Techniques de vérification formelle de propriétés : Contribution à leur intégration dans les processus industriels d'ingénierie logicielle

Soutenance HDR
28 mars 2014

Philippe Dhaussy

Univ. Européenne de Bretagne
Lab-STICC
UMR CNRS 6285
ENSTA-Bretagne, Brest.

philippe.dhaussy@ensta-bretagne.fr

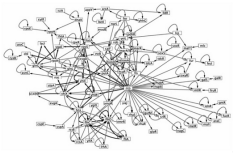
Remerciements

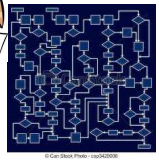
- Merci à **Yamine, Yves, Benoit, Frédéric** et **Antoine** d'avoir accepté leur participation à ce jury.
- Merci à mes nombreux **collègues académiques, industriels, aux membres de l'équipe IDM.**
- Mes travaux n'auraient pu être menés sans leur collaboration.
- Sans oublier **Michèle** et **Annick !**

Mes années 80, le cauchemar des tests manuels…

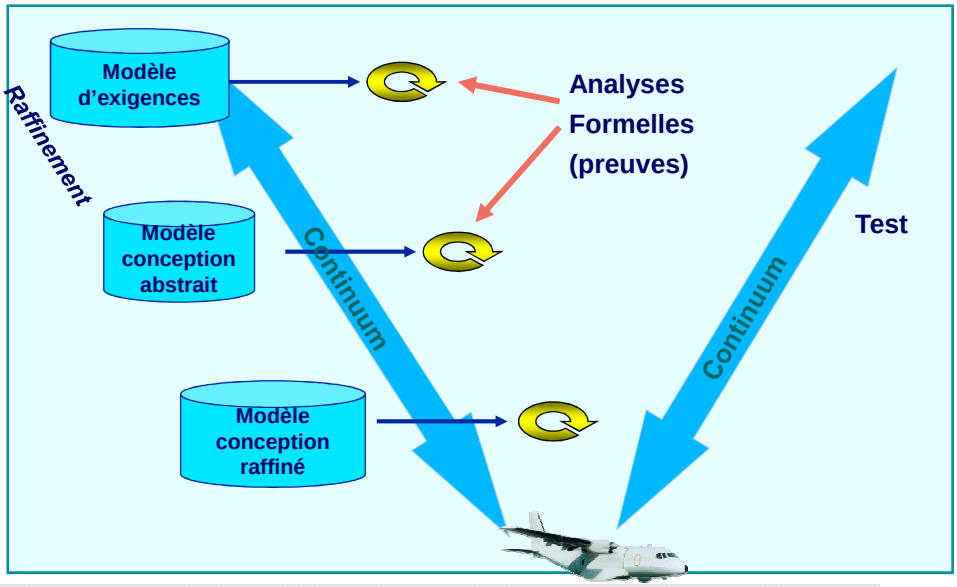
Centre d'archivage CERSAT (Satellite ERS-1)

1milion de lignes de code !

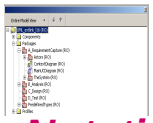




Processus IDM et Analyses Formelles



Enjeux pour les analyses formelles en contexte industriel



Notations

User Models
(UMLx, AADL, SDL, ...)

Exigences

Processus

Comment intégrer des techniques d'analyse formelle dans l'ingénierie des exigences et du logiciel ?

Formalisation des contextes environnementaux et des propriétés
Réduction de l'explosion combinatoire

Techniques, Outils

Model-Checkers

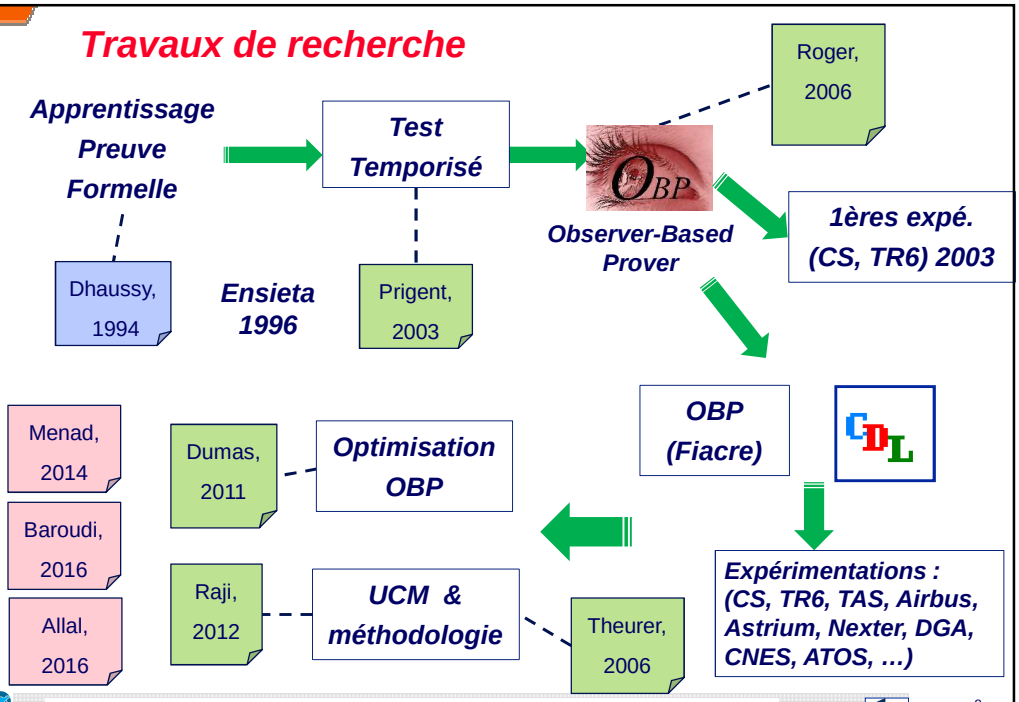
[« *Research Directions in Requirements Engineering* », Cheng & Atlee, FOSE'07]

Requirements Tasks	Requirements Technologies		
	Notations	Methodologies, Strategies, Advice	Techniques, Analyses, Tools
Elicitation	Goals [19, 109, 173] Policies [18] Scenarios [1, 32, 47] Agents [106, 183] Anti-models [157, 166, 174] Nonfunctional requirements [28, 69]	Identifying stakeholders [152] Metaphors [133, 136] Persona [9, 34] Contextual requirements [33, 160] Inventing requirements [117]	Animation [84, 115, 170] Simulation [164] Invariant generation [93]
Modeling	Object models [89] Behavioral models [92, 167] Domain descriptions [11] Property languages [14, 50, 105] Notation Semantics [59, 120, 125, 163]	RE reference model [75, 77, 131] Model elaboration [169] Viewpoints [128, 155] Patterns [49, 54, 90, 99, 171] Modeling facilitators [6, 31, 72, 97, 129] Formalization heuristics [18, 67] Methodologies [15]	Model merging [147, 165] Model synthesis [3, 39, 107, 168, 182] Model composition [80]
Requirements Analysis		Negotiation [87] Aligning requirements with COTS [5, 144] Conflict management [143]	Linguistic analysis [16, 27, 176] Ontologies [95] Checklists [177] Consistency checking [58, 83, 123] Inspections [60, 132] Conflict analysis [25, 79] Obstacle analysis [114, 175] Risk management [62] Impact analysis [101] Causal order analysis [12] Prioritization [122] Variability analysis [74, 108, 110] Requirements selection [139, 159]
Validation & Verification	Model formalisms [22, 51]	???	Simulation [164] Animation [84, 115, 170] Invariant generation [93] Model checking [26, 55, 158] Model satisfiability [89]
Requirements Management	Variability modeling [21, 38, 140, 150]	Scenario management [2] Feature management [179] Global RE [44]	Traceability [30, 81, 146, 151] Stability analysis [23]

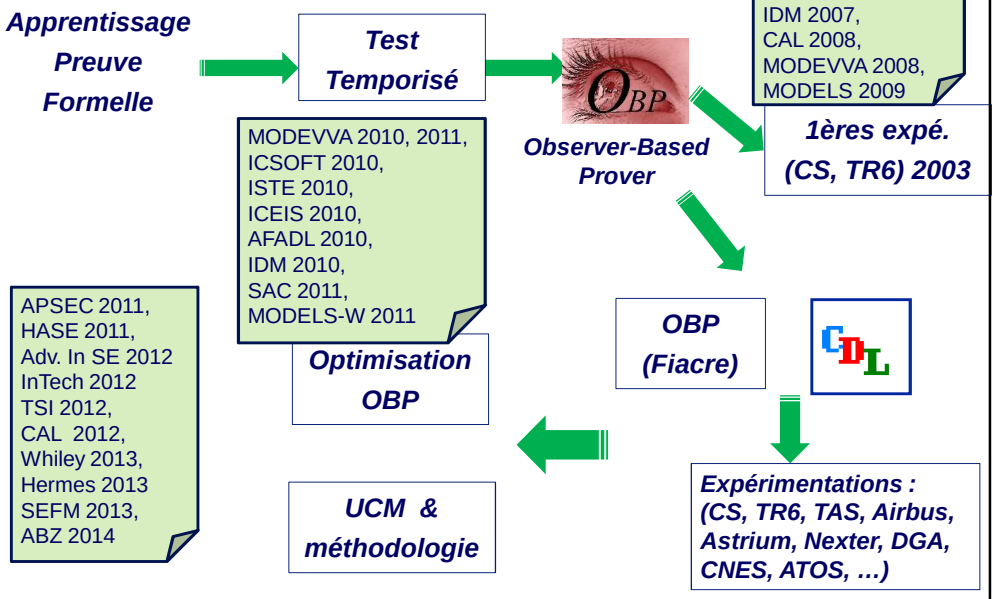
Plan

- Motivations & Synthèse
- Travaux, résultats, retour d'expérience
- Perspectives

