Ampère
Unité Mixte de Recherche CNRS
Génie Électrique, Électromagnétisme, Automatique, Microbiologie environnementale et Applications

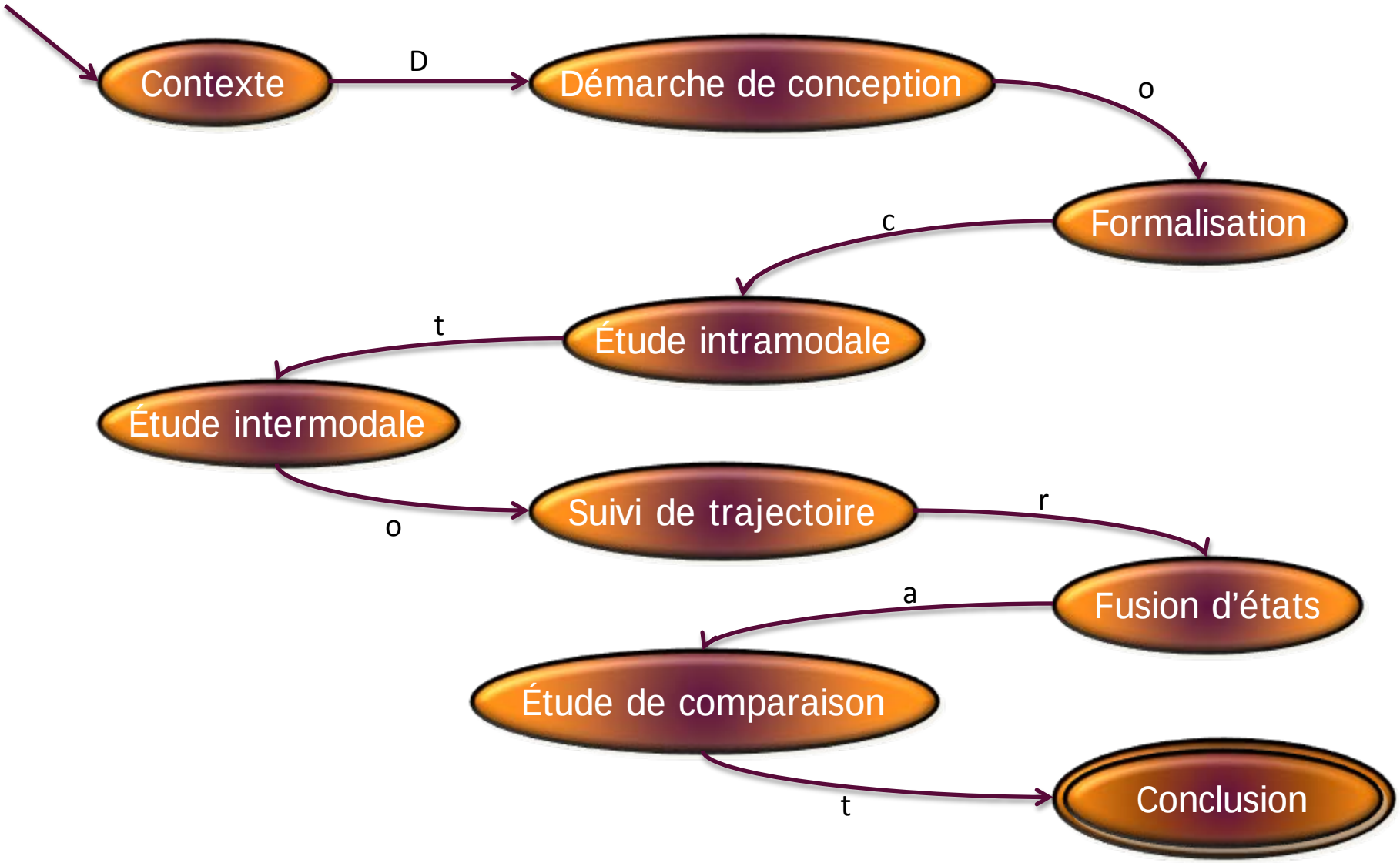
Commutations sûres de mode pour les systèmes à événements discrets

Présentée par : **Gregory FARAUT**

Devant le jury d'examen

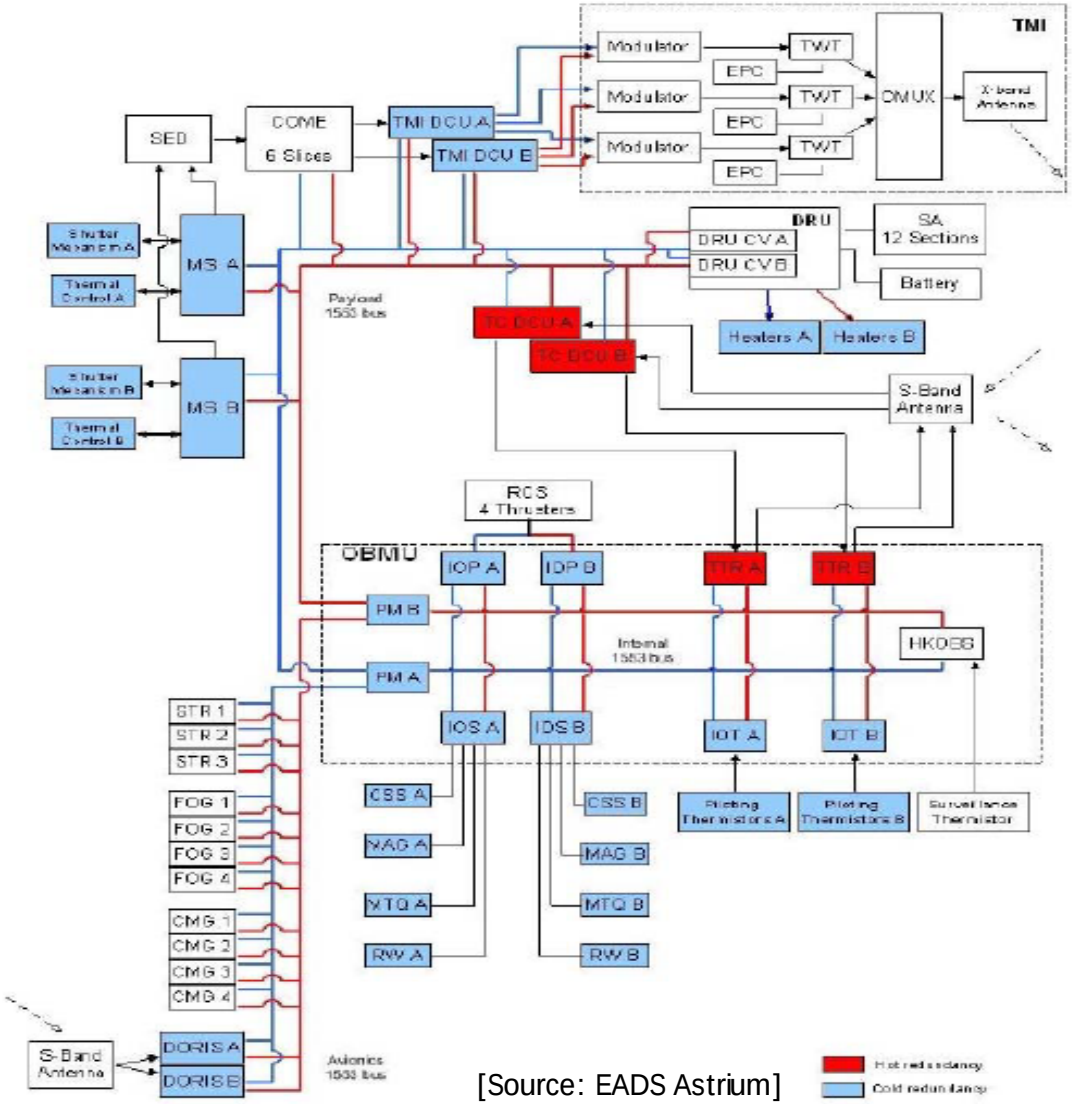
MM.	Etienne Craye	Professeur (LAGIS, École Centrale de Lille), Rapporteur
	Olivier H. Roux	Professeur (IRCCyN, École Centrale de Nantes), Rapporteur
	Charles André	Professeur (I3S/INRIA, Univ. Nice-Sohpia), Examinateur
	Nidhal Rezg	Professeur (LGIPM/ISGMP, Univ. de Metz), Examinateur
	Eric Niel	Professeur (Ampère, INSA-Lyon), Directeur de thèse
	Laurent Piétrac	Maître de Conférences (Ampère, INSA-Lyon), Co-directeur

Plan de l'exposé



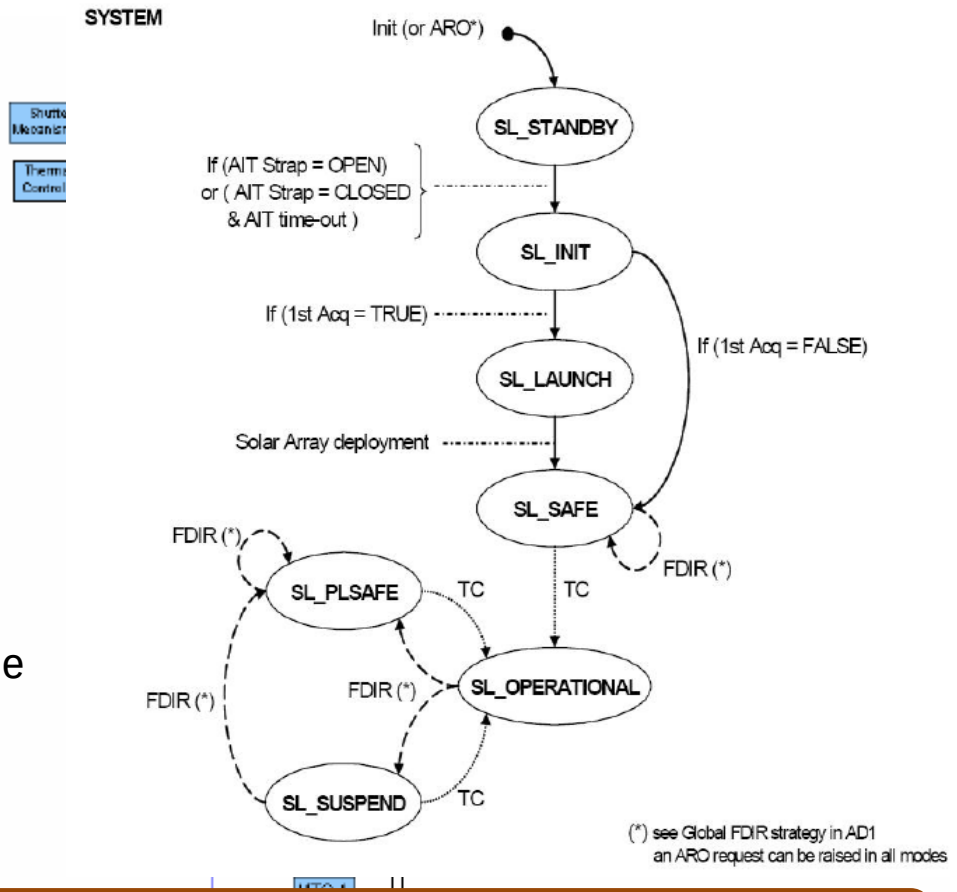
Approche modale

- Ensemble de composants
- Activation/désactivation des composants s'effectue selon les modes



Approche modale

- Dans chaque mode :
  - un ensemble prédéfini de composants est utilisé
  - Le système assure une ou un ensemble de missions



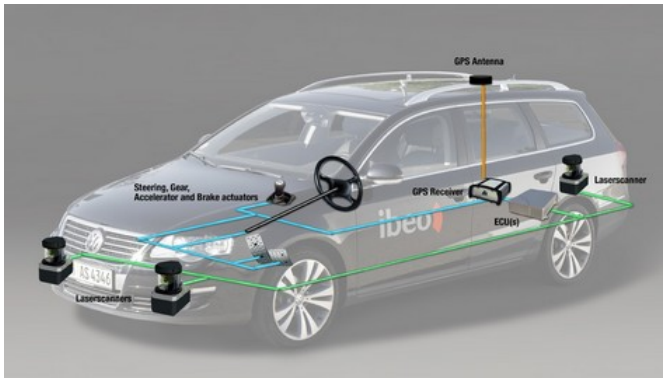
Définition

Un mode est une configuration particulière du système tel qu'il utilise un ensemble de composants et doit respecter un ensemble de spécifications dans le but de répondre à un besoin de production, de qualité de service, de rendement, etc.

