FORMOSE

Financé par ANR

FORMOD : un outil d'ingénierie des exigences basé sur la fédération de modèles

Régine Laleau
Université Paris-Est Créteil
laleau@u-pec.fr

Journées du GDR GPL – GT Ingénierie des exigences
Juin 2019

UPEC
UNIVERSITÉ PARIS-EST CRÉTEIL VAL DE MARNE
Connaissance - Action

lacl

Contexte : Projet FORMOSE

Projet ANR 2014-2019

Objectif : Définir une méthode d'ingénierie des exigences pour des systèmes complexes critiques, orientée modèles et formelle, supportée par un environnement open-sour

SysML/KAOS

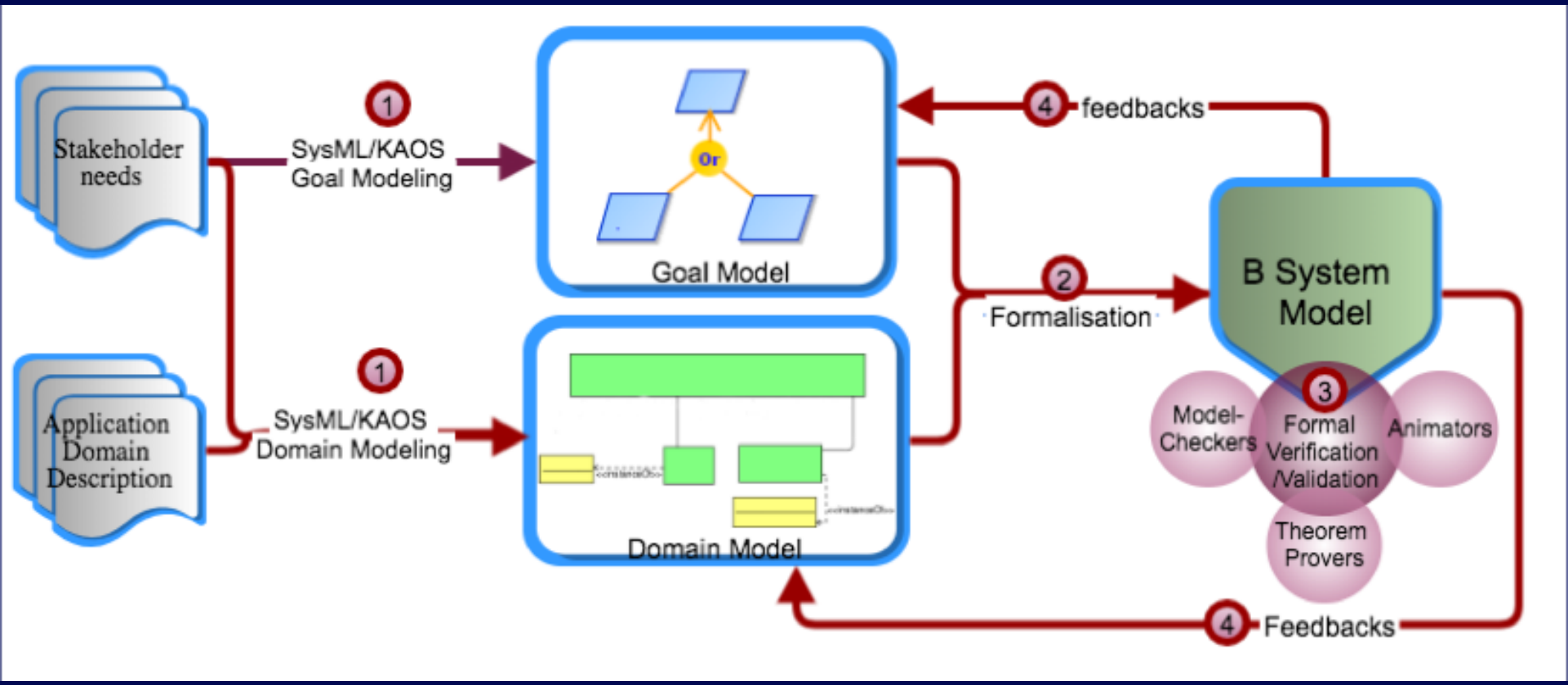
- **Un langage de modélisation :**
  - Exigences fonctionnelles et non-fonctionnelles (sûreté et performance)
  - Modélisation du domaine
  - Multi-vues (langage naturel, graphique et formelle)
- Un framework pour vérifier formellement les exigences : combinaison d'outils formels ***existants*** (prouveurs, model-checkers …)

Domaine d'application : systèmes de transpo

(ferroviai* *que)

Event-B

Aperçu de la méthode FORMOSE



Plan de l'exposé

- Le langage de modélisation des buts SysML/KAOS
- D'un modèle de buts vers un modèle Event-B
- Principes de l'outil FORMOD
- Conclusion

Le langage de modélisation des buts SysML/KAOS

Modèle de buts de SysML/KAOS :