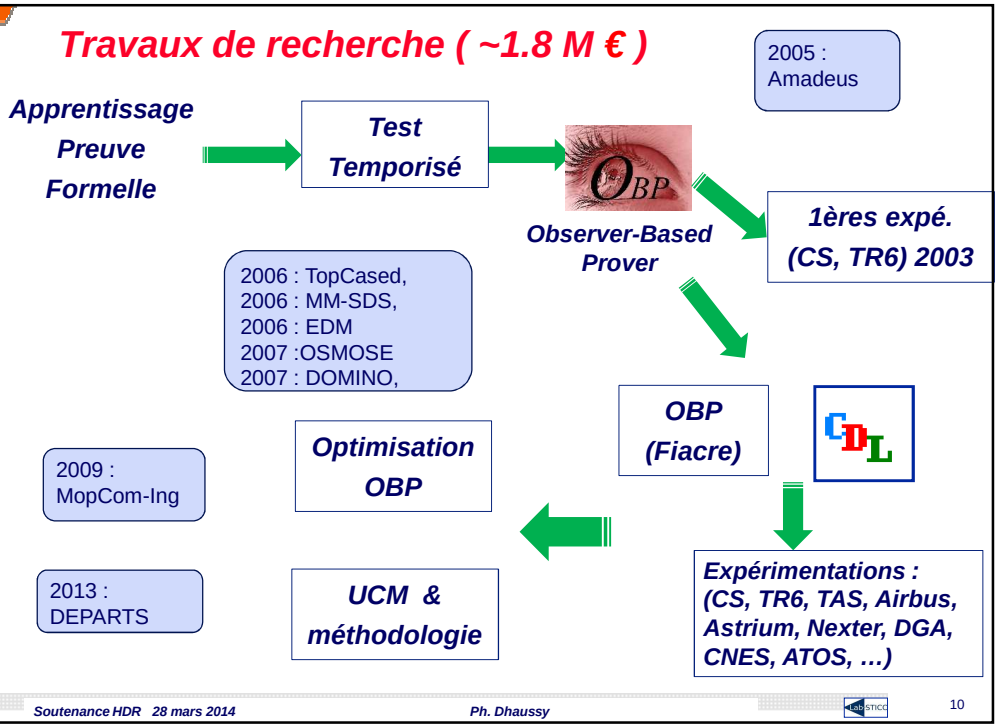
Travaux de recherche



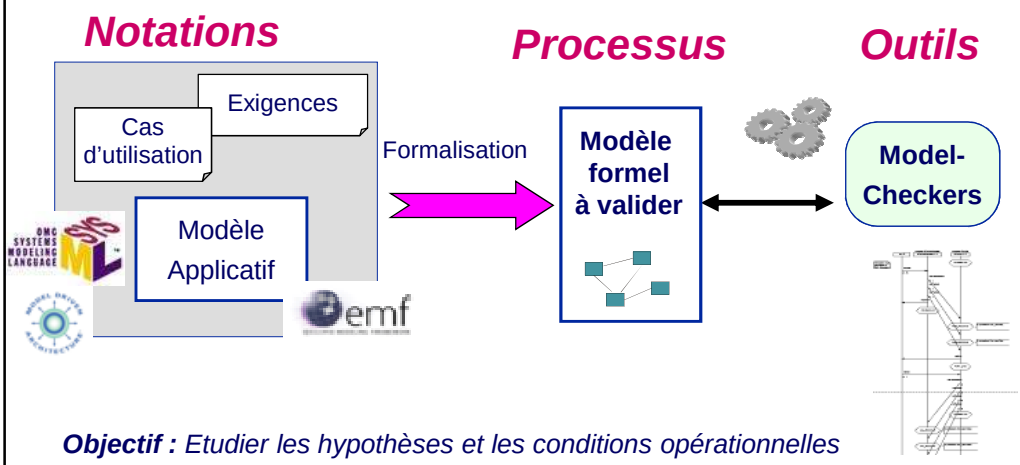
Travaux de recherche



Travaux de recherche (~1.8 M €)



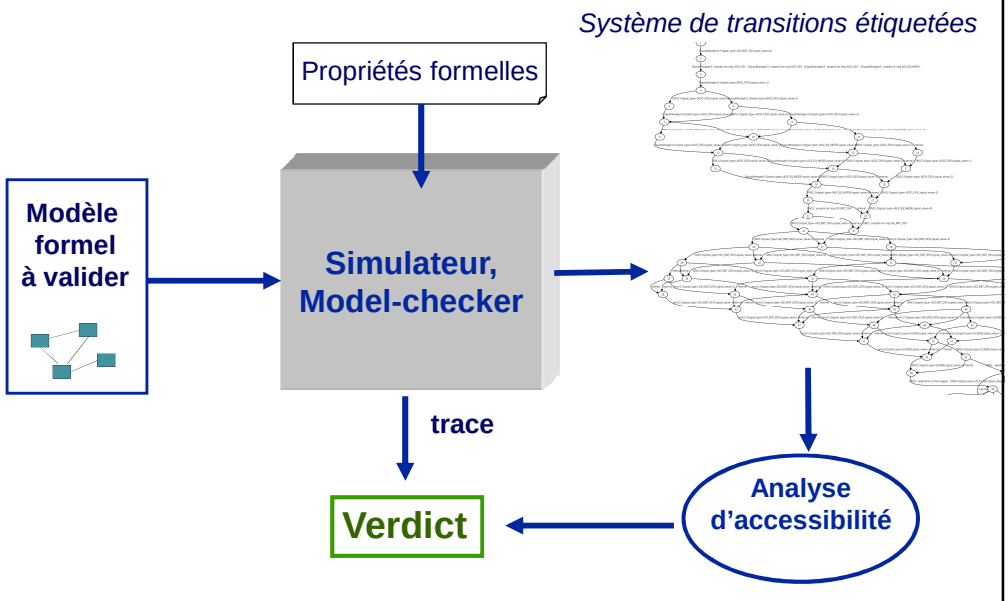
Motivation : Intégration des méthodes formelles dans les processus d'ingéniérie



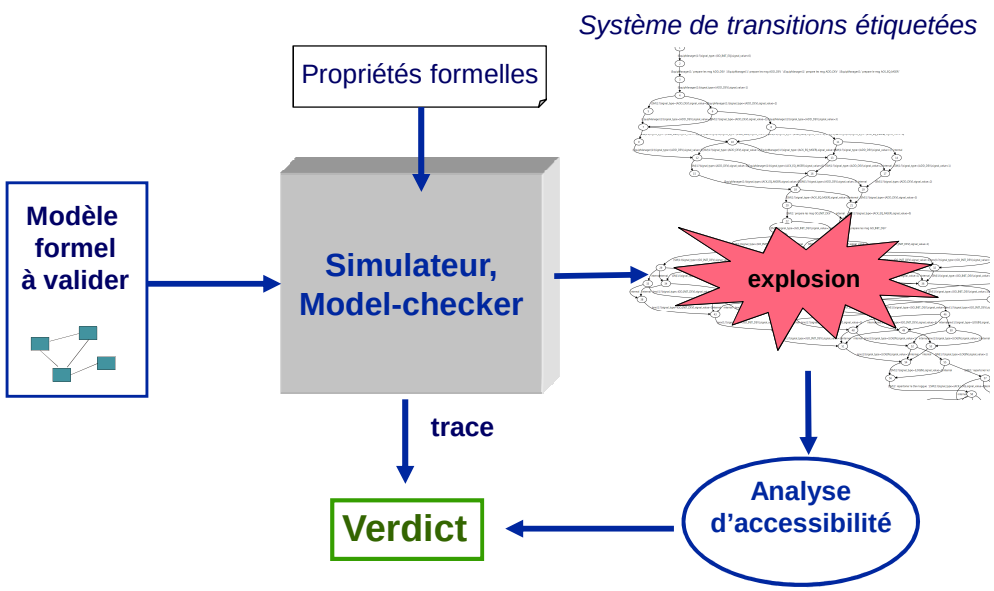
Objectif : *Etudier les hypothèses et les conditions opérationnelles pour rendre possible l'intégration des méthodes dans les processus.*

Disposer de modèles formels pour les outils de vérification

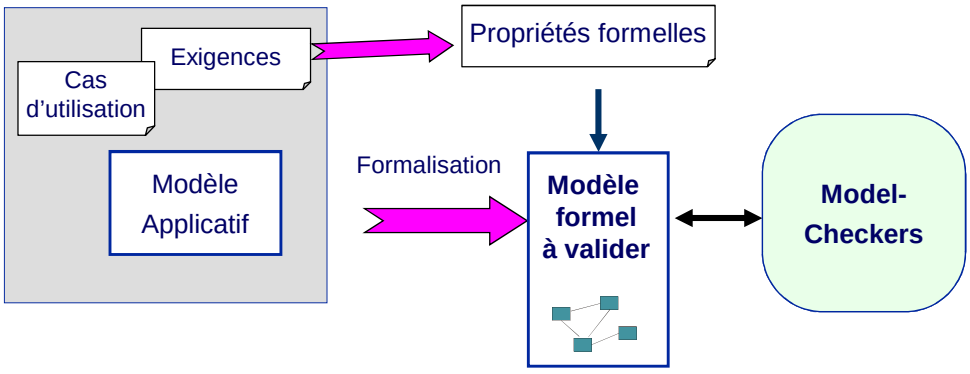
Principe de vérification de propriétés



Principe de vérification de propriétés



Difficulté: formalisation des propriétés



Gap entre le modèle à valider et le modèle formel

Logique temporelle : non adéquat

Difficulté: formalisation des propriétés

SYST-DP-REQ-6

During initialization procedure, the SYST_DP shall associate a generic equipment identifiers to one or several role in the system (MainSensor, OtherSensor, IFF, Actuator, ...). It shall also associate an identifier to each console.
The SYST_DP shall send an evtEquipmentRole message, in preparation mode, for each connected generic equipment, to each connected console.
Initialization procedure shall end successfully, when the SYST_DP has set all the generic equipment identifiers and all console identifiers and all evtEquipmentRole message have been sent.

End

SYST-DP-REQ-8

Once initialization is achieved, the SYST_DP shall send to each console an evtCurrentMission with curMission set to IDLE, to set current mission to idle, followed by an evtCurrentActivity with curActivity to LOGIN and status to TRUE to activate login.