Approche modale

- Trains:
  - Couplement / désacouplement de rames
  - Préconditionnement rame
  - Maintien de service
  - KVB (sécurité)

- Systèmes industriels:
  - Vitesse de production
  - Qualité
  - Personnalisation du produit
  - Hétérogénéité de production



- Automobile:
  - Voiture sans pilote
  - Stationnement automatique
  - Moteurs hybrides (essence/électrique)

Approche modale : Problématique

- Démarche de conception appliquée à la gestion des modes
  - Améliore l'interprétation sur le fonctionnement d'un système

- Détermination des modes
  - Stratégie de détermination des modes d'un système physique

Données du cahier des charges

- Construction des modèles de modes
  - Comportement interne des modes
  - Respect des spécifications propres à chaque modes, indépendamment des autres

- Construction commutations entre modèles de modes
  - Représentation fidèle des commutations entre modes
  - Prise en compte des spécifications de commutations propres à chaque modes
  - Possibilité de commuter entre modes de manières sûres

Synthèse des travaux sur gestion de mode

- Ne pas imposer un canevas de modes pour utiliser la démarche
  - Ne pas cibler un domaine précis

  [Nou97, Kam04, Dan00, Rak05]

- Démarche reposant sur des bases mathématiques:
  - Nécessité de prouver mathématiquement des propriétés sur les modèles obtenus

  [Kam04, Dan00, Ham05, Rak05]

- Unicité de mode actif

  [ADE81, Nou97, Dan00, Koo01, Kam04, Rak05, Ham05]

- Exhaustivité des commutations possibles
  - Nécessite l'ajout d'un modèle de description du comportement du système

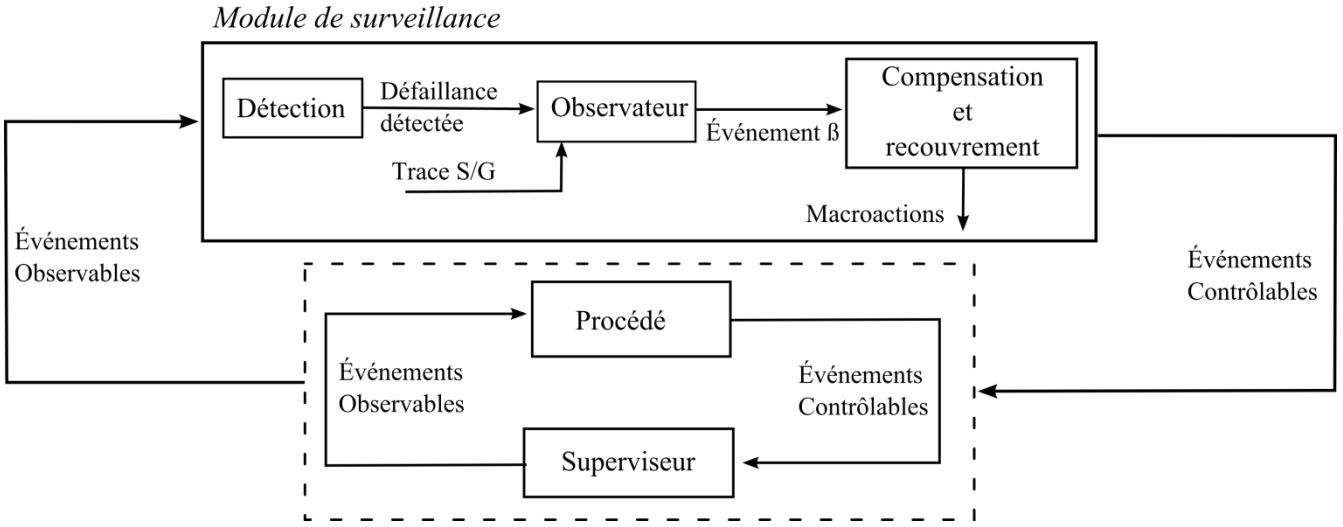
  [Nou97, Dan00, Rak05, Koo1]

- Démarche complètement définie (automatisation)

  [Koo01, Rak05]

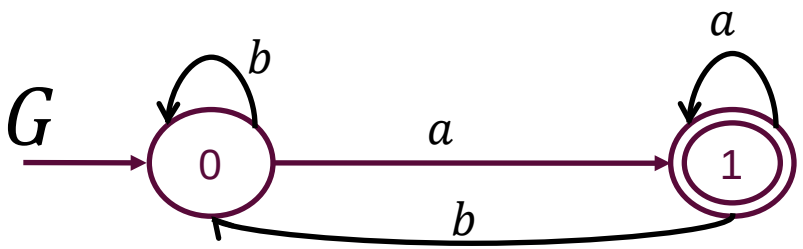
Précédents Travaux : Nourelfath (1997)

- Apports
  - Détection des défaillances et une fonction de compensation recouvrement
  - Désactivation du mode nominal : état inactif
  - Suivi des traces pour la détection et l'identification de la défaillance
  - Un mode nominal construit par la TCS : modèle sûr par construction

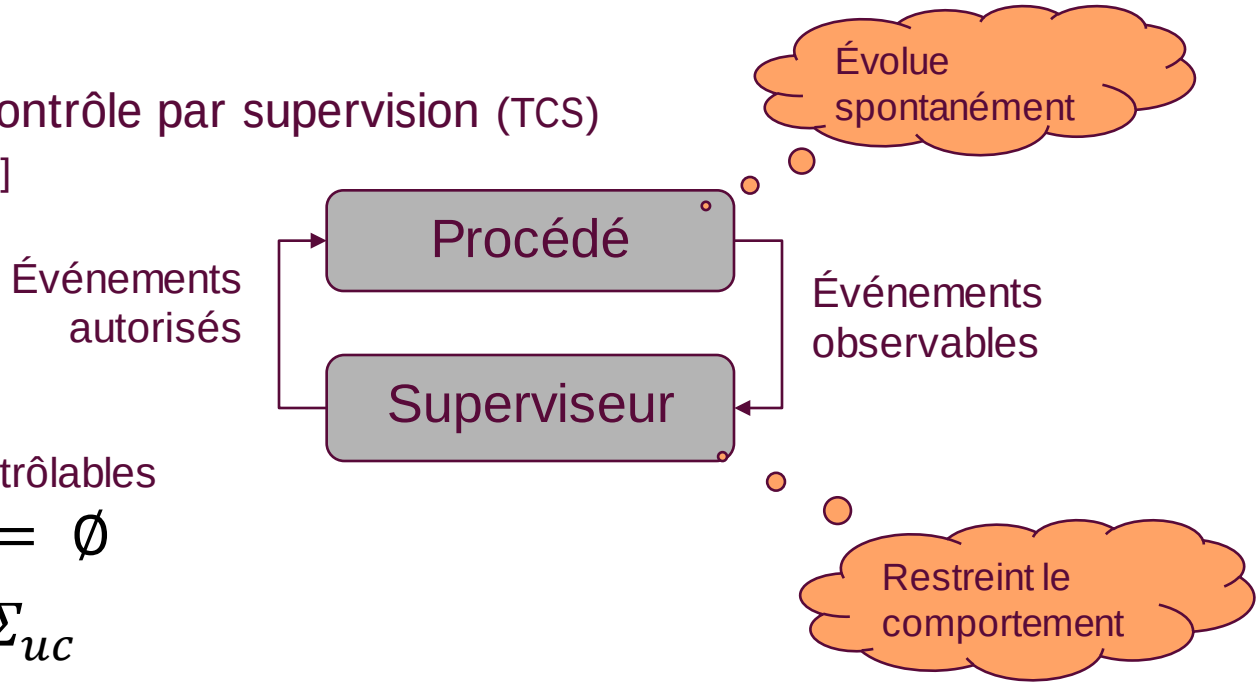


Précédents Travaux : Utilisation de la TCS

- Théorie du langage et représentation en automates
  - Ex. : l'alphabet $\Sigma = \{a, b\}$, le langage $L = (b^*a^*)^*$, et le langage marqué $L_m = (b^*a^*)^*a$



- Théorie de contrôle par supervision (TCS) [Ram87,Won87]



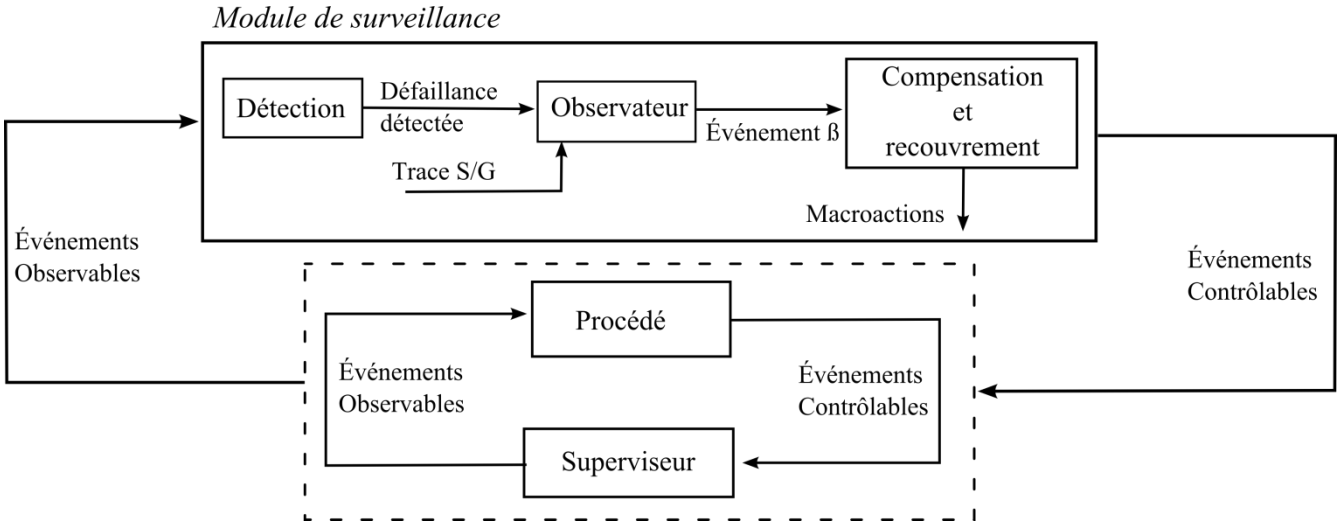
Événements contrôlables

$$\Sigma_c \cap \Sigma_{uc} = \emptyset$$

$$\Sigma = \Sigma_c \cup \Sigma_{uc}$$

Précédents Travaux : Nourelfath (1997)

- Apports
  - Détection des défaillances et une fonction de compensation recouvrement
  - Désactivation du mode nominal : état inactif
  - Suivi des traces pour la détection et l'identification de la défaillance
  - Un mode nominal construit par la TCS : modèle sûr par construction