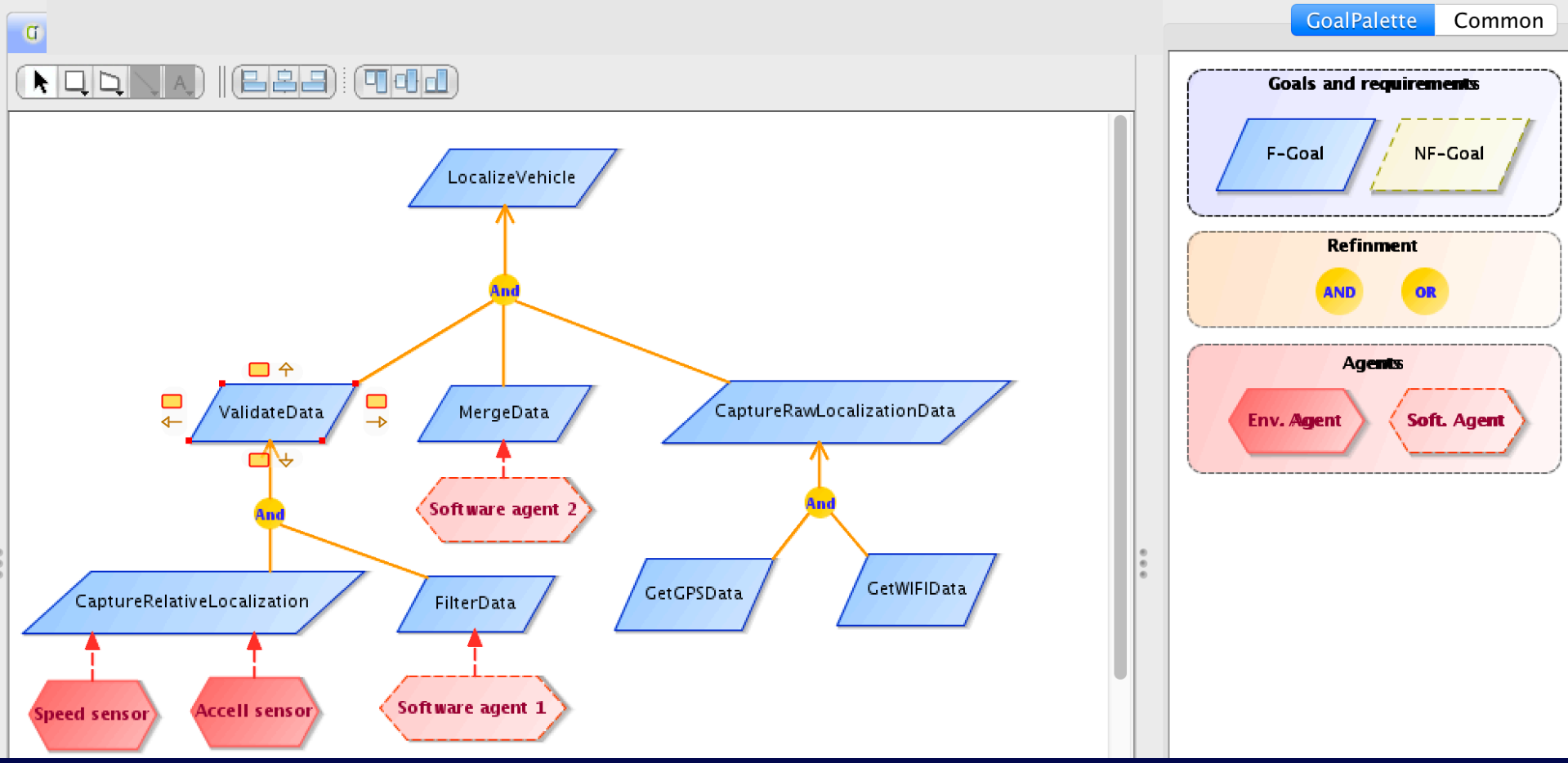
- Défini comme une extension du modèle d'exigences de SysML avec des concepts de la méthode KAOS.
- Hiérarchie de raffinements AND/OR

But AND-refined : tous les sous-buts doivent être satisfaits pour que le but parent le soit

But OR-refined : satisfaction d'un des sous-buts suffisant pour la satisfaction du but parent

Le processus de raffinement cesse quand chaque sous-but est assignable à un agent

Exemple : modèle de buts d'un composant de localisation



Event – B : concepts de base

Modélisation d'un système :

- **Un ensemble de variables pour décrire l'état**
- **Un ensemble d'événements pour décrire le comportement**

  Event E = SELECT G(v) THEN S(v) END

- **Un processus de raffinement pour la construction incrémentale de la spécification.**

La sémantique des modèles et des raffinements est donnée par des obligations de preuve.

Supporté par des outils industriels (AtelierB, ProB, plateforme Rodin, …)

De SysML/KAOS vers Event-B

Objectif : exprimer un modèle de buts avec Event-B pour utiliser les outils de vérification.