End

Lien : Contexte – propriété

SYST-DP-REQ-6

During initialization procedure, the SYST_DP shall associate a generic equipment identifiers to one or several role in the system (MainSensor, OtherSensor, IFF, Actuator, ...). It shall also associate an identifier to each console.
The SYST_DP shall send an evtEquipmentRole message, in preparation mode, for each connected generic equipment, to each connected console.
Initialization procedure shall end successfully, when the SYST_DP has set all the generic equipment identifiers and all console identifiers and all evtEquipmentRole message have been sent.

End

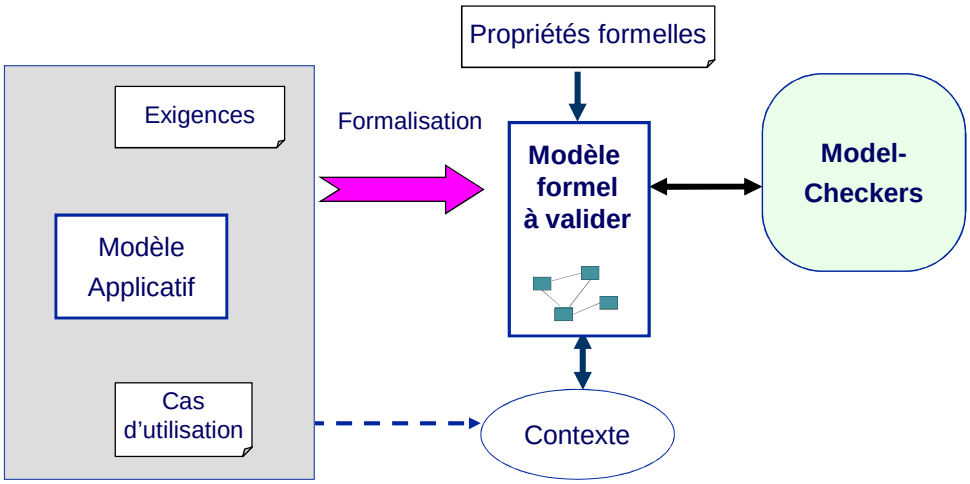
SYST-DP-REQ-8

Once initialization is achieved, the SYST_DP shall send to each console an evtCurrentMission with curMission set to IDLE, to set current mission to idle, followed by an evtCurrentActivity with curActivity to LOGIN and status to TRUE to activate login.

End

Contexte

Lien : Contexte – propriété



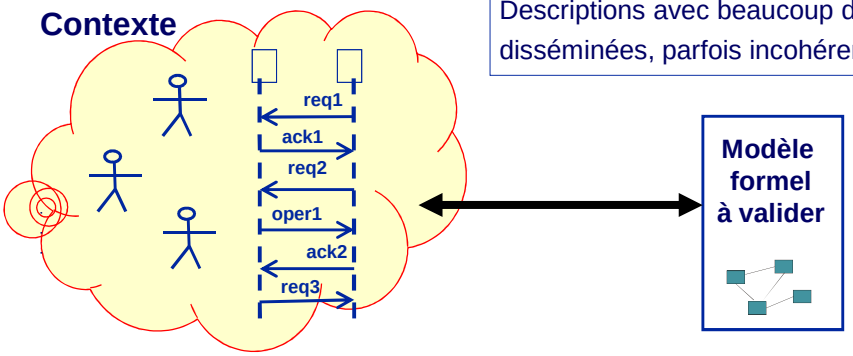
Vérifier les propriétés dans leur contexte

Expression des contextes

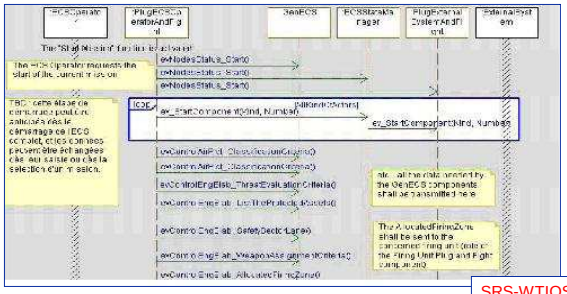
Représentent le comportement de l'environnement (Phases opérationnelles)

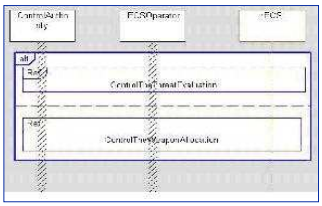
Initialisation, reconfiguration, modes dégradés, scénarios d'erreurs, etc.

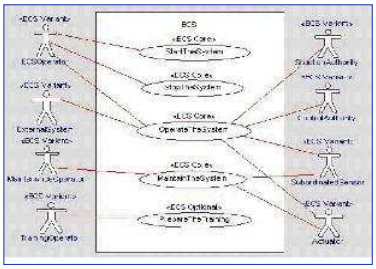
En réalité dans les spécifications :
Descriptions avec beaucoup d'implicite, disséminées, parfois incohérentes



Expression des contextes

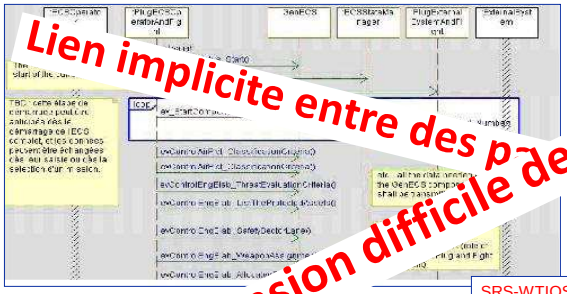


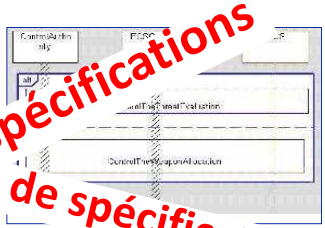


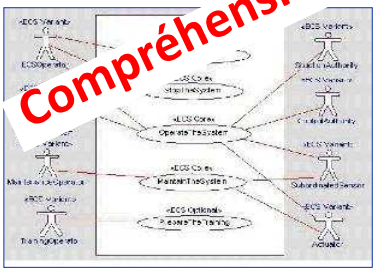


SRS-WTIOS-REQ-004
On receipt of a *MsgFieldMask* message from the COMM_WT, the WT_IOS shall set the WT_State to 'STANDBY' and transmit the *EvtTechnicalStateIos* message to the ECDP_DP with the following parameters:
equipmentId = equipmentId of the WT_IOS
roleId = roleId of the WT_IOS
state = STANDBY
If the requested WT_State is OPERATIONAL, the WT_IOS shall transmit the *MsgControlNetwork* message to the COMM_WT with the following parameters:
orderId
command = 'READY'
End Requirement

Expression des contextes

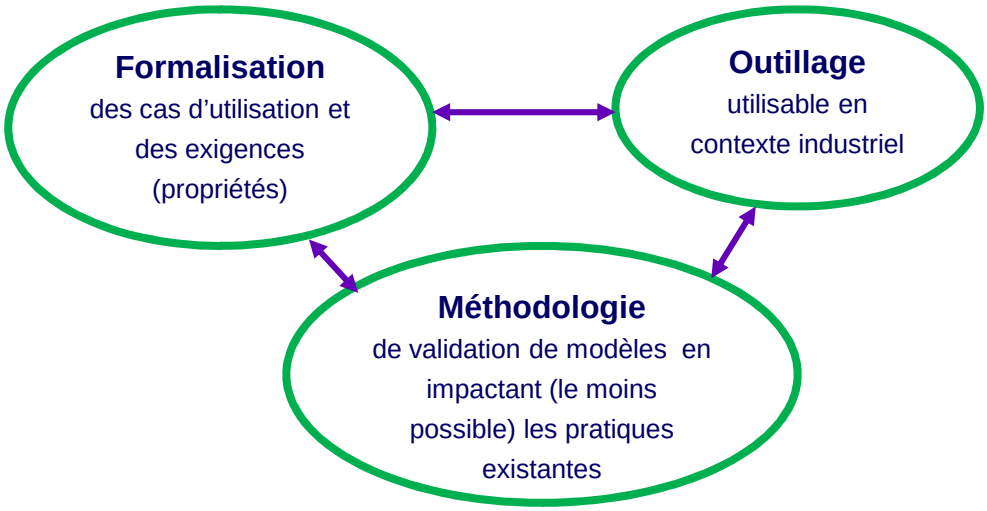






SRS-WTIOS-REQ-004
On receipt of a *MsgFieldMask* message from the COMM_WT, the WT_IOS shall set the WT_State to 'STANDBY' and transmit the *EvtTechnicalStateIos* message to the ECDP_DP with the following parameters:
equipmentId = equipmentId of the WT_IOS
roleId = roleId of the WT_IOS
state = STANDBY
If the requested WT_State is OPERATIONAL, the WT_IOS shall transmit the *MsgControlNetwork* message to the COMM_WT with the following parameters:
orderId
command = 'READY'
End Requirement