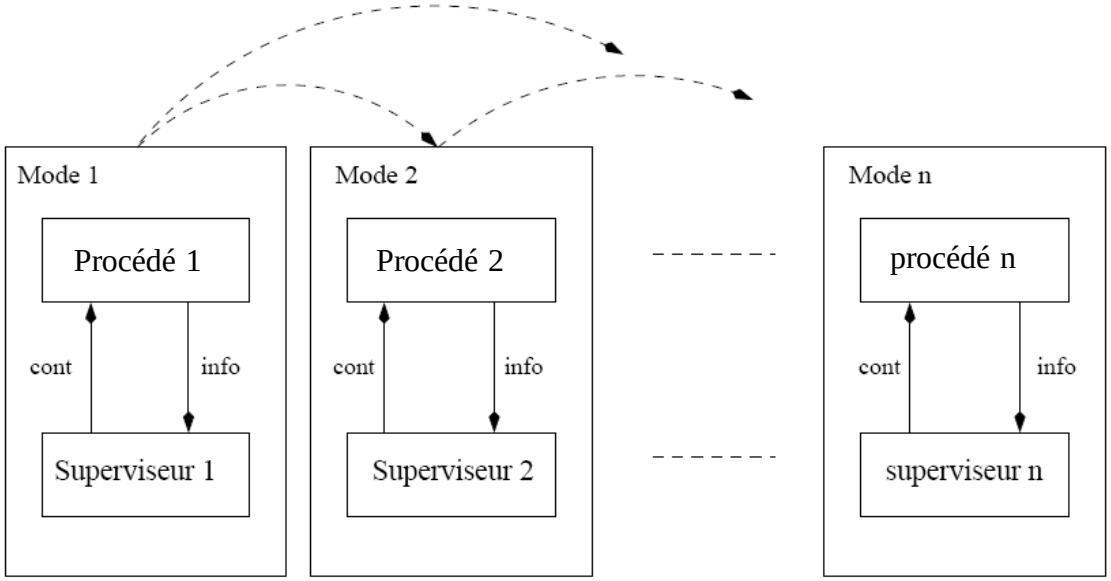


- Limitations
  - Un seul mode construit par une méthode mathématiquement définie
  - Module de surveillance construit manuellement
  - Étude pour chaque commutation

Précédents Travaux : Kamach (2004)

Apports

- Tous les modes construits par la TCS
- Études du comportement interne et externe séparées
- Proposition d'un suivi de trajectoire
- Suffisance d'un seul superviseur par mode



Limitations

- Démarche non complètement définie
- Commutations ajoutées manuellement
- Assurance de commutations respectant les spécifications non prouvées

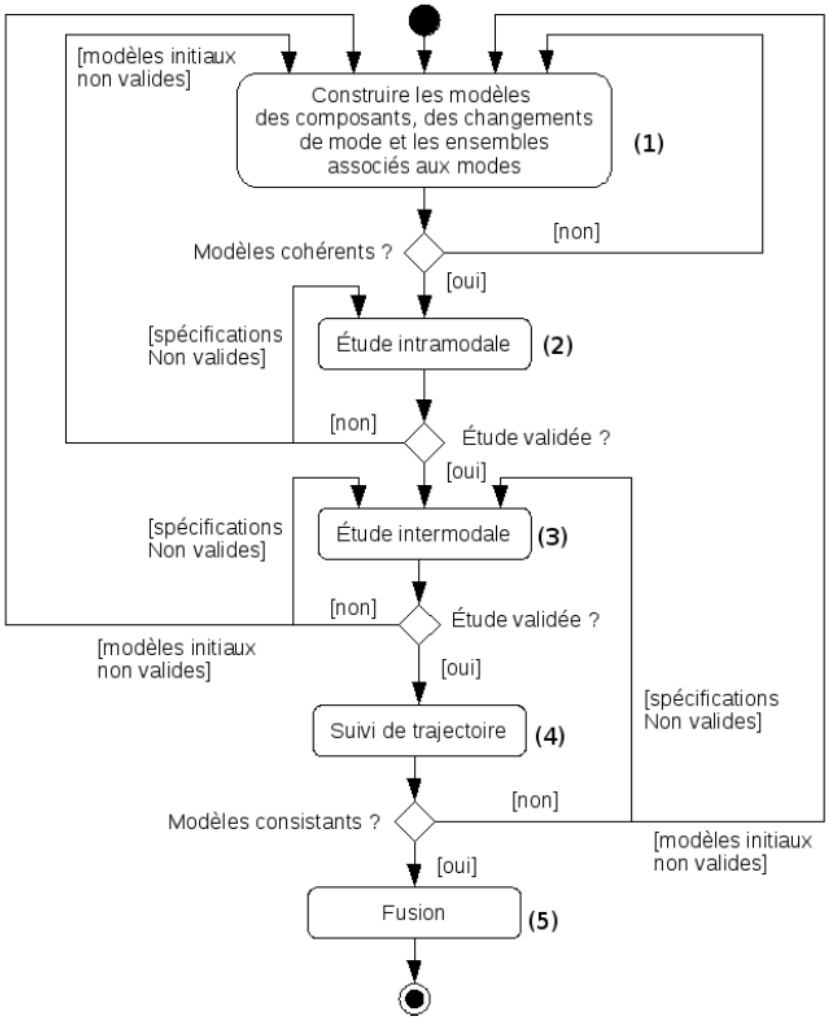
Objectifs

- Ne pas imposer un canevas de modes pour utiliser la démarche
  - Utilisable dans plusieurs domaines
- Démarche reposant sur des bases mathématiques:
  - Utilisation de la théorie de contrôlable par supervision (TCS)
- Unicité de mode actif
  - Un seul modèle doit représenté le comportement admissible à la fois
- Exhaustivité des commutations possibles
  - Toutes les commutations doivent être étudiées
- Démarche complètement définie (automatisation)
  - Toujours définir mathématiquement le passage d'une étape à une autre

Contributions

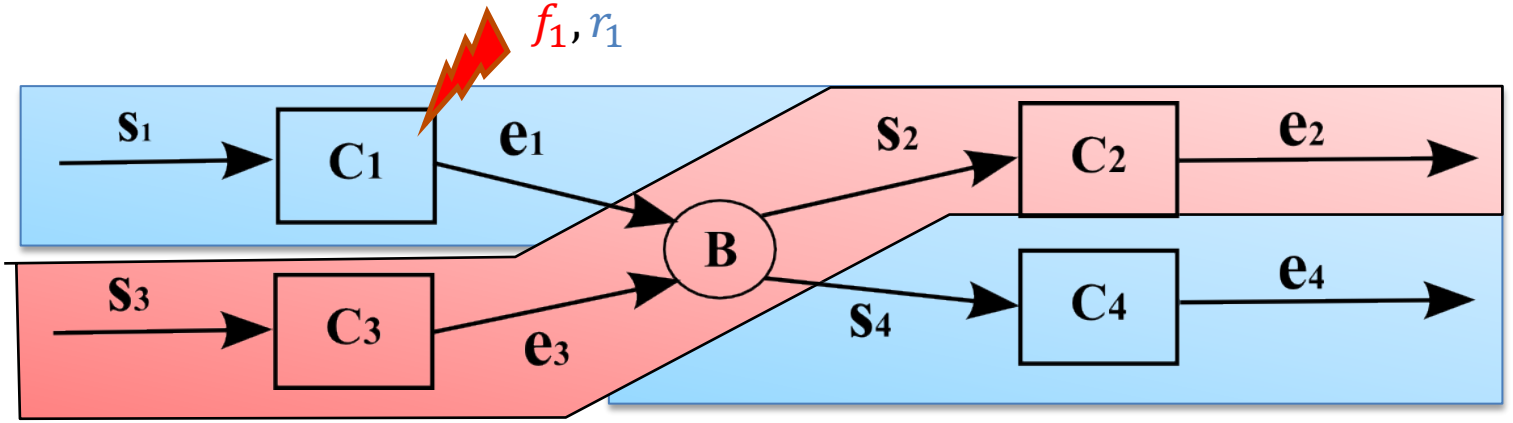
- Démarche de conception
  - 5 étapes
  - Aide à la conception

1. Formalisation du cahier des charges
   - Construction des modèles
   - Validation de la cohérence
2. Étude Intramodale
   - Construction des procédés sous contrôle interne
   - validation des spécifications intramodale
3. Étude Intermodale
   - Construction des procédés sous contrôle
   - validation des spécifications intermodales
4. Suivi de trajectoire
   - Suivi de trajectoire
   - Vérifications des commutations entre modes
5. Fusion d'états
   - Regroupement des états non significatifs



Exemple directeur

- Système à quatre machines C_i et un stock B



- 2 modes de fonctionnement
  - Mode nominal (N) -> utilisation des composants C_1, C_2 et C_4
  - Mode dégradé (D) -> utilisation des composants C_3 et C_2 (redondance de composant)

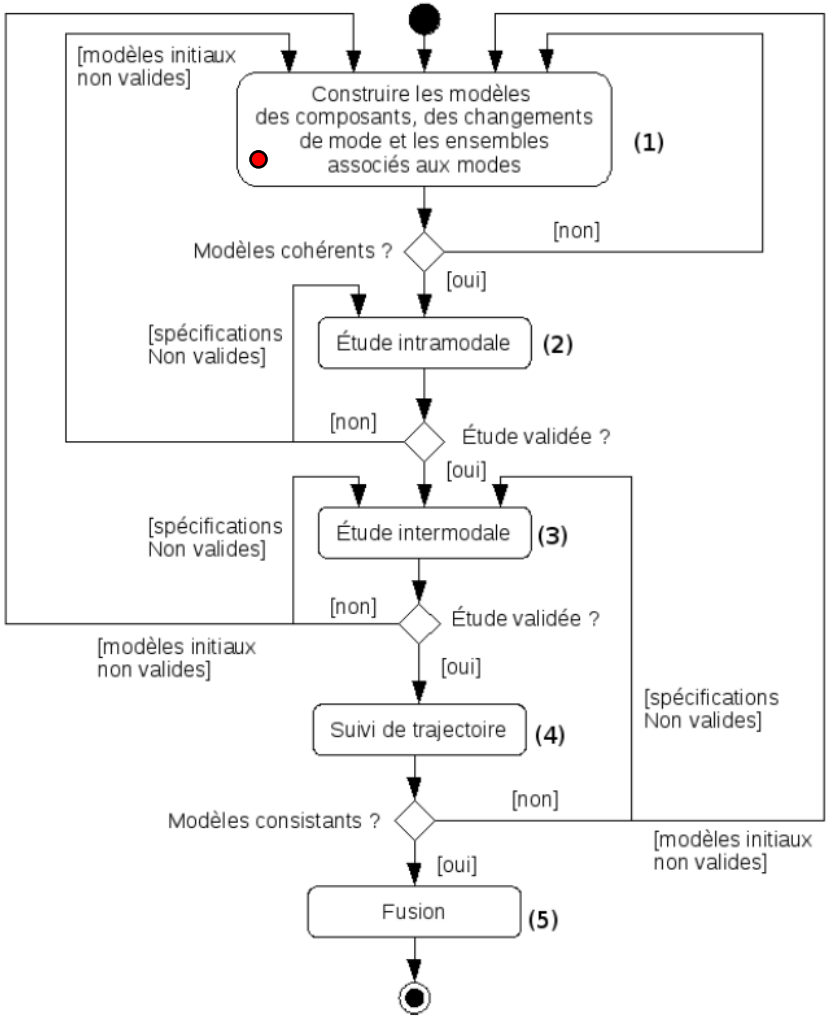
- Changement de mode
  - Sur occurrence de faute f_1
  - Sur occurrence de réparation r_1

- Spécifications du mode nominal
  - Taille maximale de 1

- Spécifications du mode dégradé
  - Taille maximale de 1
  - C_3 en redondance sur C_1