Goal G

If **[G-CurrentCondition]**
Then sooner or later
[G-TargetCondition]

Un but SysML/KAOS:
Une propriété doit être vérifiée

EvG= Select G-Guard
Then G-PostCondition
End

Un but = un événement
Sa propriété = post-condition

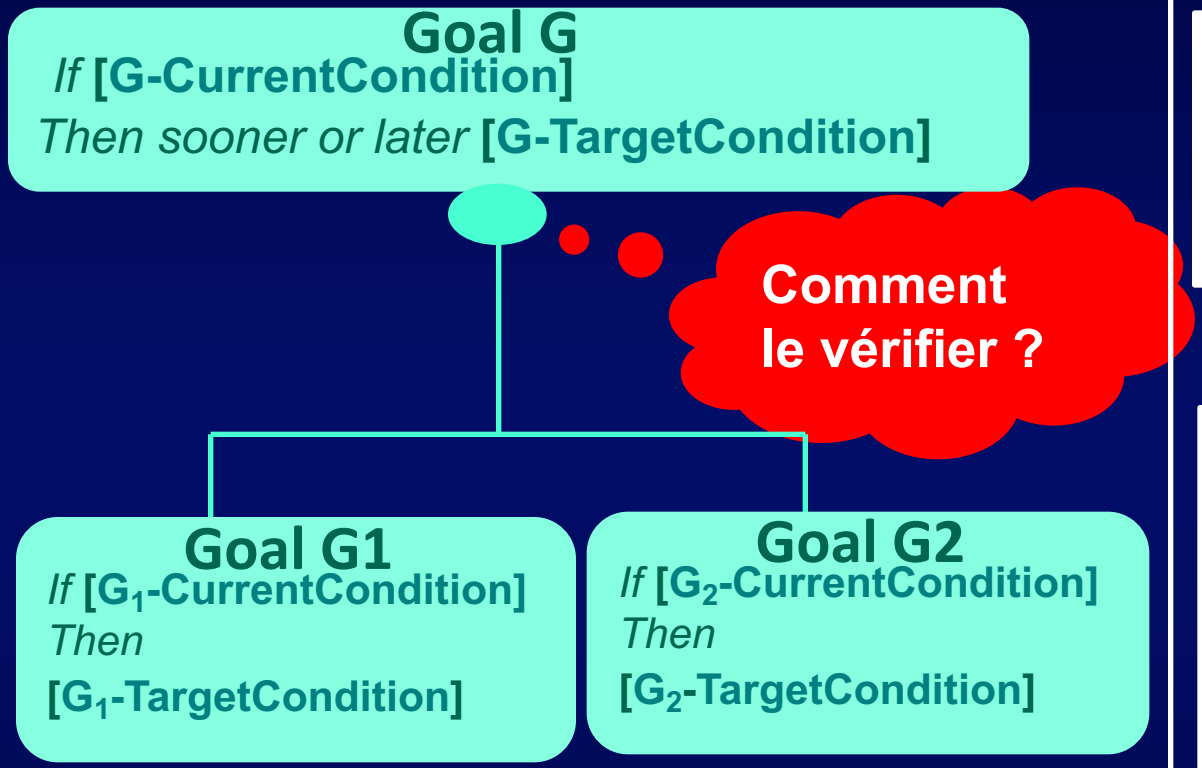
Exemple: composant localisation – événement abstrait

Goal G: LocalizeVehicle
InformalDef: The Cycab/vehicle must be localized.

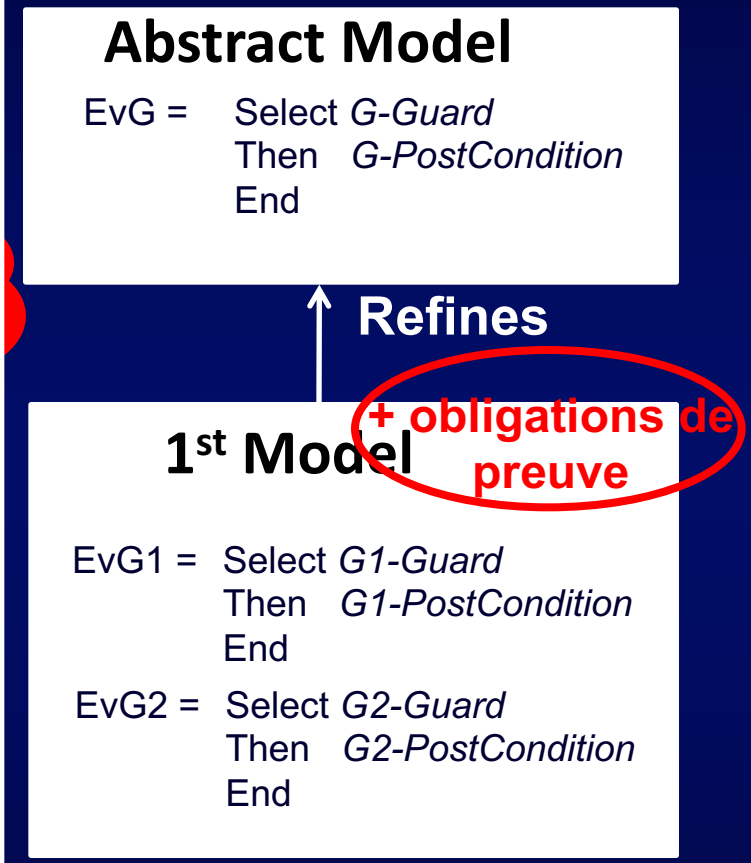
```
SYSTEM  R1_skeleton
SEES       …
VARIABLES …
INVARIANT …
INITIALISATION …

EVENTS
            LocalizeVehicle =
              Select Grd_LocalizeVehicle
              Then Act_LocalizeVehicle    //The Cycab/vehicle must be localized.
END
```