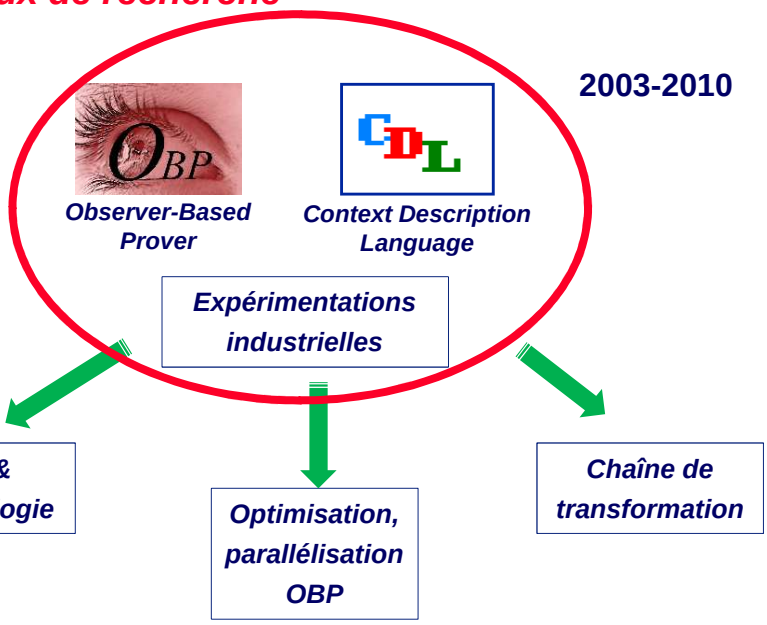
Une approche pragmatique



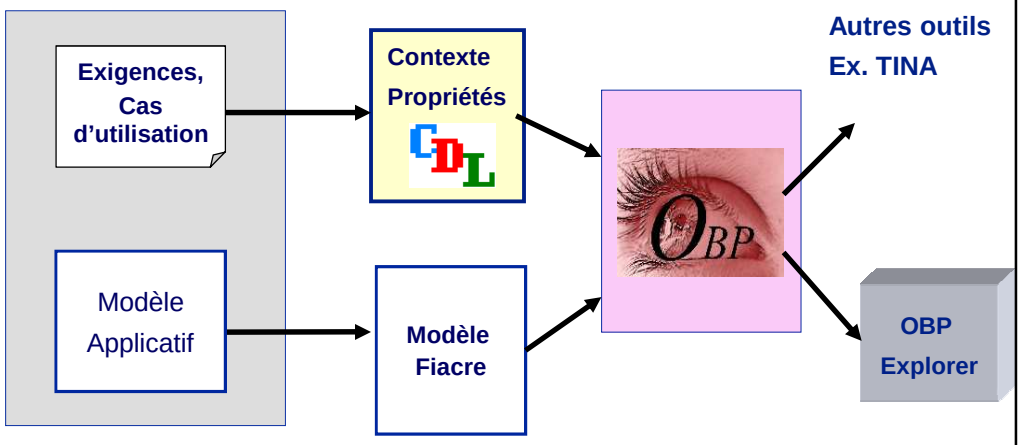
Plan

- Motivations & Synthèse
- Travaux, résultats, retour d'expérience
- Perspectives

Travaux de recherche



L'outillage OBP et le langage CDL



Diffusion : www.obpcdl.org

L'outillage OBP et le langage CDL

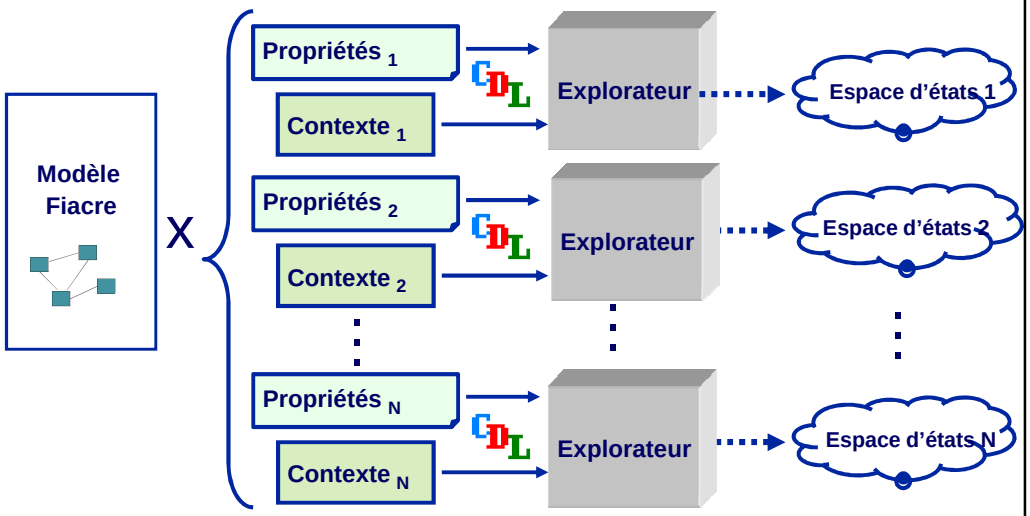
Merci aux nombreux contributeurs !

JC.Roger, F.Boniol, V.Leilde, S.Creff, PY. Pillain, X.Dumas, T. Abdoul, O.Habart, B.Chabibi, Ussef Faghihi, S.Heng, S.De Belloy, M.Fromentin, O.Diallo, E.Landel, T.De Sury, E.Prun, J.Auvray, P.Deschamps, L.Nedelec, V.Treimany, S.Charlet, J.Ventadour, K.May, A.Raji, B.Aizier, L.Leroux, C.Teodorov, …

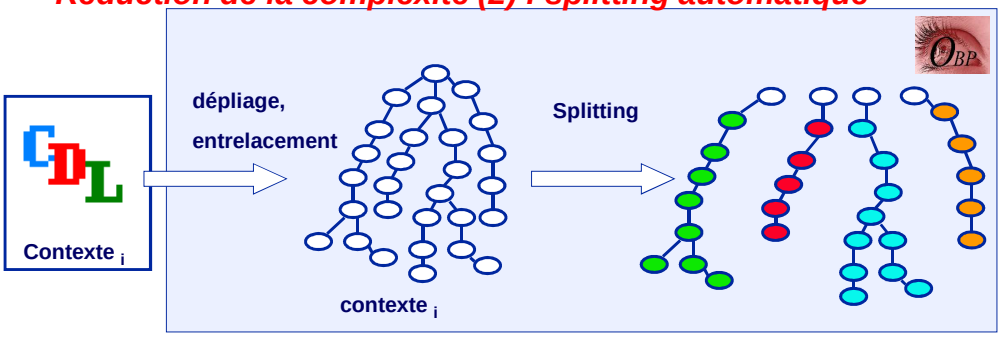
Langage CDL

- ***Gestion des contextes***
- ***Gestion des propriétés***

Réduction de la complexité (1) : Identification des contextes



Réduction de la complexité (2) : splitting automatique



Ensemble de K_i sous-contextes

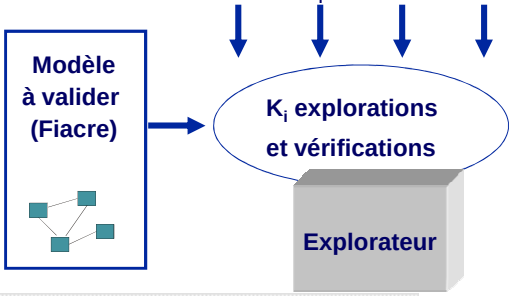
Thèse X. Dumas 2011

(équivalence de chemins)

AFADL 2011

Gestion des arbres :

HASE 2011,
Adv. In SE 2012
InTech 2012
TSI 2012



Exemple de résultats (sans CDL)

N (Number of devices)	Exploration & analyze time (sec)	N.of LTS configurations	N.of LTS transitions
1	1	43 828	321 002
2	4	350 256	2 475 392
3	19	1 466 934	6 430 265
4	[illegible]	–	–

explosion

Configuration mémoire 3 G.O.

Exemple de résultats (avec CDL)

N. of devices	Exploration time (sec)	N. of sub-contexts	N. of LTS config.	N. of LTS trans.
4	954	22	16 450 288	75 362 832
5	1 256	28	33 568 422	156 743 290
6	3 442	242	68 880 326	368 452 864
7	6 480	344	126 450 324	634 382 590
...	...	...	...	...
...	...	...	...	...

Splitting

Langage CDL

- ***Gestion des contextes***
- ***Gestion des propriétés***

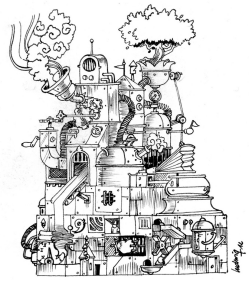
Type et expression des propriétés

Disposer de primitives élémentaires d'observation, à grain fin

- **Invariants :** expression basée sur des prédicats

  Valeur d'une variable, Etat d'un processus, Etat d'une fifo
- **Observateur :** expression basée sur des patrons de définition de propriétés :

  Réponse, Précédence, Absence, Existence



Extension des patrons de Dwyer…

Type et expression des propriétés

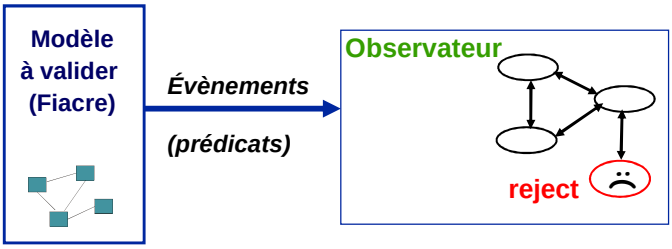
Disposer de primitives élémentaires d'observation, à grain fin

- **Invariants :** expression basée sur des prédicats

  Valeur d'une variable, Etat d'un processus, Etat d'une fifo

- **Observateur :** expression basée sur des patrons de définition de propriétés :

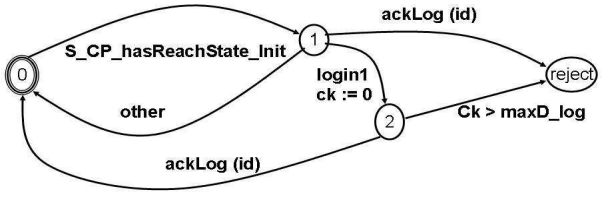
  Réponse, Précédence, Absence, Existence