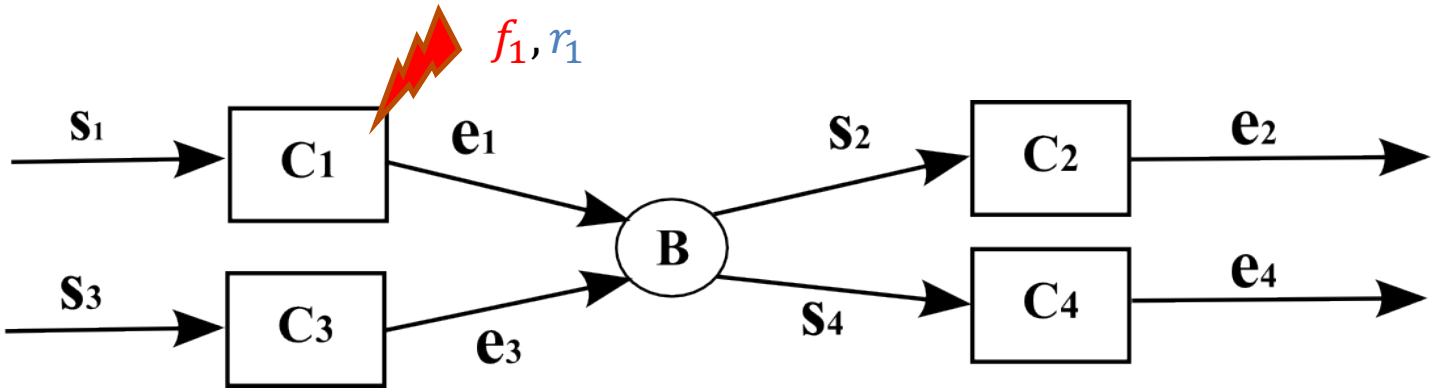
Démarche de conception

1. Formalisation du cahier des charges
   - Construction des modèles

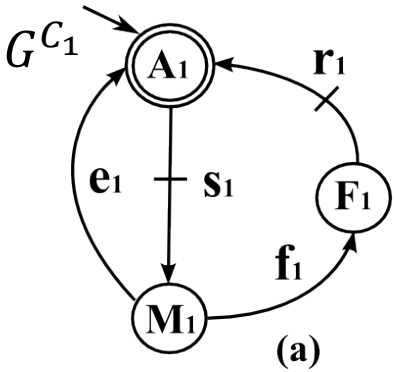


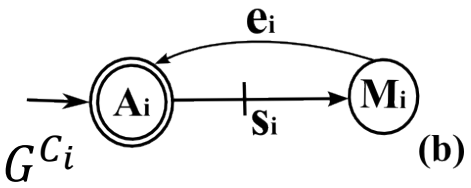
Formalisation des données du cahier des charges

- Système à quatre machines C_i et un stock B



- Modèles de composants



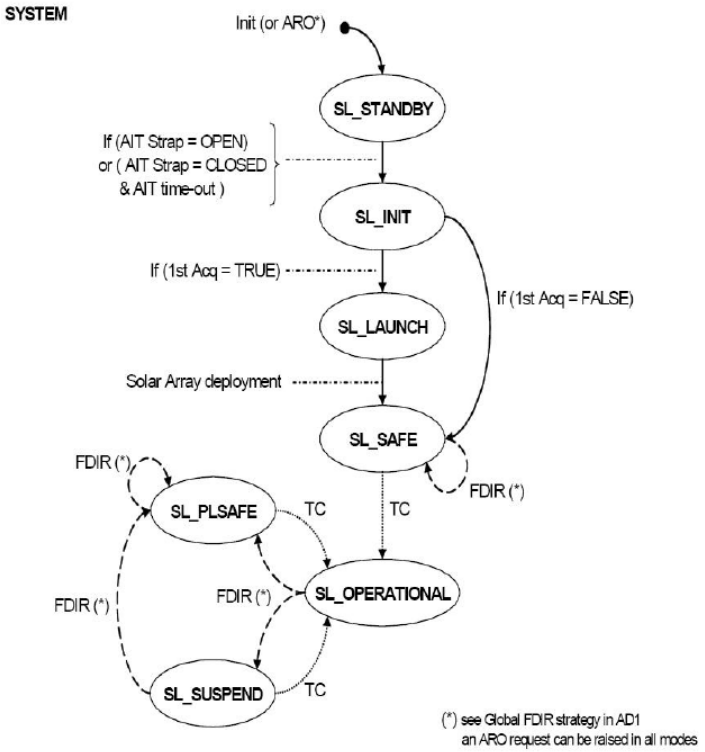


$C_i \in \{C_2, C_3, C_4\}$

Formalisation des données du cahier des charges

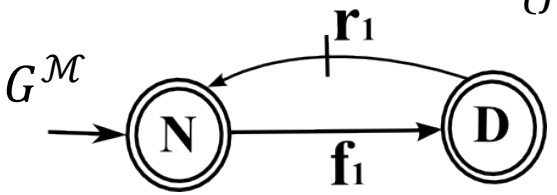
- Modèle de l'automate de mode
  - Décrit le comportement commutatif du système
  - Permet de représenter une séquence de modes

- Ex: Satellite
  - quatre premiers modes transitoires
  - Un mode nominal
  - Deux modes dégradés



- Dans l'exemple directeur:
  - Deux modes $\mathcal{M} = \{N, D\}$
  - Commutations sur événements de commutation générés par C_1
  - Un modèle par mode

$\{f_1, r_1\} \in \Sigma^{C_1}$



- Représente l'activation/désactivation d'un mode

Formalisation des données du cahier des charges

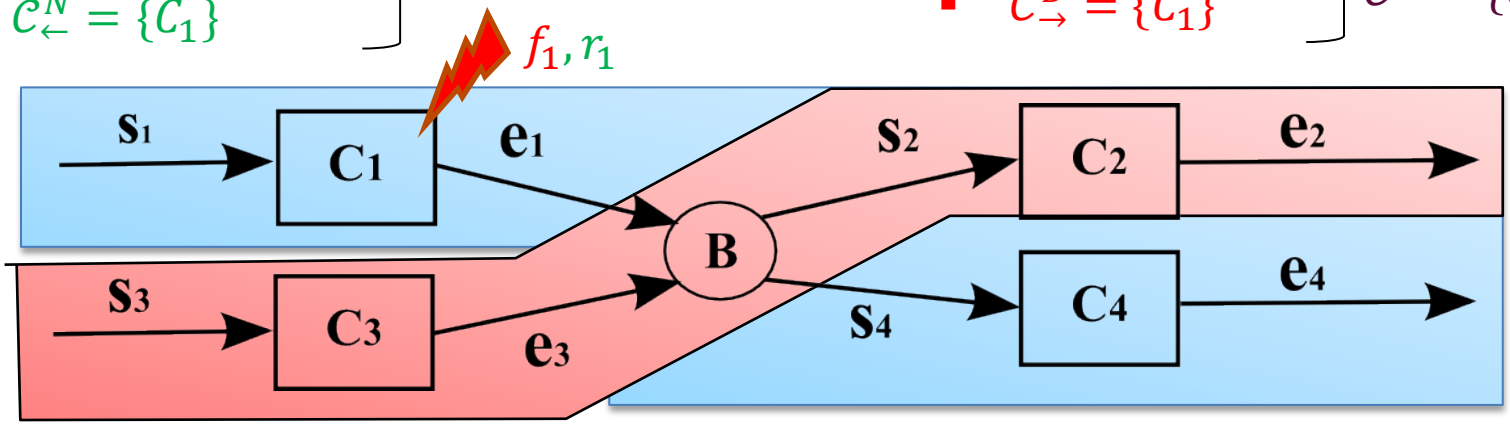
- Ensembles associés aux modes :
  - $\mathcal{C}^{M_j}$: ensemble des composants utilisés dans le mode Mj
    - $\mathcal{C}_{\circlearrowleft}^{M_j}$: ensemble des composants représentant le comportement interne,
    - $\mathcal{C}_{\leftarrow}^{M_j}$: ensemble des composants générant un événement qui active le mode,
    - $\mathcal{C}_{\rightarrow}^{M_j}$: ensemble des composants générant un événement qui désactive le mode,

- mode nominal (N)
  - $\mathcal{C}_{\circlearrowleft}^{N} = \{C_1, C_2, C_4\}$
  - $\mathcal{C}_{\rightarrow}^{N} = \{C_1\}$
  - $\mathcal{C}_{\leftarrow}^{N} = \{C_1\}$

  $\mathcal{C}^{N} = \{C_1, C_2, C_4\}$

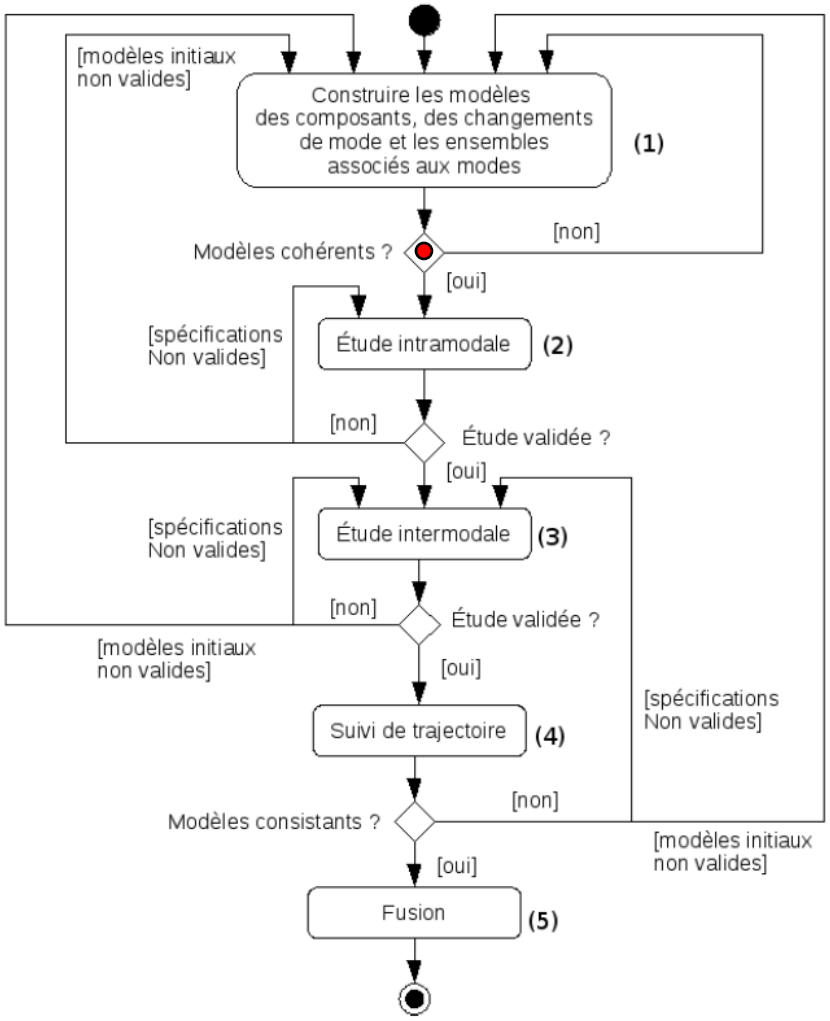
- mode dégradé (D)
  - $\mathcal{C}_{\circlearrowleft}^{D} = \{C_2, C_3\}$
  - $\mathcal{C}_{\leftarrow}^{D} = \{C_1\}$
  - $\mathcal{C}_{\rightarrow}^{D} = \{C_1\}$