Hiérarchie de buts et raffinement Event-B



Modèle de buts SysML/KAOS



Modèle Event-B

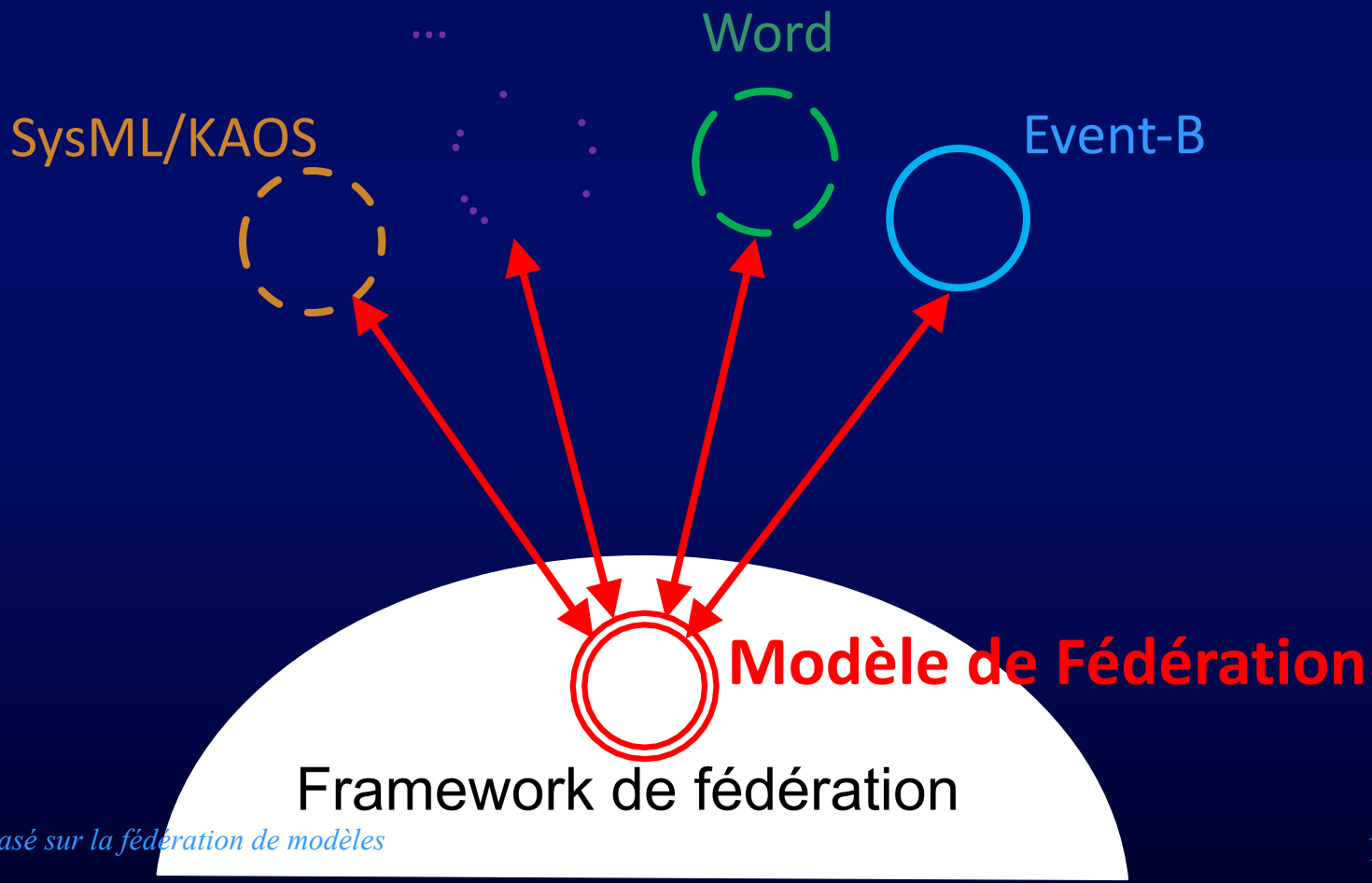
Ce que j'ai présenté …

- **Modélisation des exigences fonctionnelles avec un modèle de buts SysML/KAOS**