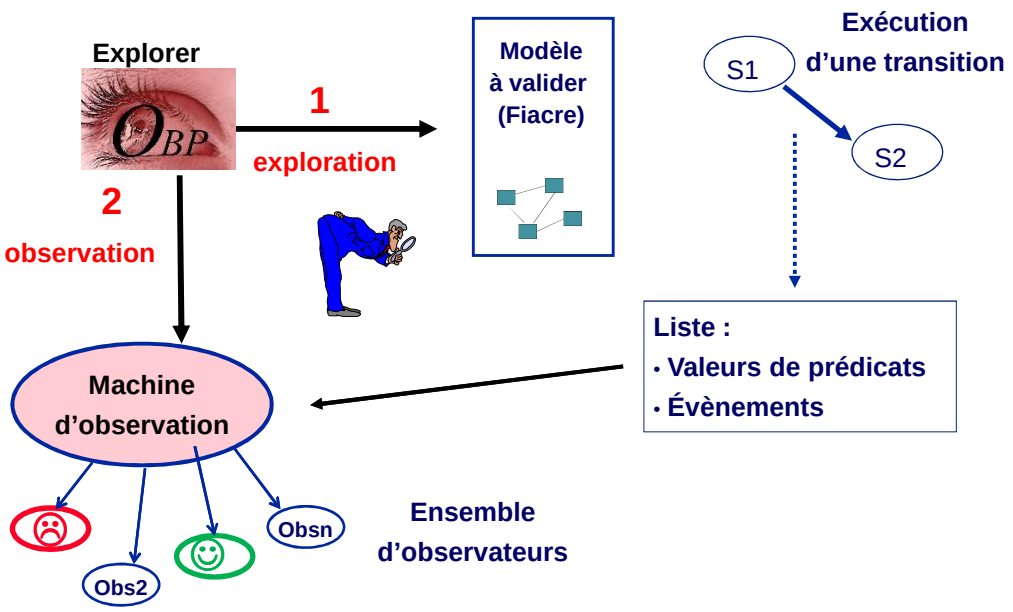
Exemple de patron de définition de propriété (Réponse)

```
Property P;

      ALL Ordered
        exactly one occurrence of S_CP_hasReachState_Init
              exactly one occurrence of login1
      end
eventually  leads-to  [0..maxD_log]
      AN
        one or more occurrence of ackLog (id)
      end

S_CP_hasReachState_Init may never occurs
login1 may never occurs
one of ackLog (id) cannot occur before login1
repeatability: true
```

Transformation automatique



OBP : noyau d'observation



Quelques expérimentations

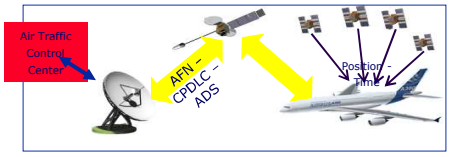
AIRBUS ATOS	**Commandes de vol A380** (SysML)
AIRBUS	**Protocoles ATC - A340, A380** (SDL)
THALES	**Composants logiciels embarqués**(UML)
DGA	**Spécifications fonctionnelles SLAM-F** (NAF)
cnes	**Logiciels de maintenance satellites** (SysML)
Astrium	**Logiciels de bord satellites** (SysML / AADL-Like)
nexter	**Spécifications fonctionnelles système-Logiciel** (SysML)

Pacemaker [Hermes'13, Willey'13], Chalenge **Landing Gear System** [ABZ'14]

Quelques résultats

Nombres de propriétés formalisées avec les patrons de définition

Nombre de propriétés étudiées	Cas 1 (49)	Cas 2 (94)	Cas 3 (136)	Cas 4 (85)	Cas 5 (188)	Cas 6 (151)	Total (703)
Propriétés prouvables	38 (78%)	73 (78%)	72 (53%)	49 (58%)	155 (82%)	41 (27%)	428 (61%)
Non-prouvables	11 (22%)	21 (22%)	64 (47%)	36 (42%)	33 (18%)	110 (73%)	275 (39%)



AIRBUS

Quelques résultas

Nombres de propriétés formalisées avec les patrons de définition

Nombre de propriétés étudiées	Cas 1 (49)	Cas 2 (94)	Cas 3 (136)	Cas 4 (85)	Cas 5 (188)	Cas 6 (151)	Total (703)
Propriétés prouvables	38 (78%)	73 (78%)	72 (53%)	49 (58%)	155 (82%)	41 (27%)	428 (61%)
Non-prouvables	11 (22%)	21 (22%)	64 (47%)	36 (42%)	33 (18%)	110 (73%)	275 (39%)

Rédaction des propriétés en amont des spécifications

Travaux de recherche

Observer-Based Prover

Context Description Language

2009-2011

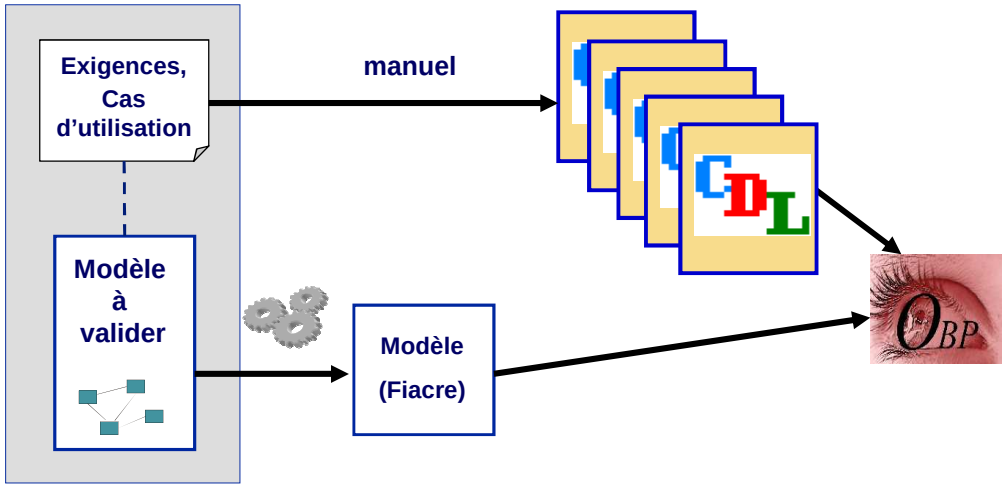
Expérimentations industrielles

UCM & Méthodologie

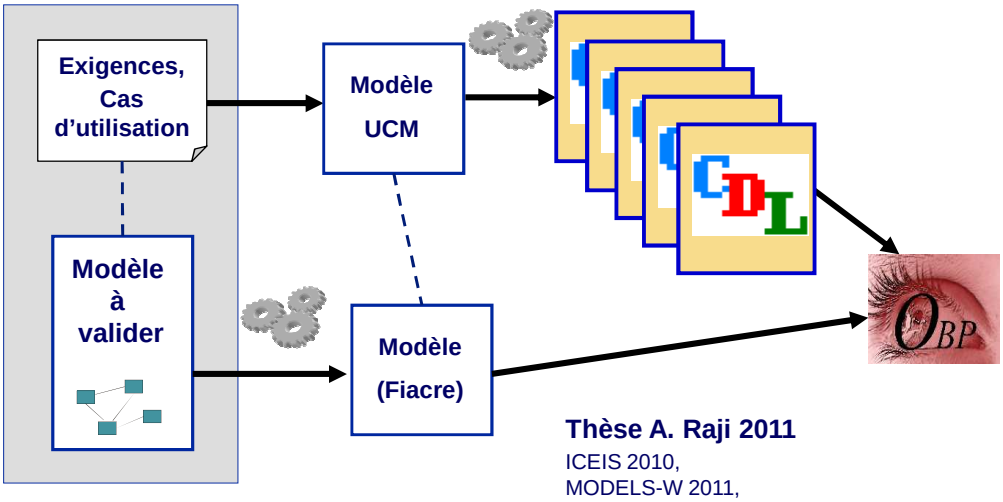
Optimisation, parallélisation OBP

Chaîne de transformation

Génération de codes CDL : User Context Model (UCM)



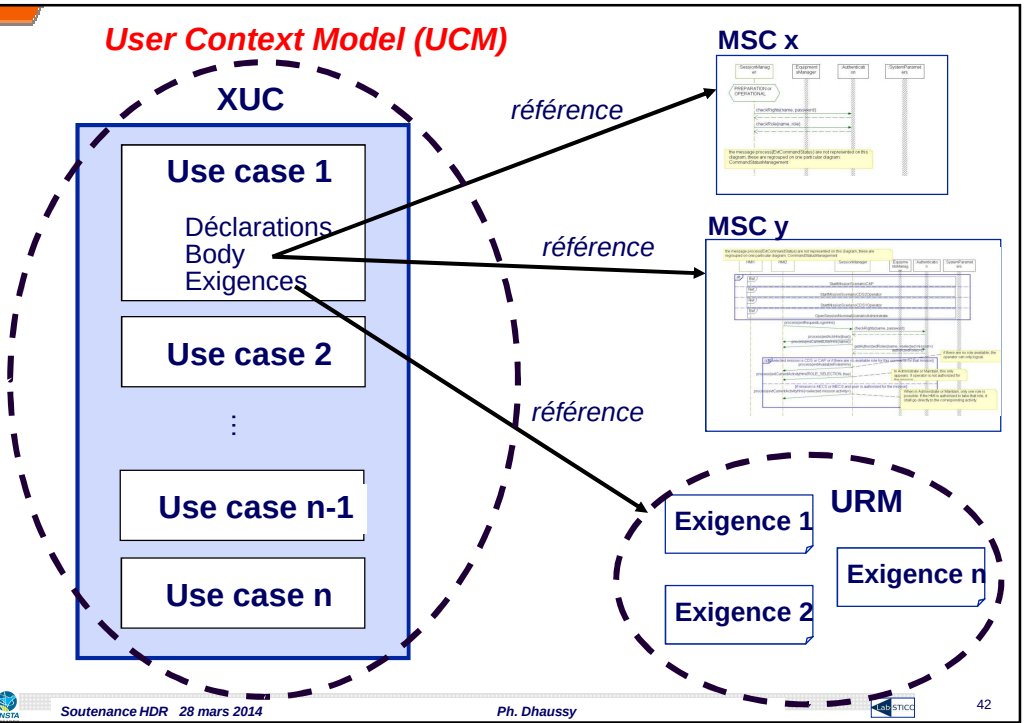
Génération de codes CDL: User Context Model (UCM)