  $\mathcal{C}^{D} = \{C_1, C_2, C_3\}$



Test de cohérence

1. Formalisation du cahier des charges
   - Construction des modèles
   - Validation de la cohérence des modèles



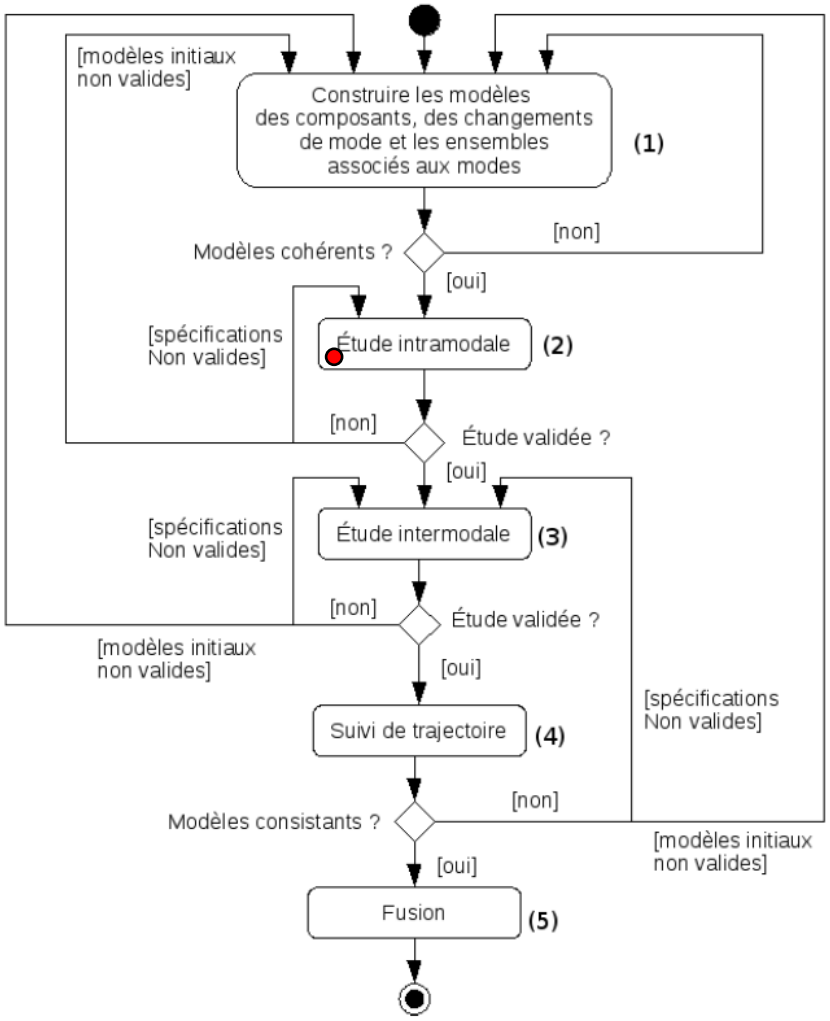
Validation de la cohérence des modèles

- Objectifs
  - Vérifier la cohérence dans les choix de modélisation
  - Identifier précocement les problèmes possibles
- Validation si :
  - Tout mode a un comportement interne et commutatif: $\forall M_j \in \mathcal{M}, \mathcal{C}_{\circlearrowleft}^{M_j} \neq \emptyset \wedge \mathcal{C}_{\rightleftarrows}^{M_j} \neq \emptyset$
  - Les composants générant les événements de commutation appartiennent à au moins un ensemble de commutation: $\forall C_i \in \mathcal{C}, [\Sigma_{\rightleftarrows}^{M_j} \neq \emptyset \iff \exists M_j \in \mathcal{M}, C_i \in \mathcal{C}_{\rightleftarrows}^{M_j}]$
  - Tous les événements de commutation sont bien utilisés dans l'automate de mode: $\Sigma^{\mathcal{M}} = \bigcup_{C_i \in \mathcal{C}} \Sigma_{\rightleftarrows}^{C_i}$
  - Les événements de l'automate de mode appartiennent bien à un ensemble d'événements de commutation d'un mode:

$$\forall M_j \in \mathcal{M}, [C_i \in \mathcal{C}_{\rightleftarrows}^{M_j} \iff (\forall \alpha \in \Sigma_{\rightleftarrows}^{C_i}, \exists M_k \in \mathcal{M}, \delta^{\mathcal{M}}(M_j, \alpha) = M_k \vee \delta^{\mathcal{M}}(M_k, \alpha) = M_j)]$$

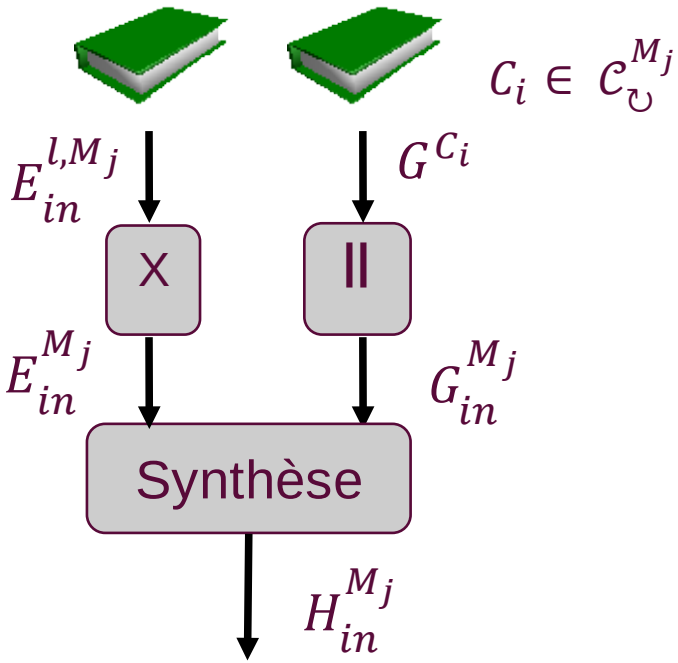
Étude intramodale

1. Formalisation du cahier des charges
   - Construction des modèles
   - Validation de la cohérence
2. Étude Intramodale
   - Construction des procédés sous contrôle interne
   - validation des spécifications intramodales



Étude intramodale

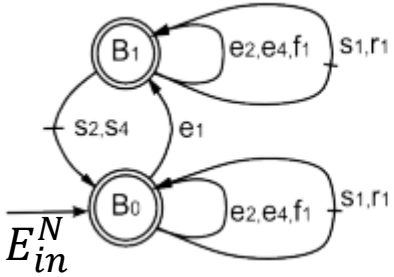
➢ Construire le modèle représentant le comportant interne dans chaque mode

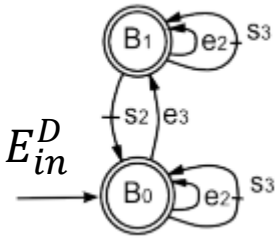


$$L_m(H_{in}^{M_j}) = \left[L_m\left(G_{in}^{M_j} \times E_{in}^{M_j}\right)\right]^{\uparrow c}$$

- Complexité inhérente à la SCT réduite
- Meilleure interprétation des modèles
- Permet la recherche du comportement admissible qui respect les spécifications

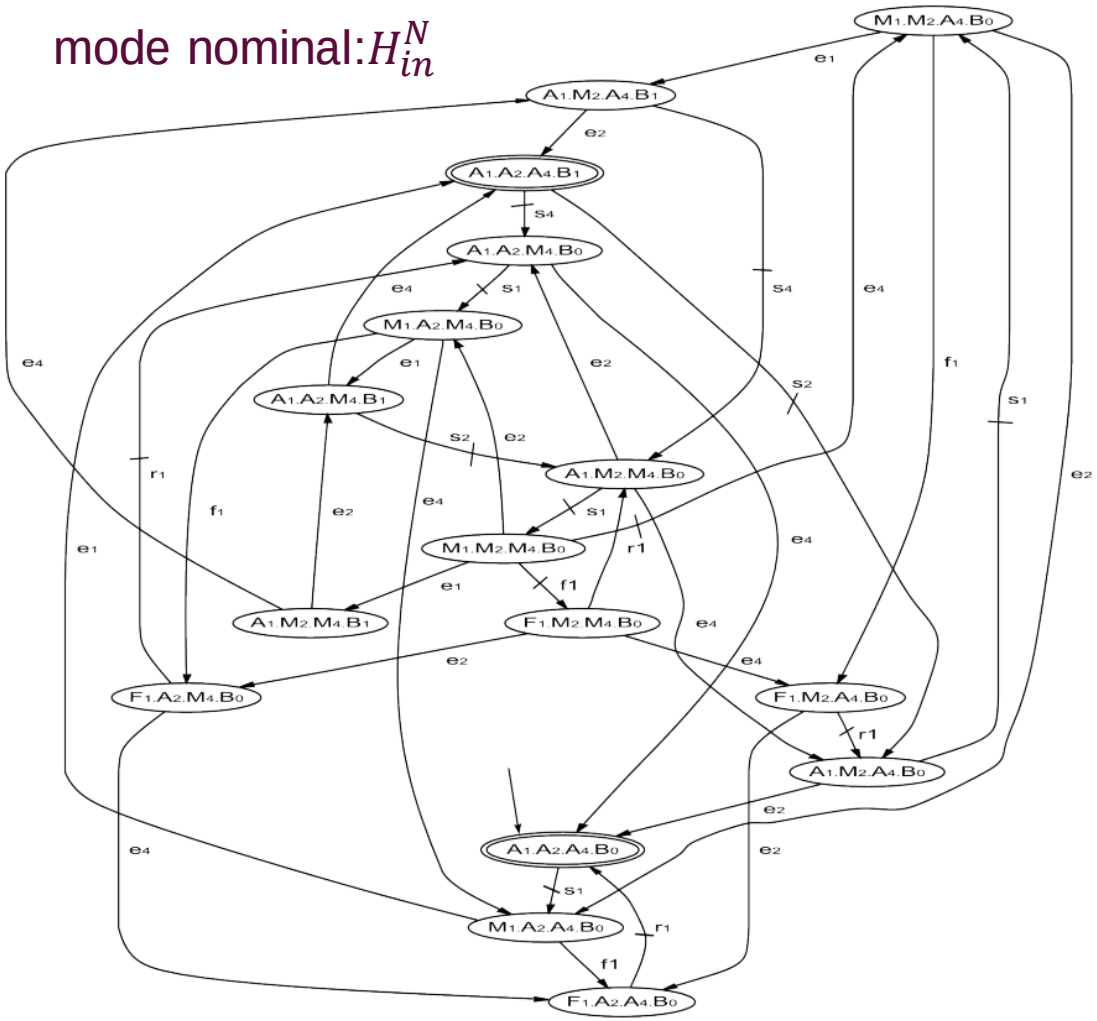
➢ Modèles de spécifications: limitation du stock





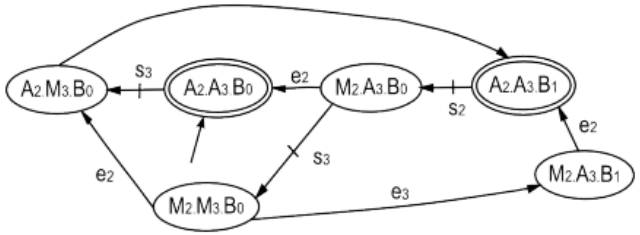
Étude intramodale

mode nominal: H_{in}^{N}



- Outils utilisés:
  - DESUMA [Ric06]
  - Supremica [Ake06]

mode dégradé: H_{in}^{D}



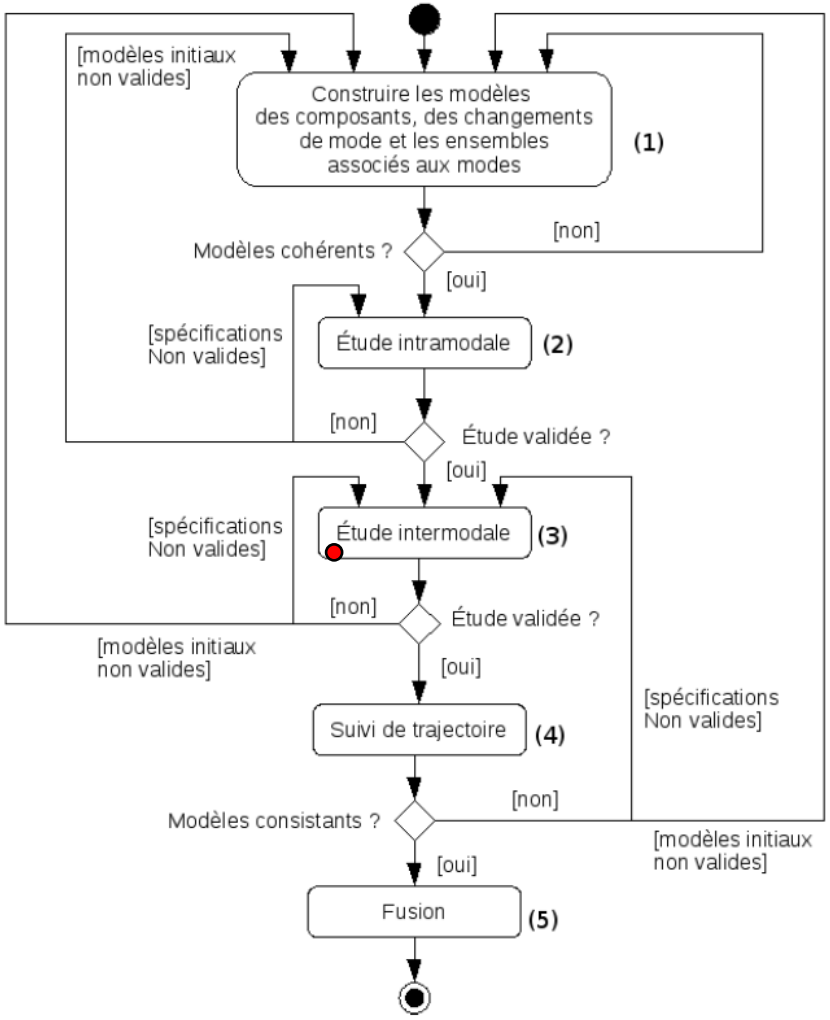
- Le langage peut être vide ou trop restreint:
  - Spécifications trop restrictive, dynamique des composants trop limité ou problème de contrôlabilité