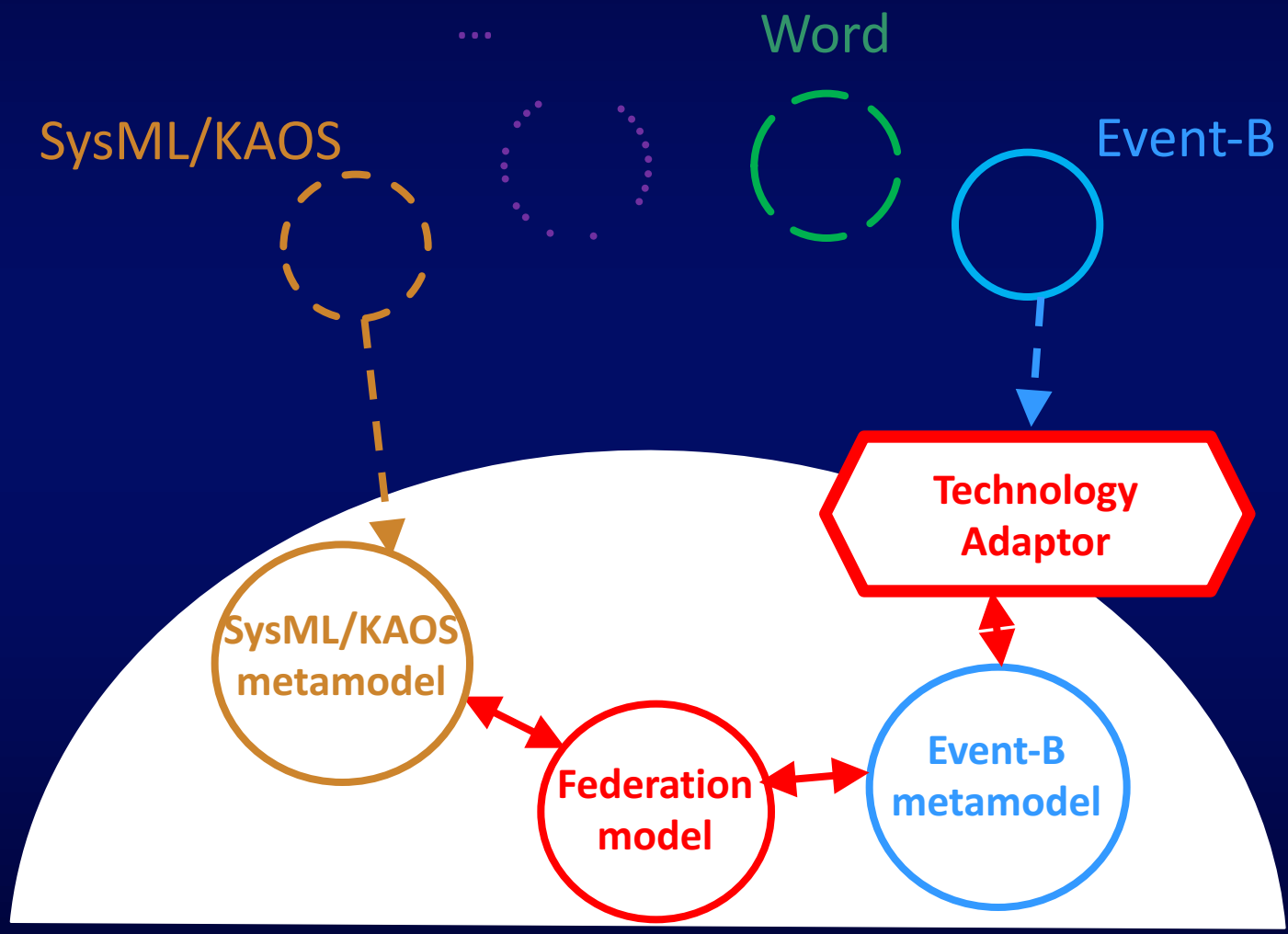
- **Représentation avec un modèle Event-B**

Fédération de modèles

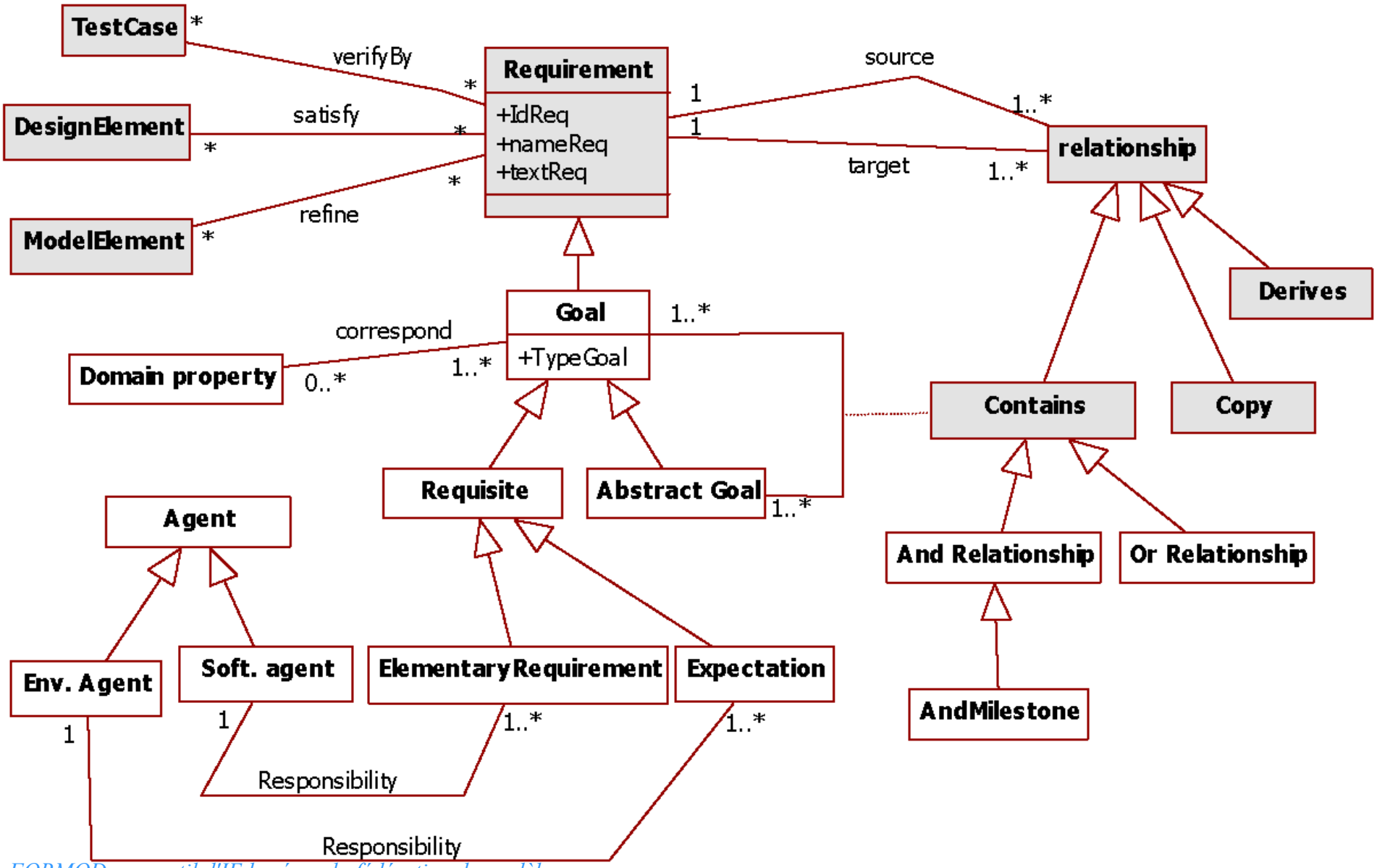
Intégration de modèles hérérogènes en les conservant dans leur paradigme respectif pour faciliter leur synchronisation et éviter les redondances.