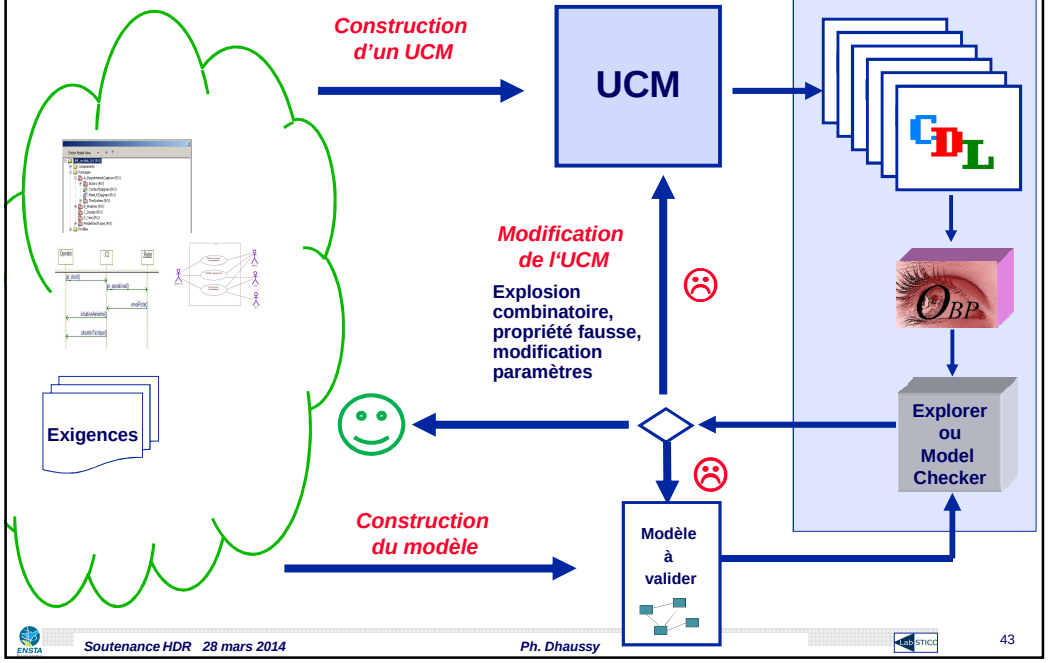
Thèse A. Raji 2011

ICEIS 2010,
MODELS-W 2011,
MODEVVA 2010, 2011,
APSEC 2011
Projet MopCom-Ing

User Context Model (UCM)



Validation de modèles : Méthodologie



Travaux de recherche

Observer-Based Prover

Context Description Language

Expérimentations industrielles

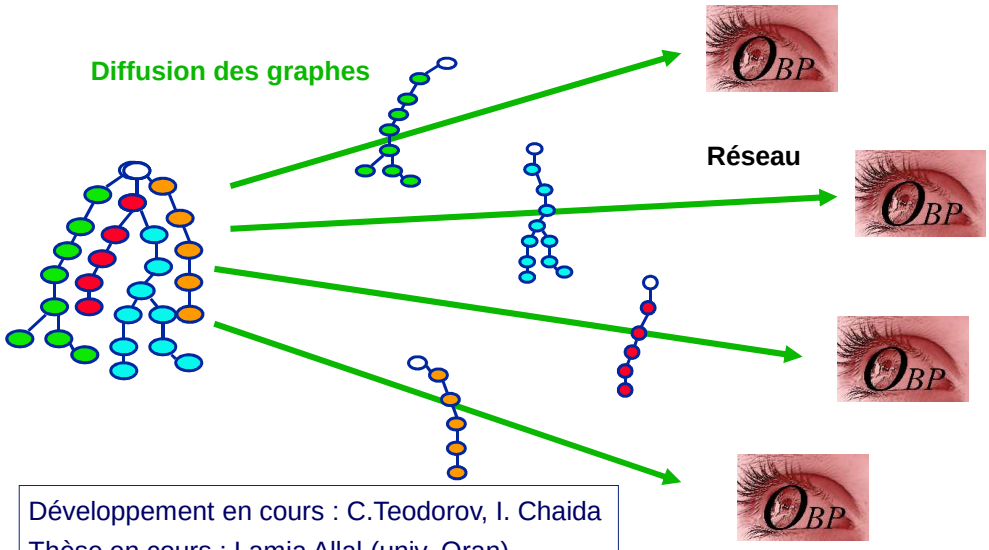
UCM & Méthodologie

2013 …

Optimisation, parallélisation OBP

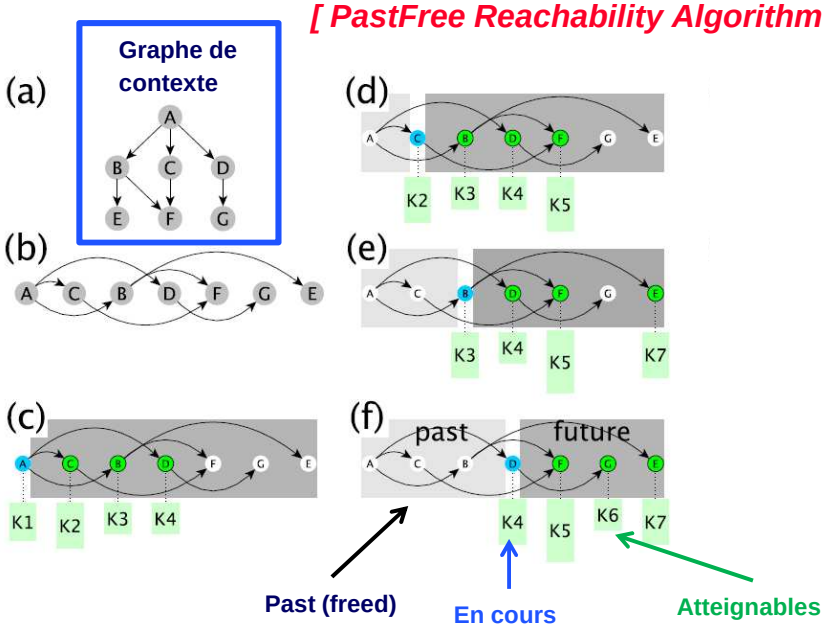
Chaîne de transformation

Explorations distribuées sur un réseau de machine

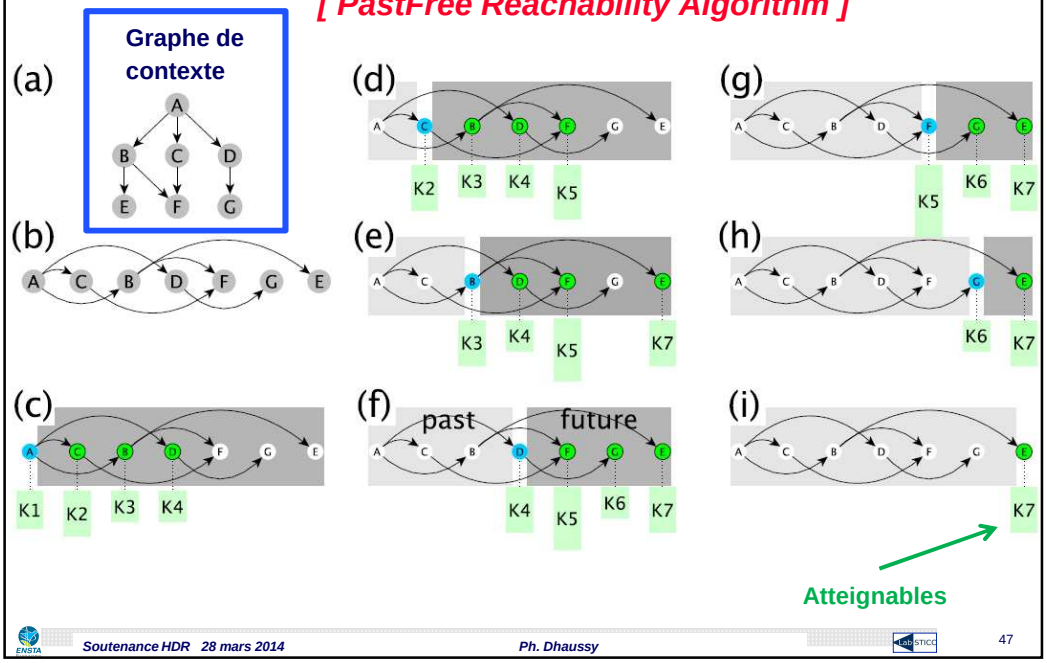


Développement en cours : C.Teodorov, I. Chaida
Thèse en cours : Lamia Allal (univ. Oran)

Optimisation des explorations
[PastFree Reachability Algorithm]

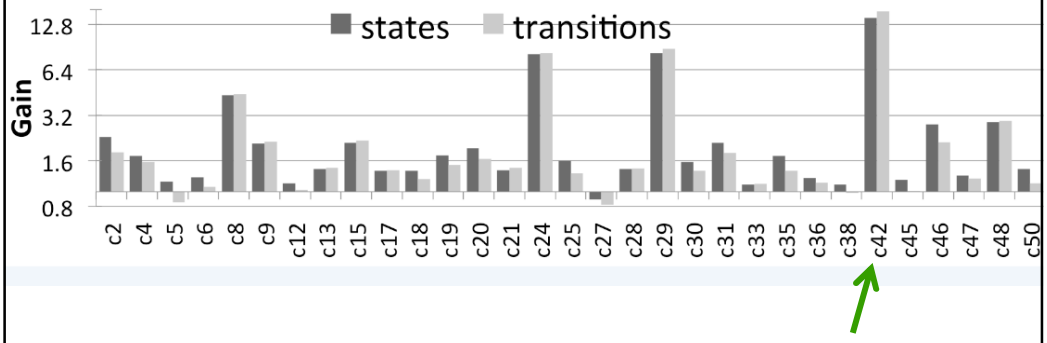


Optimisation des explorations
[PastFree Reachability Algorithm]



Optimisation des explorations
[PastFree Reachability Algorithm]

Gain obtenu avec l'algorithme



14 fois plus de configurations parcourues

Travaux de recherche

Observer-Based Prover

Context Description Language

Expérimentations industrielles

UCM & Méthodologie

Optimisation, parallélisation OBP

2012 …

Chaîne de transformation

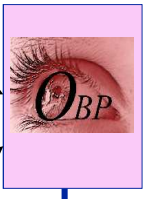
Chaîne de transformation

Editeurs

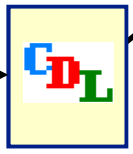
(Rhapsody, Artisan Studio, Mélody Advance, Obeo Designer, Papyrus, Modeleur NAF, …)

?