⇒ Revoir le cahier des charges

- Permet de détecter les premières erreurs de conception

Étude Intermodale

1. Formalisation du cahier des charges
   - Construction des modèles
   - Validation de la cohérence
2. Étude Intramodale
   - Construction des procédés sous contrôle interne
   - validation des spécifications intramodales
3. Étude Intermodale
   - Construction des procédés sous contrôle
   - validation des spécifications intermodales



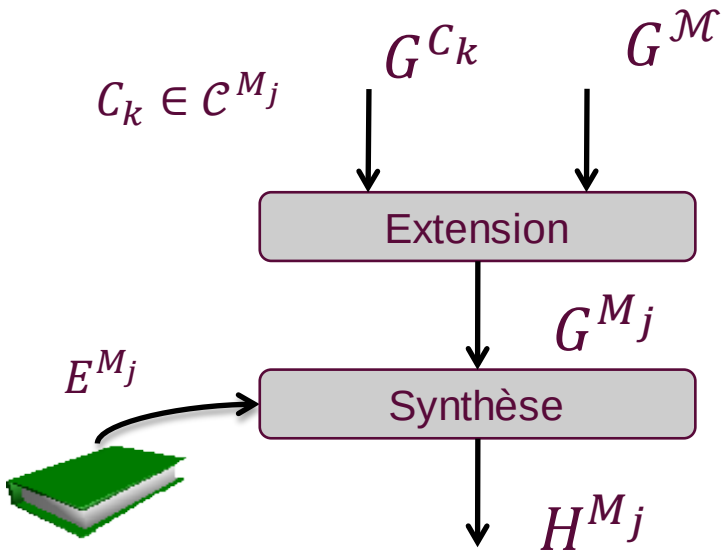
Étude Intermodale

- Objectif : construire le modèle représentant le comportant interne et le comportement commutatif dans chaque mode

  - Étendre les modèles en prenant en compte les composants générant un comportement commutatif

  - Ajouter l'automate de mode pour identifier le mode en cours et inclure une séquence de modes

$$G^{M_j} = G^{\mathcal{M}} \parallel_{C_k \in \mathcal{C}^{M_j}} G^{C_k}$$



  - Réutiliser les spécifications validées à l'étape précédente

  - Ajouter des spécifications de commutation

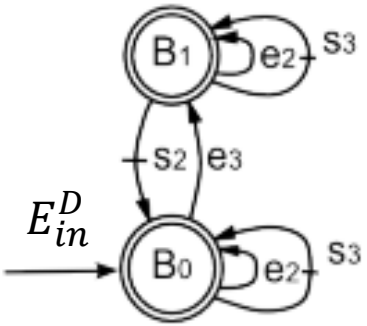
$$E^{M_j} = E_{\circlearrowleft}^{M_j} \times E_{\rightleftarrows}^{M_j}$$

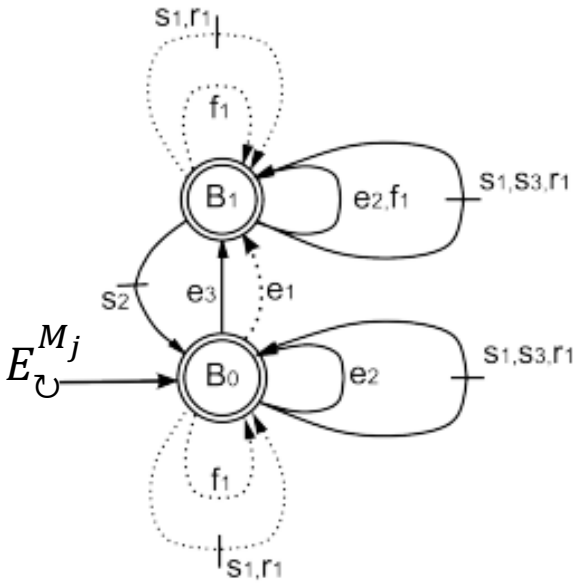
$$L_m(H^{M_j}) = \left[L_m\left(G^{M_j} \times E^{M_j}\right)\right]^{\uparrow c}$$

Étude Intermodale: spécifications intermodales

- Modèles des spécifications intermodales: $E^{M_j} = E_{\circlearrowleft}^{M_j} \times E_{\rightleftarrows}^{M_j}$
  - Spéficiations intramodales étendues
  - Spécifications de commutations

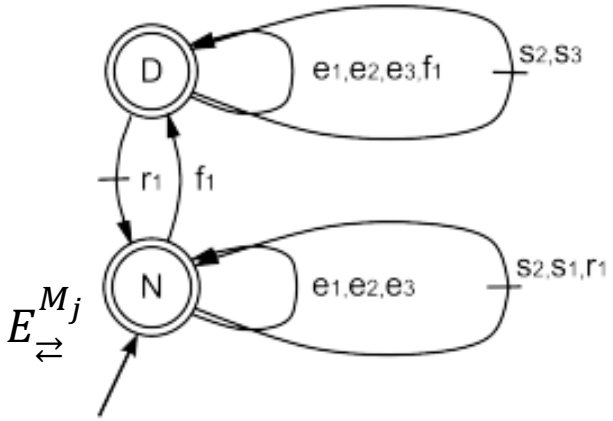
- Rappel spécification intramodale:
  - limitation du stock





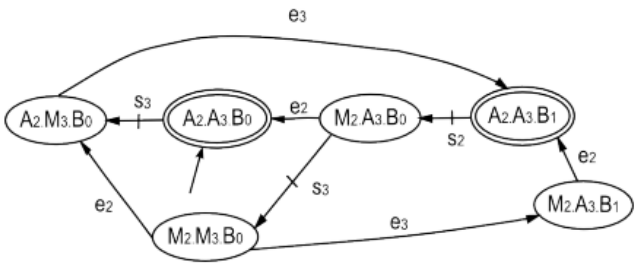
- Ajout du composant C_1

- Spécification de commutation
  - Redondance des composants

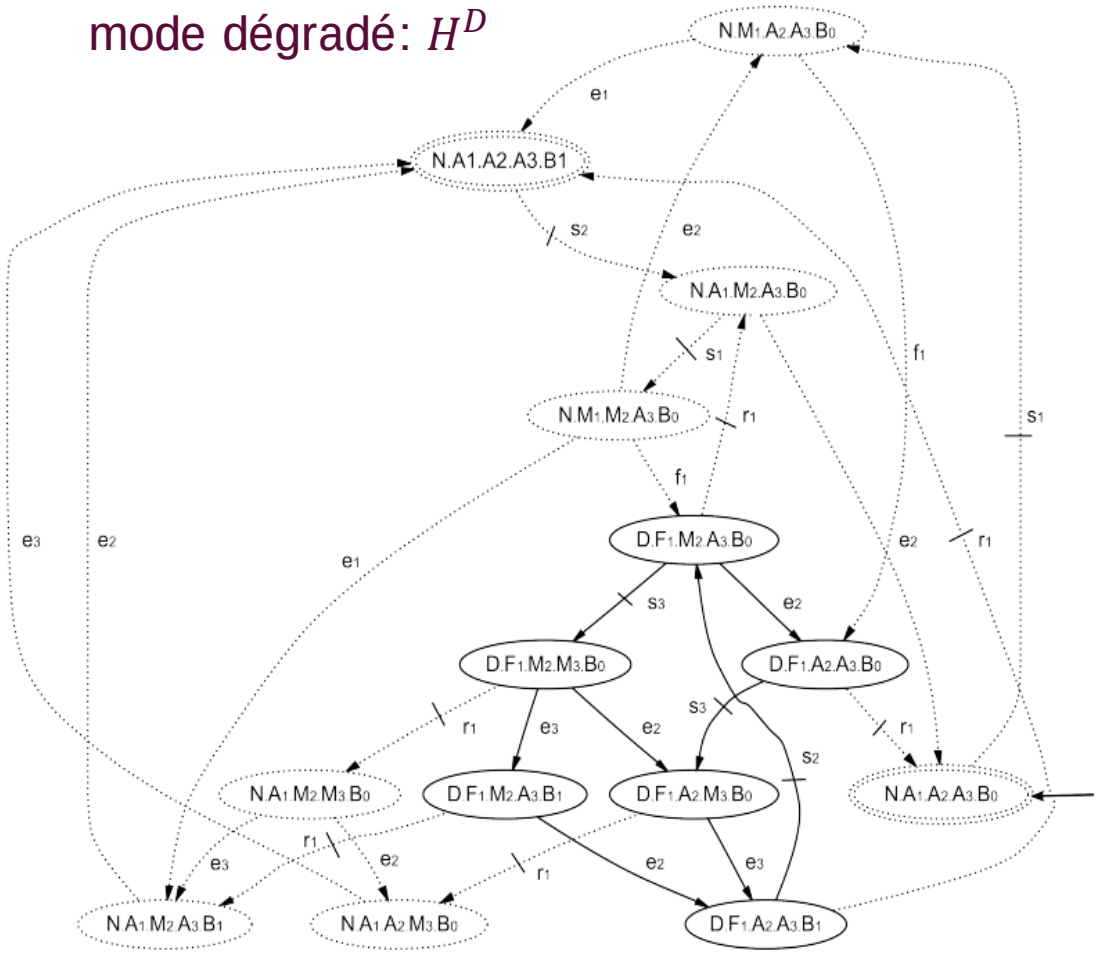


Étude Intermodale

mode dégradé: H_{in}^{D}



mode dégradé: H^{D}



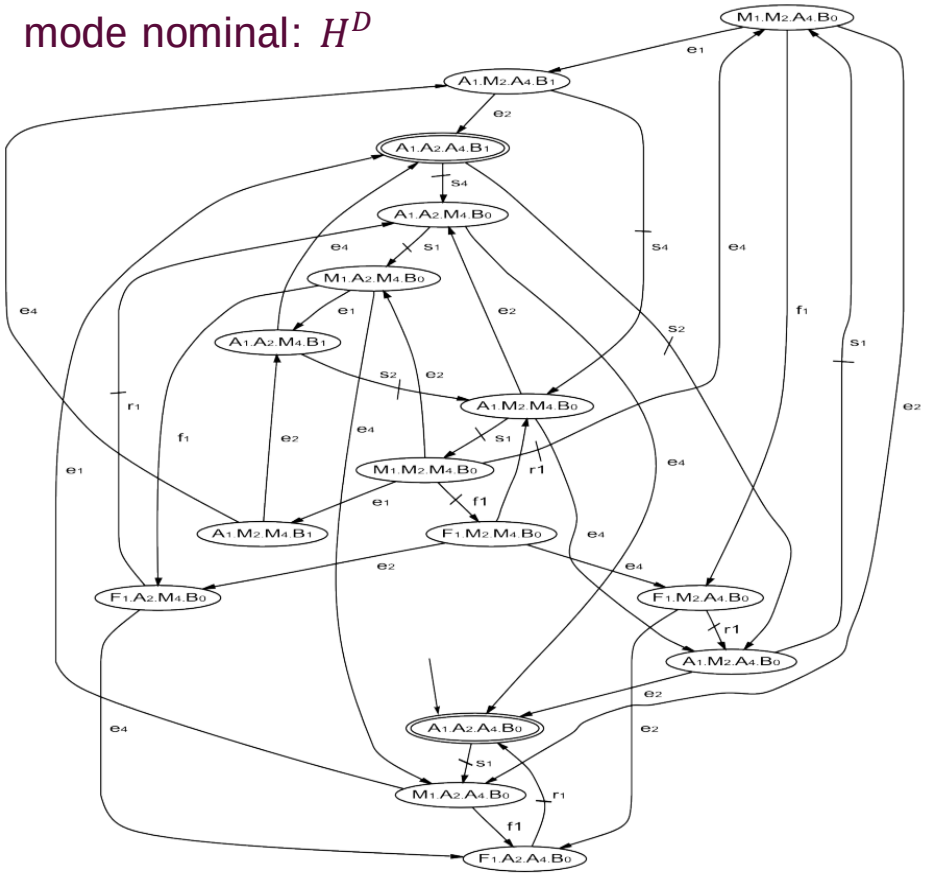
- Le langage est-il vide ou trop restreint ?
- Si nécessaire : revoir les spécifications de commutations