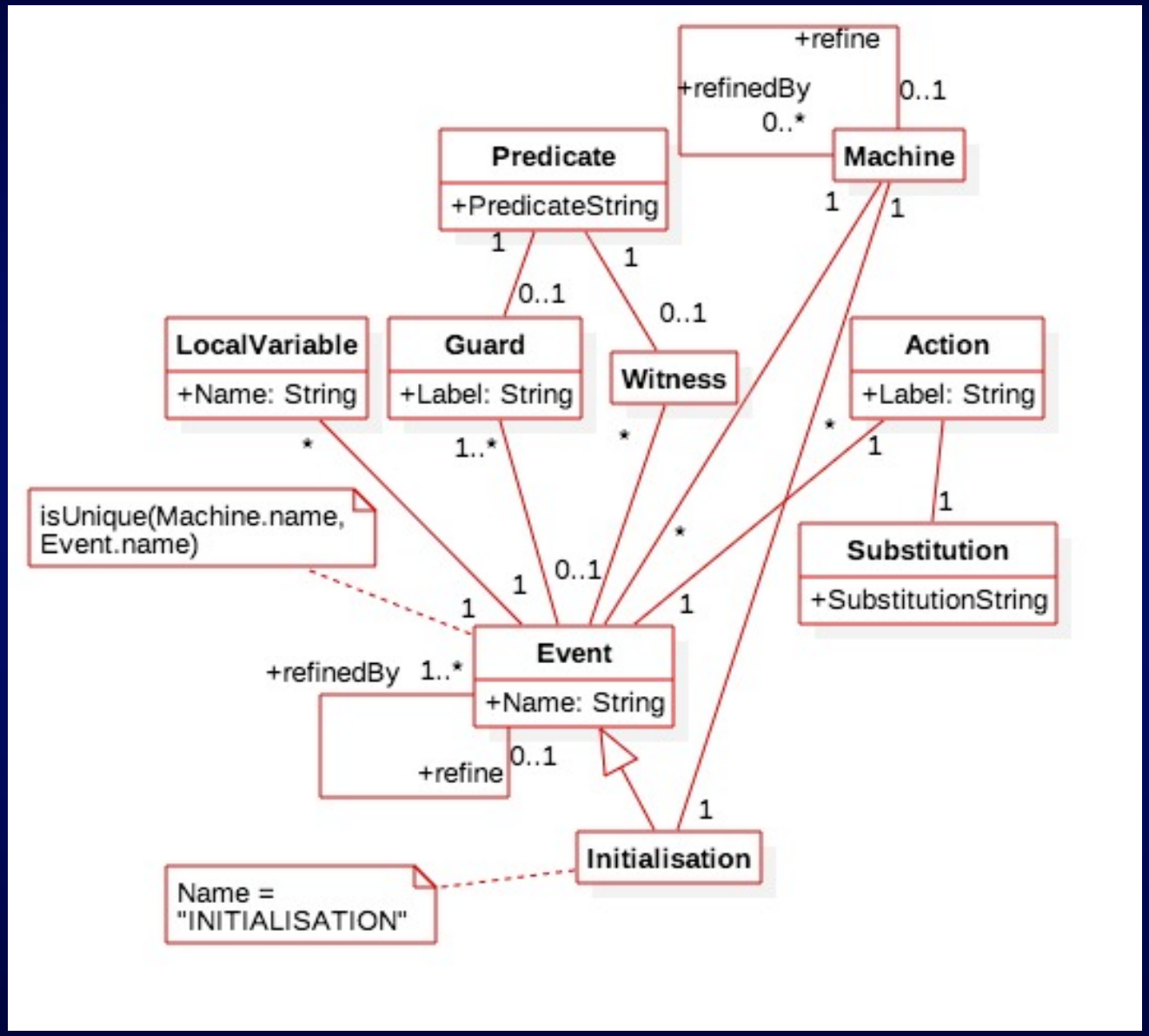
Framework de fédération



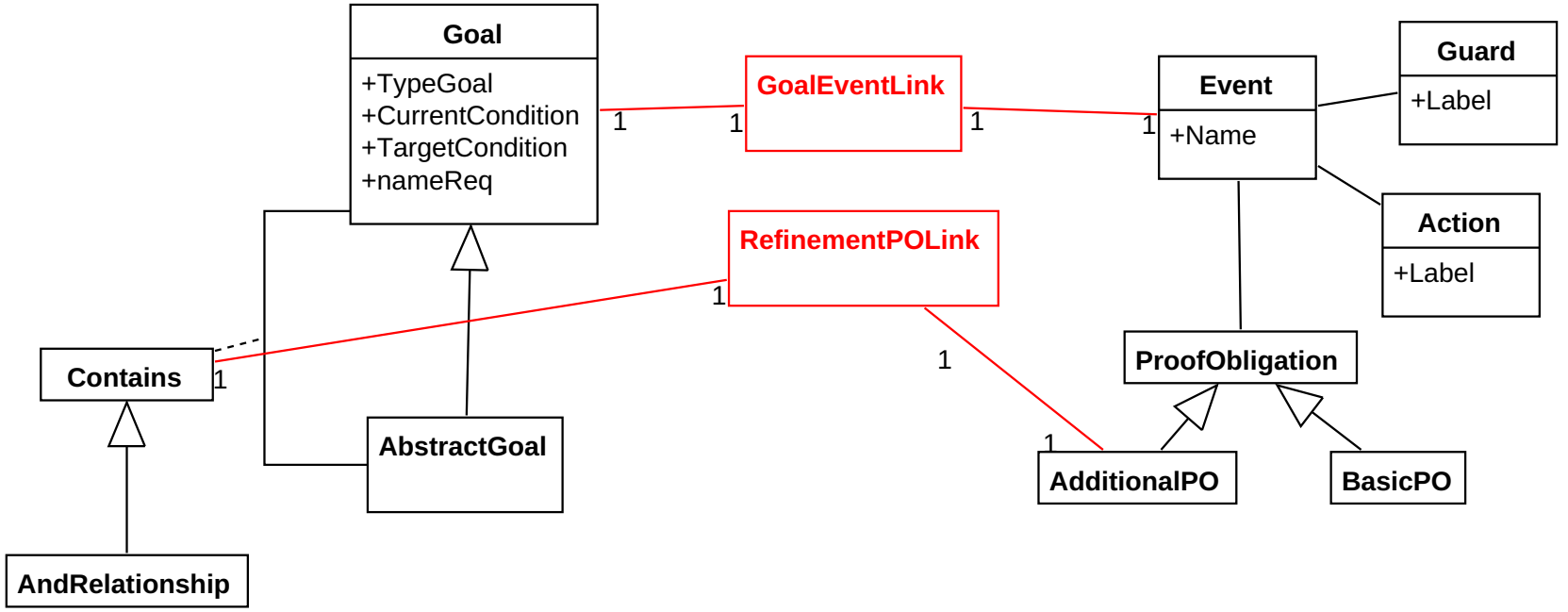
Meta-modèle SysML/KAOS (extrait)



Meta-modèle Event-B (extrait)



Modèle de Fédération



Principe de la fédération

- Des procédures de **Synchronisation** sont définies dans les classes du modèle de fédération et des meta-modèles de **SysML/KAOS** et **Event-B**.