Modèle Fiacre



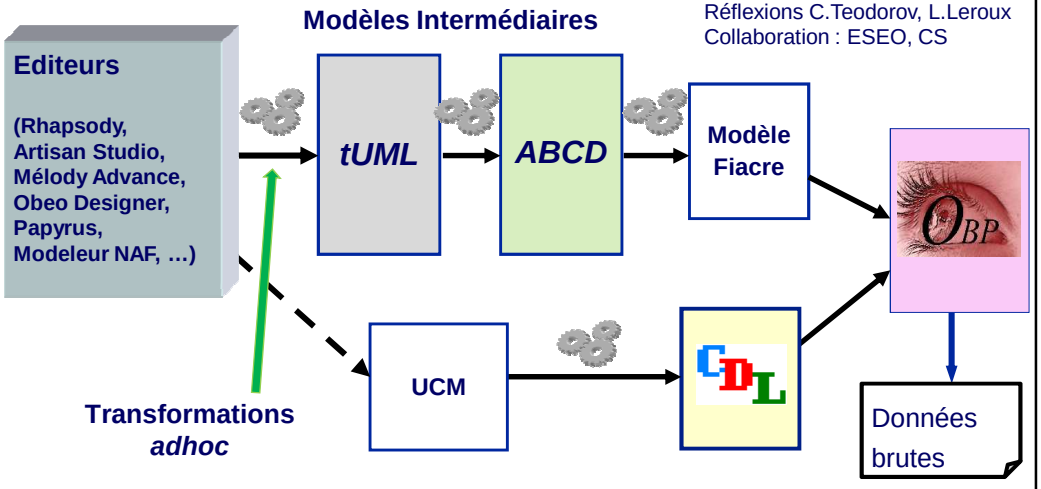
UCM



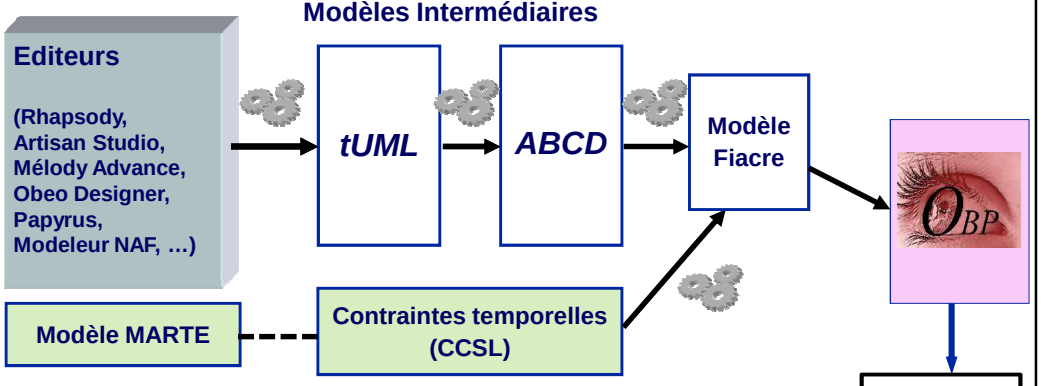
Données brutes

Chaîne de transformation

Projet DEPARTS
[Neptune 2014]
Réflexions C.Teodorov, L.Leroux
Collaboration : ESEO, CS



Chaîne de transformation



Thèse N. Menad (en cours)
[SEFM'13]
Master Ismat et Medhi
Réflexions Z. Drey, JC.Le Lann, C.Teodorov, J.Champeau
(projet GEMOC)

Retour d'expérience : l'apport

- CDL, UCM : **permet une formalisation**

  Cas d'utilisation (contextes) et des propriétés

- Contribution à la **gestion de la complexité**
- Motivation des partenaires pour une **approche plus formelle** de leurs exigences
- Aide à la **structuration** de leurs spécifications (UCM)
- **Mise en pratique** en contexe industriel

➔ **Meilleure appropriation des processus de validation formelle**

Retour d'expérience : difficultés et limites

- Spécifications industrielles :
  - Problèmes de **complétude et de cohérence**
  - Non pensées pour la validation formelle
- Effort important nécessaire pour la **compréhension**

  ~ plusieurs semaines pour une application
- Dialogue incontournable avec les experts métier

  Les bons outils, les bonnes méthodes, la conviction ne suffisent pas !
- Difficulté d'ordre **méthodologique** (peu abordé en enseignement)

Efforts à poursuivre

Minimiser les ruptures dans les pratiques industrielles

Méthodologies *ad-hoc* à imaginer, à concevoir, à développer

➔ ***Domaines et types d'application spécifiques***

Diffusion outils - méthode

www.obpcdl.org

Groupes d'échange avec la communauté industrielle

Laboratoire Communs

CALIPSO (Thales S.A)
AVS (CS : re-soumission ANR LabCom mai 2014)

Plateforme de distribution d'outils Open Source : PolarSys

- Partage des moyens entre industriels (*end user*)
- Services et écosystèmes autour des composants open source
- Gestion de la qualité et de la maturité des outils et composants
- Préparation de la certification

Plan

- Motivations & Synthèse
- Travaux, résultats, retour d'expérience
- Perspectives