Étude Intermodale

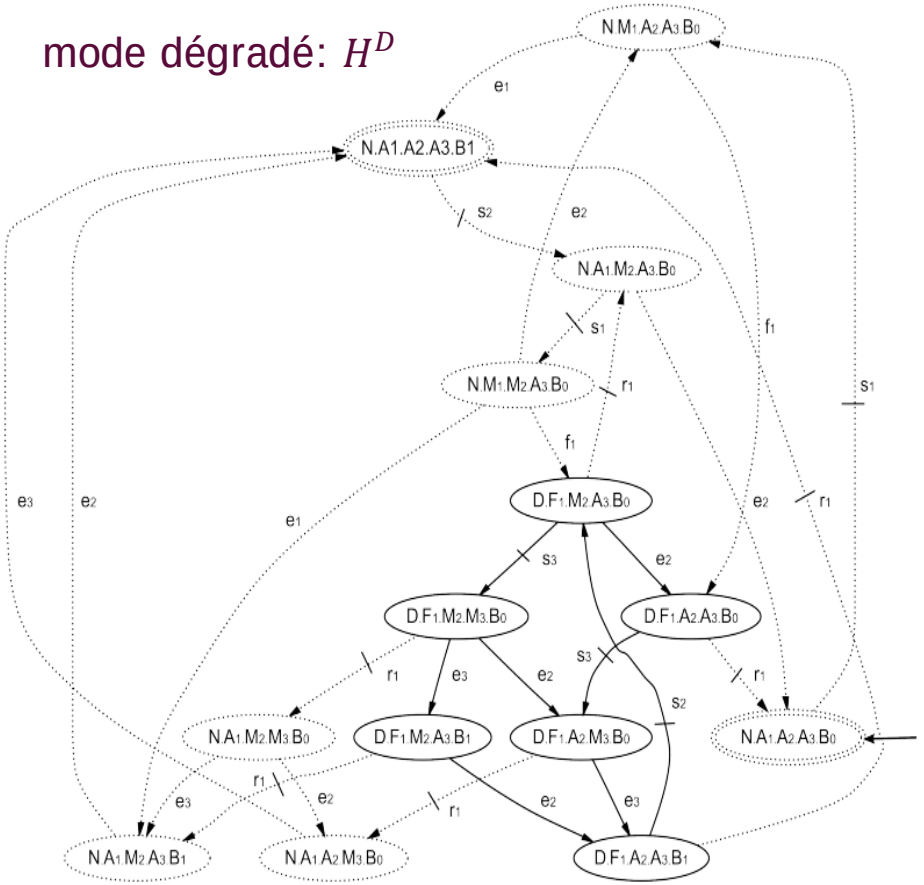
Remarque

- Les modèles construits sont:
  - Sûrs par construction (TCS)
  - Respectent les spécifications internes et de commutations

mode nominal: H^D

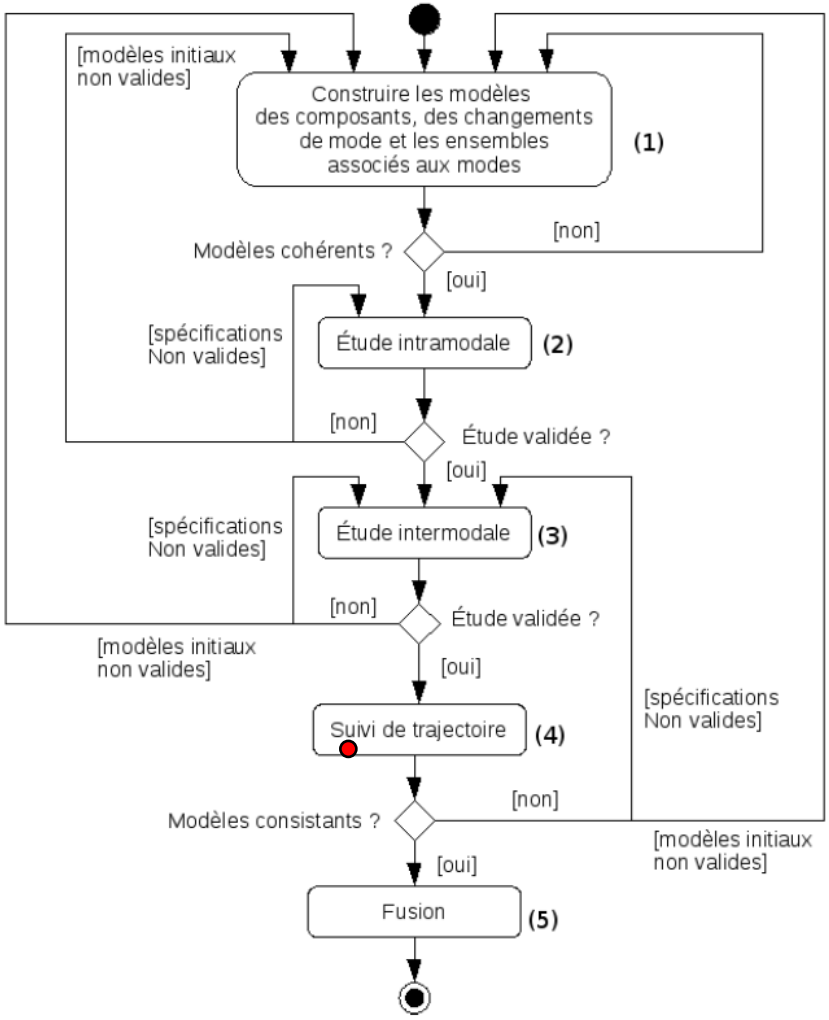


mode dégradé: H^D



Suivi de trajectoires

1. Formalisation du cahier des charges
   - Construction des modèles
   - Validation de la cohérence
2. Étude Intramodale
   - Construction des procédés sous contrôle interne
   - validation des spécifications intramodales
3. Étude Intermodale
   - Construction des procédés sous contrôle
   - validation des spécifications intramodales étendues et de commutation
4. Suivi de trajectoire
   - Suivi de trajectoire
   - Vérifications des commutations entre modes



Suivi de trajectoires

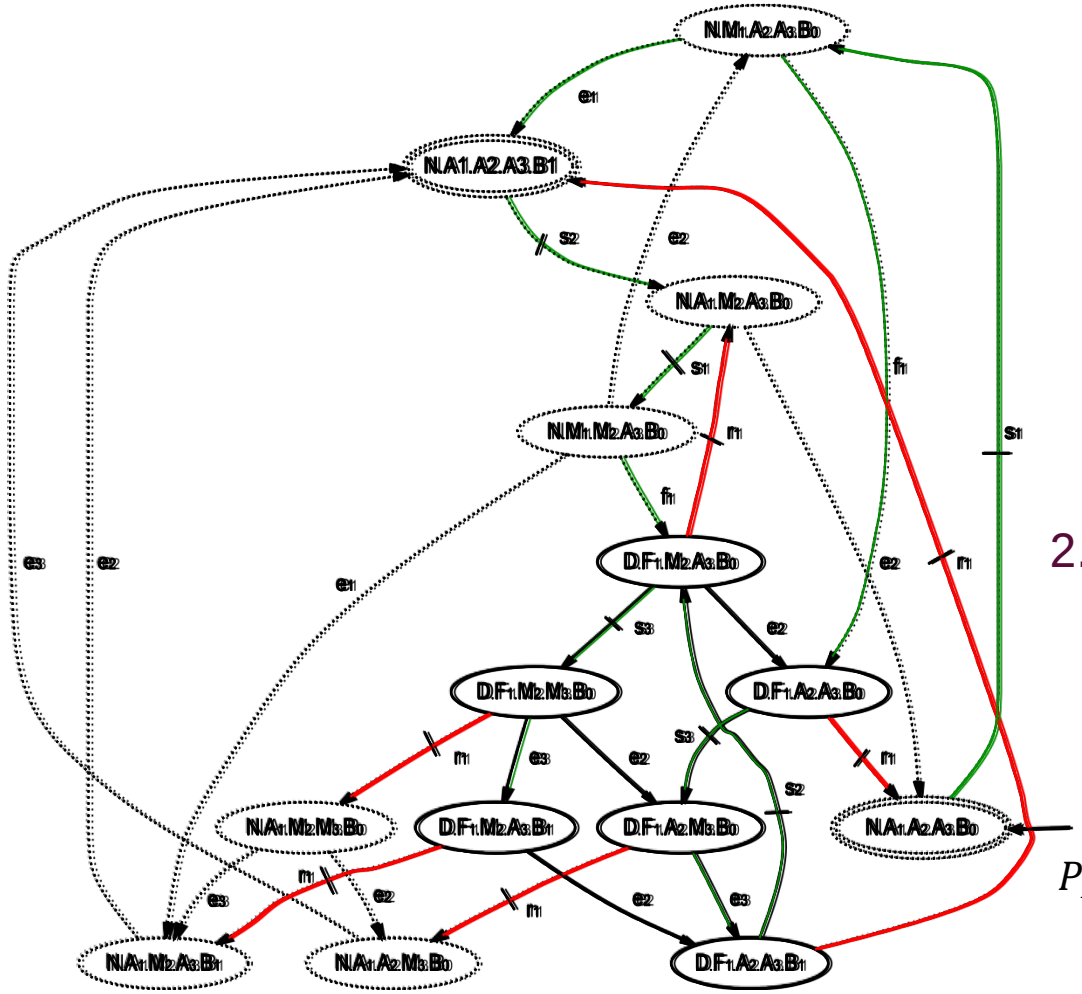
- Objectif:
  - ✓ Identifier les trajectoires menant à une commutation et s'assurer qu'entre modèle la commutation est effective

- Procédure : pour chaque événement de commutation tq : $\delta^{\mathcal{M}}(M_j, \alpha) = M_k$

1. Pour chaque état où une commutation est générée : $y \in Y^{M_j}_{M_j \xrightarrow{\alpha} M_k}$
   a. Calcul du langage menant à cet état : $L^{y}_{M_j \xrightarrow{\alpha} M_k}(H^{M_j})$
   b. Calcul du langage projeté : $L^{y}_{M_j \xrightarrow{\alpha} M_k}(H^{M_k})$
   c. Vérification de la propriété de comptabilité : $L^{y}_{M_j \xrightarrow{\alpha} M_k}(H^{M_k}) \subseteq L(H^{M_k})$
   d. Vérification de la consistance :
   $\exists y' \in Y^{M_j}_{M_j \xrightarrow{\alpha} M_k} (y \neq y' \Leftrightarrow L^{y}_{M_j \xrightarrow{\alpha} M_k}(H^{M_k}) \cap L^{y'}_{M_j \xrightarrow{\alpha} M_k}(H^{M_k}) = \emptyset$