- Une **modification** dans le modèle de **buts déclenche** une méthode dans le **modèle de fédération** qui va entraîner une **mise à jour** dans la spécification **Event-B**, et réciproquement.

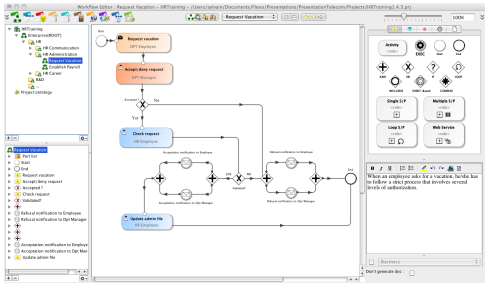
Outil Openflexo

Editing / Viewing Tool 1

Editing / Viewing Tool 2

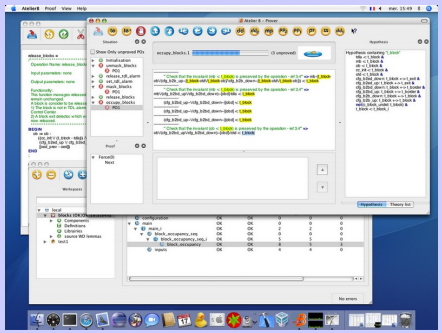
Editing / Viewing Tool 3

OpenFlexo

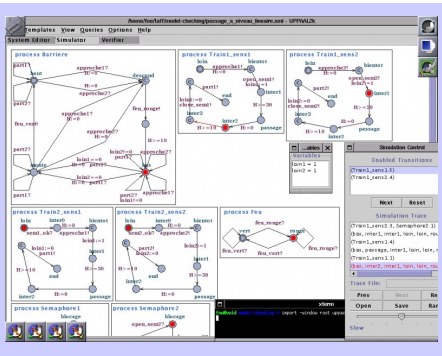


Choreography guided by the process

Any other needed tool
Word, Doors, etc.



