi des **maturités différentes**.

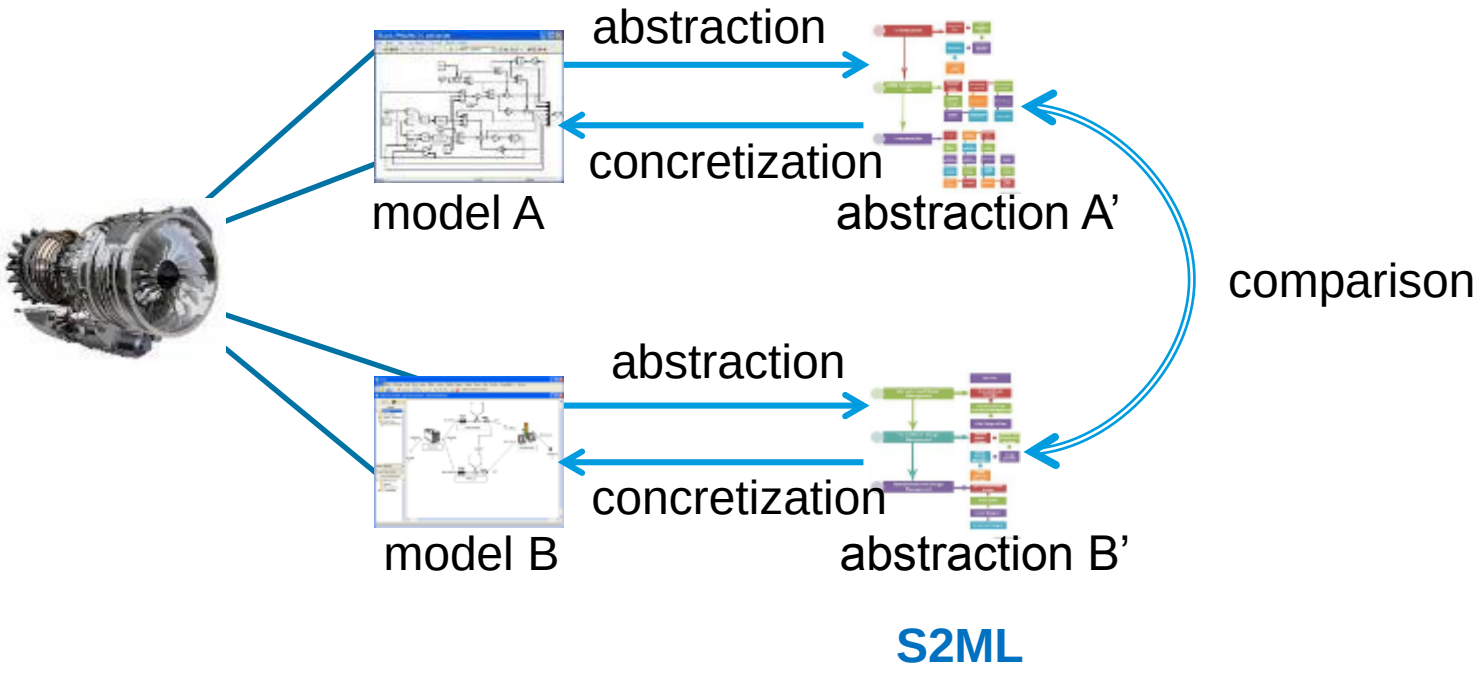
La question est donc comment s'assurer qu'ils parlent du **même systèmes**, i.e. de les **aligner**.

Comme la **partie comportementale** est **dépendante de l'objectif d'étude**, la manière principale pour comparer les modèles est de **comparer leur structure**.

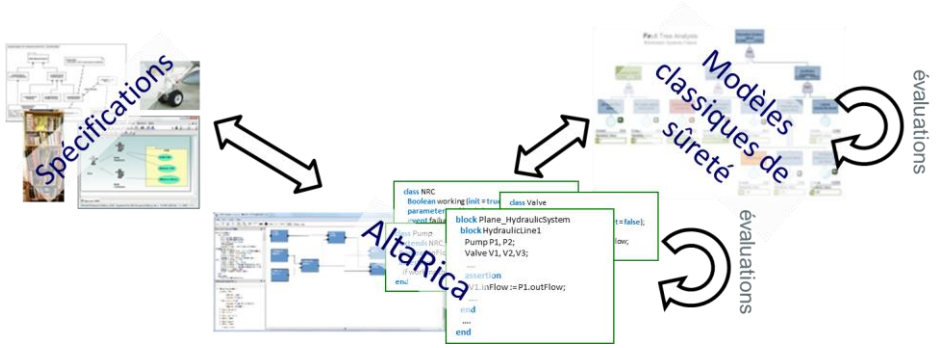


La **structure des modèles** reflète la **structure des systèmes**, même d'un **point de vue limité**…

Abstraction + Comparaison = Synchronisation



MBSA – Model Based Safety Assessment



AltaRica 3.0 = GTS + S2ML

4th International Conference
June 2014, Munich, Germany
5th International Conference
September 2017, Trento, Italy
6th International Conference
June 2018, Paris-Saclay, France

CONTACTS

- **Projet OpenAltaRica**
  www.openaltarica.fr
  contact.oar@irt-systemx.fr

- ***Michel BATTEUX* – IRT SystemX**
  michel.batteux@irt-systemx.fr
- **Antoine RAUZY – NTNU**
  antoine.rauzy@ntnu.no
- **Paolo BALLARINI – CentraleSupélec**
  paolo.ballarini@ecp.fr