Perspectives

Poursuite des expérimentations industrielles

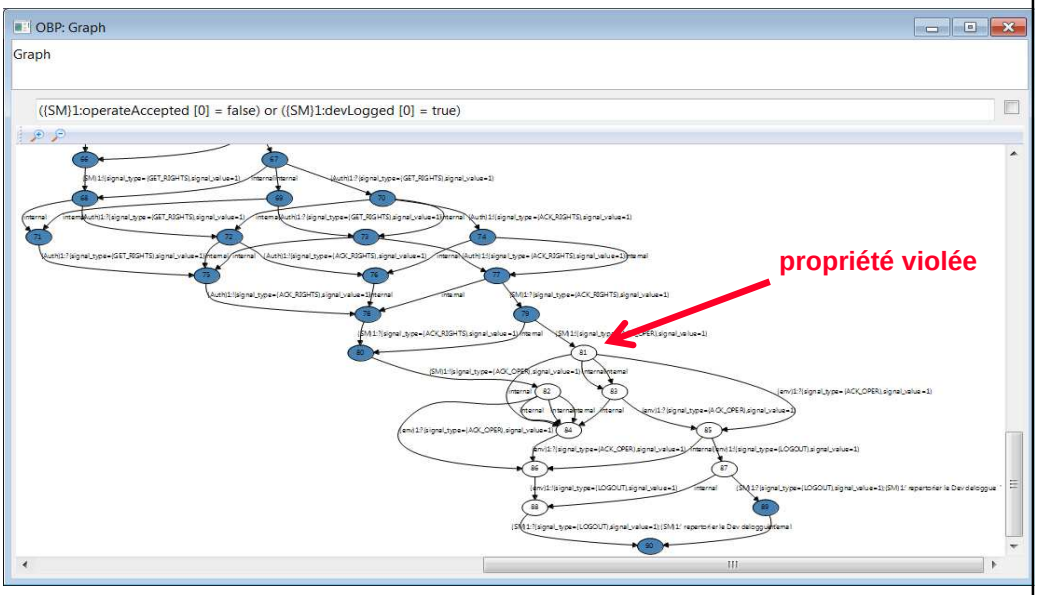
Aide au diagnostic

UCM & Méthodologie

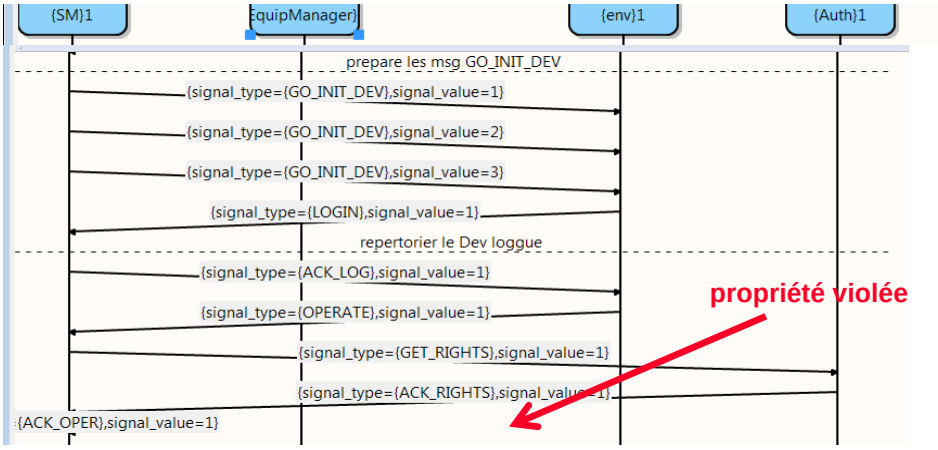
Optimisation OBP

Correction des transformations

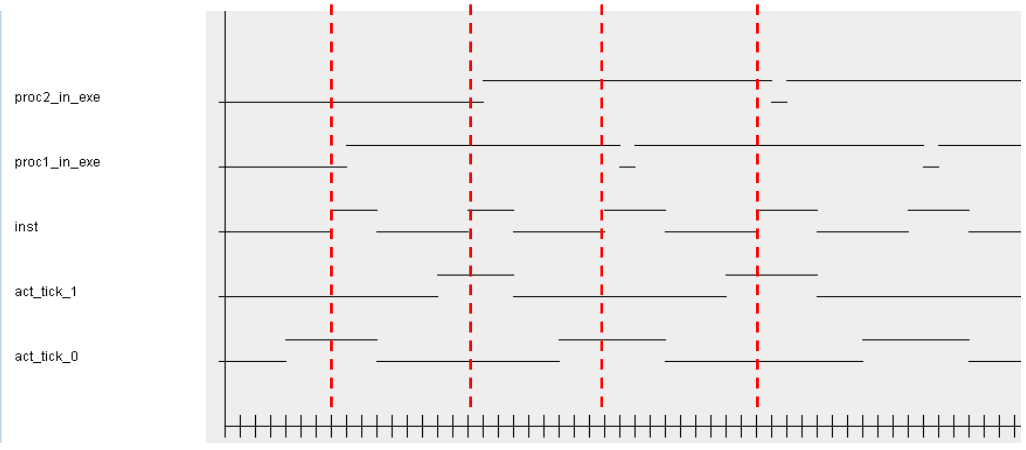
Détection d'une erreur dans le modèle



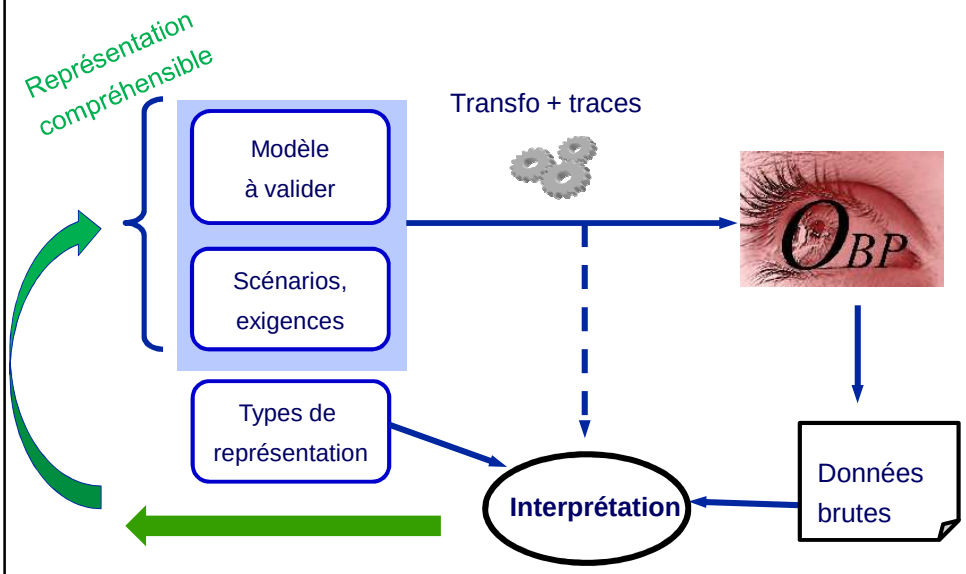
Détection d'une erreur dans le modèle



Chronogramme généré



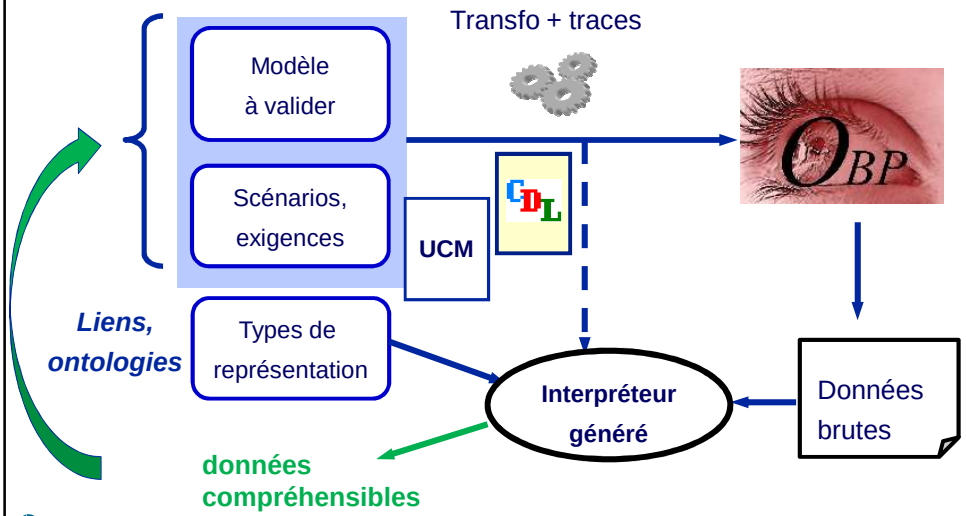
Le besoin : Aide pour le diagnostic



Le besoin : Aide pour le diagnostic

Projet OpenFlexo

Réflexion : S.Guerrin, V. Leilde



Perspectives

Poursuite des expérimentations industrielles

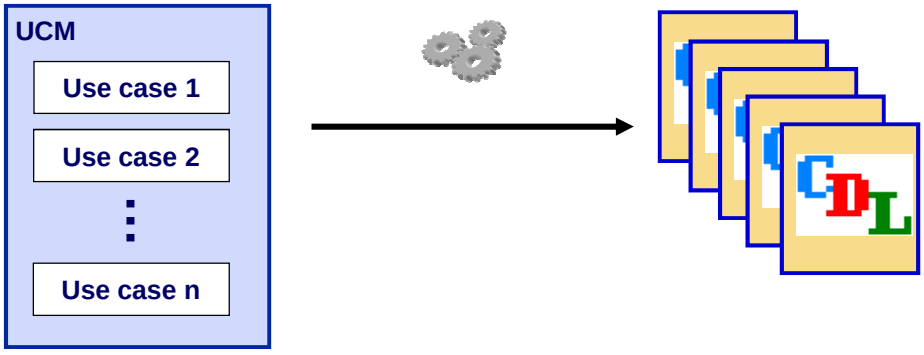
Aide au diagnostic

UCM & Méthodologie

Optimisation OBP

Correction des transformations

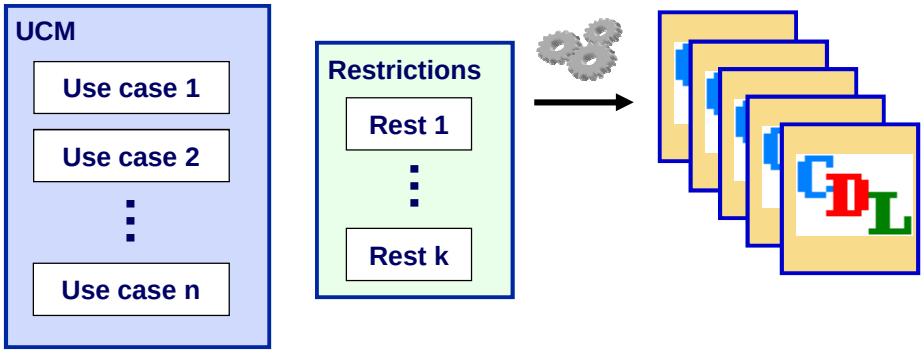
Méthodologie



- Peut générer beaucoup de complexité
- Nécessite un dialogue rationnel avec le concepteur (méthodologie)

Méthodologie

Réflexions avec L.Leroux



Restrictions basées sur la connaissance de l'expert :

- Les propriétés et modes,
- Des ensembles d'acteurs et de données (interactions restreintes)

➔ Identification :

- de contraintes de synchronisation (init, …), d'observateurs d'arrêt

➔ limiter la profondeur et la largeur des graphes de contexte

Perspectives

Poursuite des expérimentations industrielles

Aide au diagnostic

UCM & Méthodologie

Optimisation OBP

Correction des transformations

Optimisation des explorations

Réflexions avec C.Teodorov

- Sauvegarde des configurations
- Bases de données orientées graphes
- Cloud Computing

Perspectives

Poursuite des expérimentations industrielles

Aide au diagnostic

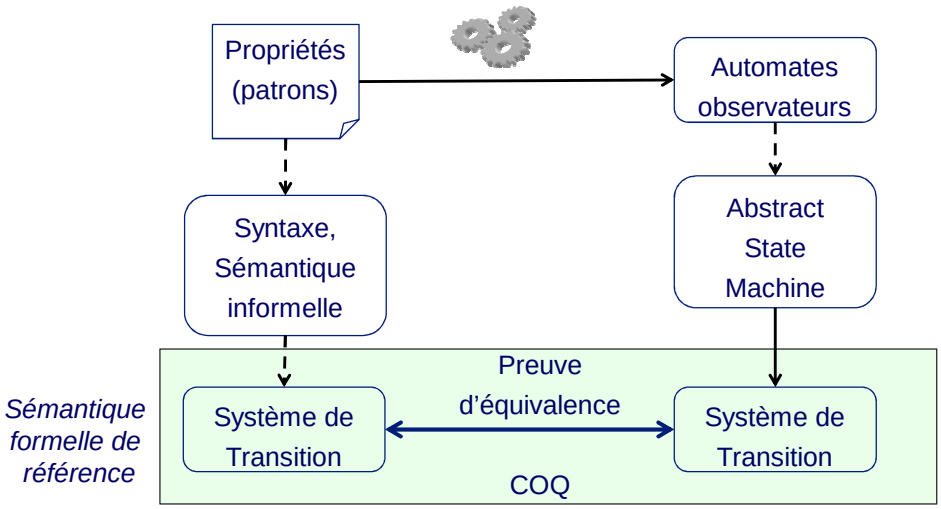
Optimisation OBP

UCM & Méthodologie

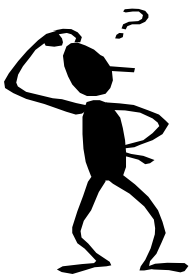
Correction des transformations

Correction des transformations des propriétés

Thèse D.Baroudi, Master I.Naas



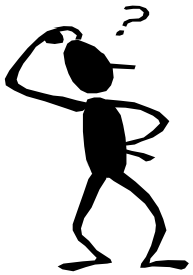
Merci de votre attention et vos questions



- Merci aux **membres du jury**
- Merci à mes nombreux **collègues académiques, Industriels,**
- Merci à **l'Equipe IDM**
- Merci aux **personnels de l'Ensta-Bretagne**
- Merci à **Michèle** et **Annick**
- Merci **Anne** pour ton soutien …

www.obpcdl.org

Merci de vos questions



www.obpcdl.org

En guise d'épilogue, osons un rêve …

Hubert, François, Joseph, Philippe, décident enfin de travailler ensemble …