Atelier B



UPPAAL

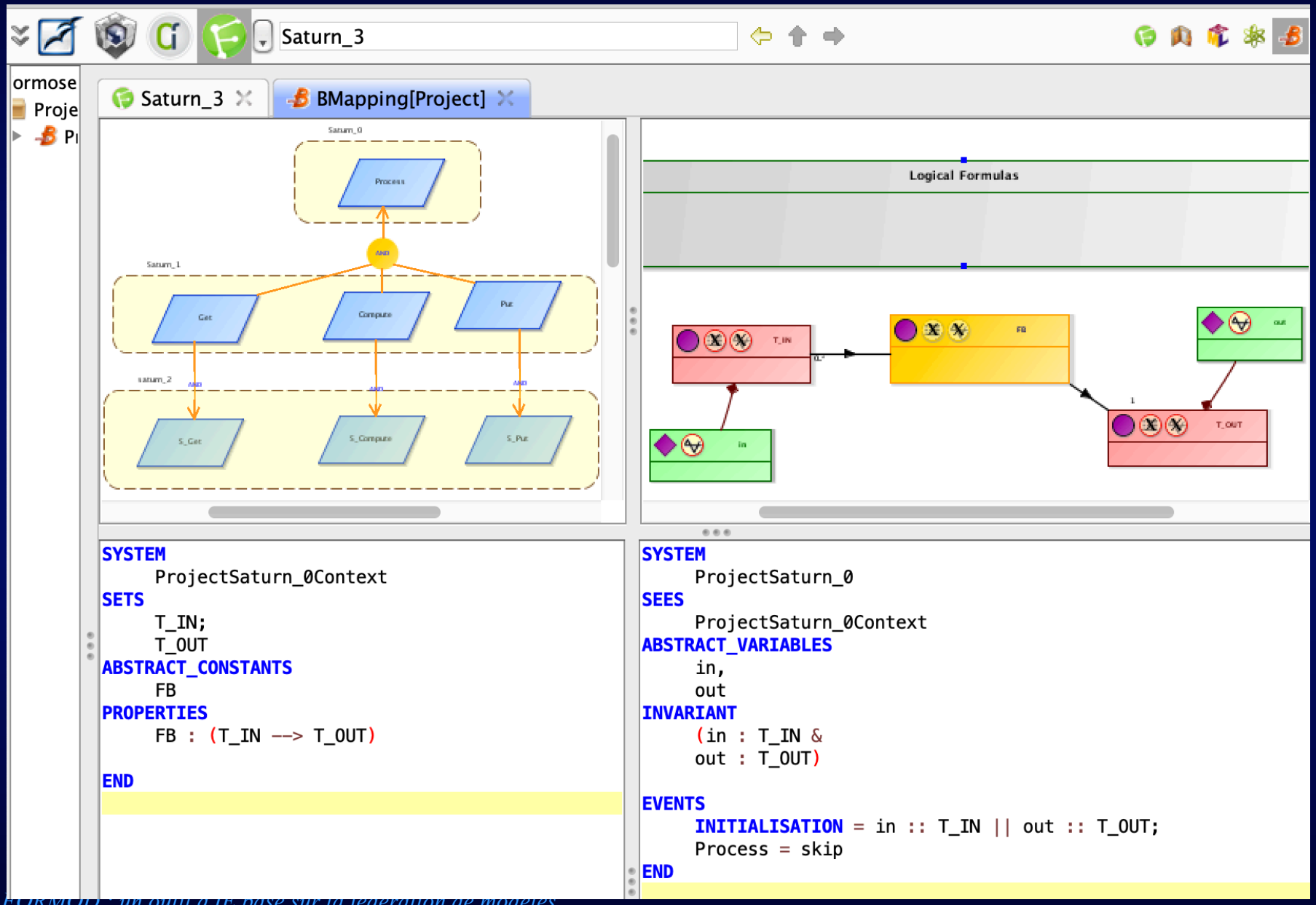
Internal tools developed with OpenFlexo

External tools

Internal connection through the OpenFlexo operational model

External connection, either by ad hoc plugin or web service

Outil FORMOD



Conclusion

Combiner méthodes formelles et semi-formelles est utile pour les premières phases de conception de systèmes.

Mais, le mettre en application reste encore problématique.

La fédération de modèles peut être une solution mais est plus difficile à implémenter que les autres modèles de combinaisons.

Travaux en cours

- Prendre en compte les exigences non fonctionnelles
- Réutiliser les preuves si les exigences changent ?
- Test sur des études de cas de nos partenaires industriels.
- Lien avec l'architecture des systèmes
- …