Suivi de Trajectoire

H^D



1. Recherche le langage de toutes les trajectoires admissible menant à un événement r_1 :
   - $s_1 \cdot f_1$
   - $s_1 \cdot f_1 \cdot s_3 \cdot e_3$
   - $s_1 \cdot e_1 \cdot s_2 \cdot s_1 \cdot f_1 \cdot s_3$
   - $s_1 \cdot e_1 \cdot s_2 \cdot s_1 \cdot f_1 \cdot s_3 \cdot e_3$
   - $s_1 \cdot f_1 \cdot s_3 \cdot e_3 \cdot s_2$

2. Fonction de projection étendue

$$P_{M_j,M_k}: \Sigma^{M_j*} \rightarrow \Sigma^{M_k*}, \forall \sigma \in \Sigma^{M_j} \wedge \forall s \in \Sigma^{M_j*}:$$

$$P_{M_j,M_k}(\varepsilon) = \varepsilon$$

$$P_{M_j,M_k}(s\sigma) = \begin{cases} P_{M_j,M_k}(s)\sigma & si \quad \sigma \in \Sigma^{M_j} \cap \Sigma^{M_k} \\ P_{M_j,M_k}(s) & si \quad \sigma \in \Sigma^{M_j} \setminus \Sigma^{M_k} \end{cases}$$

Suivi de Trajectoire

2. Projection sur Σ^{N*} avec $\Sigma^N = \{s_1, e_1, f_1, r_1, s_2, e_2, s_4, e_4\}$

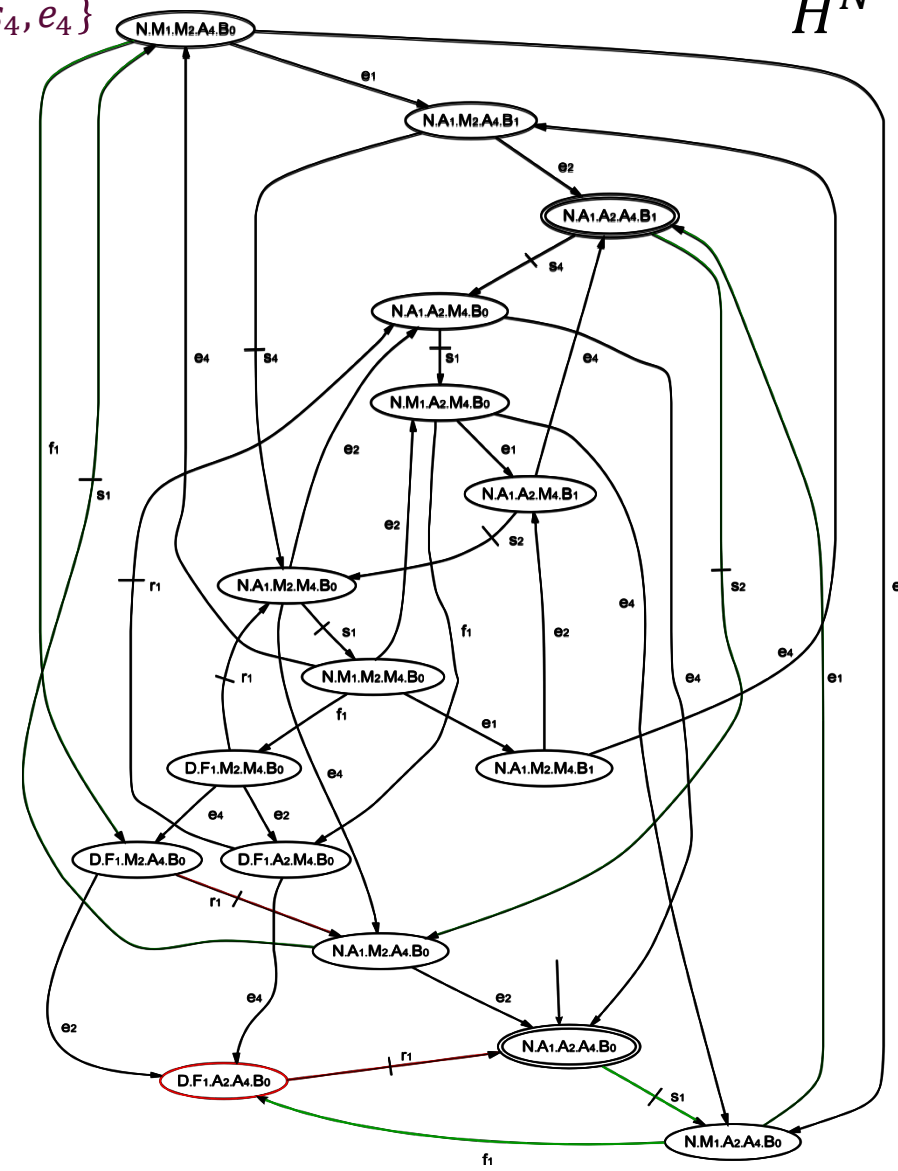
- $s_1 \cdot f_1 \longrightarrow s_1 \cdot f_1$
- $s_1 \cdot f_1 \cdot s_3 \cdot e_3 \longrightarrow s_1 \cdot f_1$
- $s_1 \cdot e_1 \cdot s_2 \cdot s_1 \cdot f_1 \cdot s_3 \longrightarrow s_1 \cdot e_1 \cdot s_2 \cdot s_1 \cdot f_1$
- $s_1 \cdot e_1 \cdot s_2 \cdot s_1 \cdot f_1 \cdot s_3 \cdot e_3 \longrightarrow s_1 \cdot e_1 \cdot s_2 \cdot s_1 \cdot f_1$
- $s_1 \cdot f_1 \cdot s_3 \cdot e_3 \cdot s_2 \longrightarrow s_1 \cdot f_1 \cdot s_2$

Inconsistance

$\notin L(H^N)$

Incompatibilité

H^N



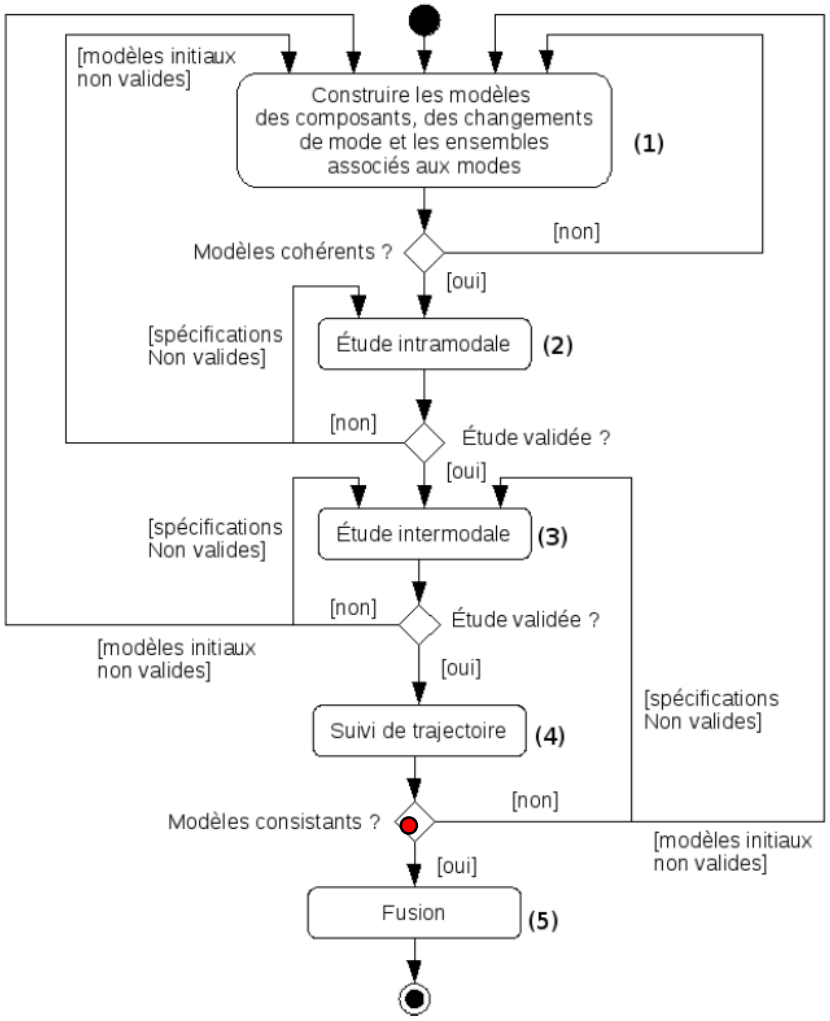
➢ Nécessite l'ajout de spécifications:

1. Machines non communes à l'arrêt
2. Stock à zéro avant une réparation

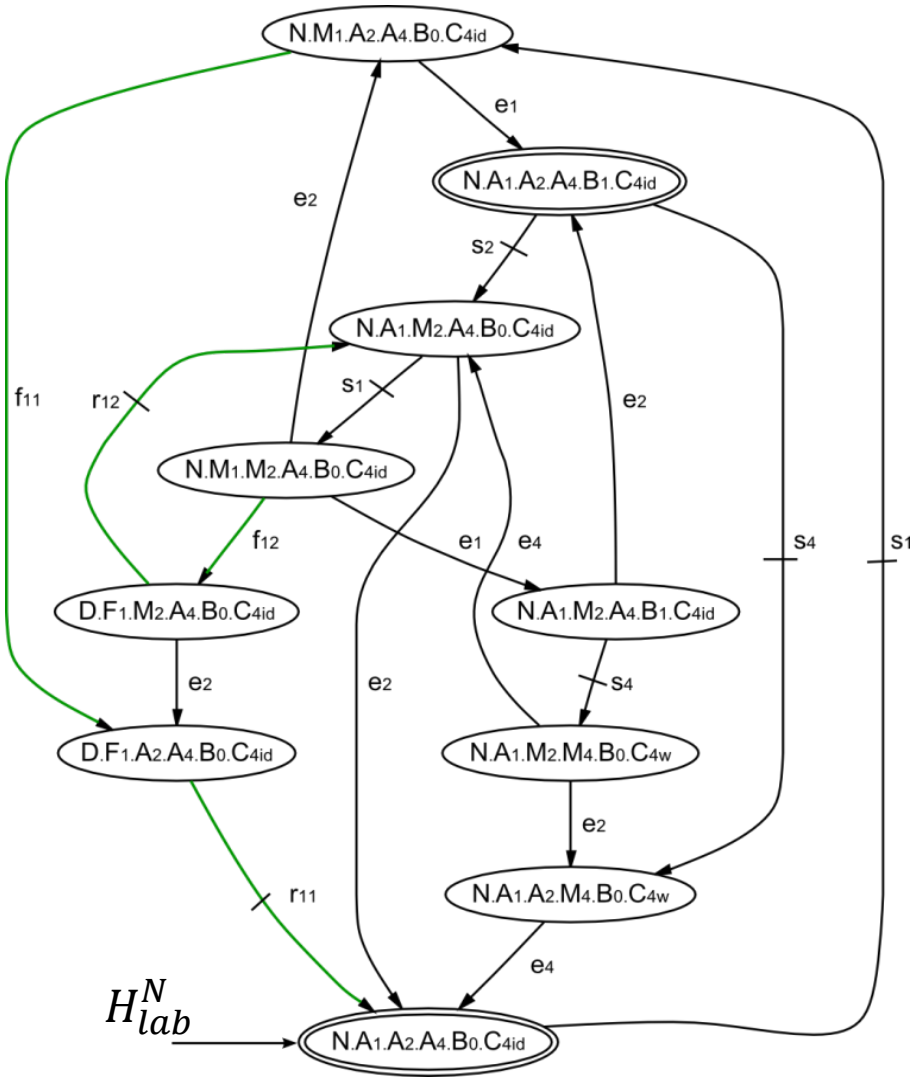
Modèles non consistants

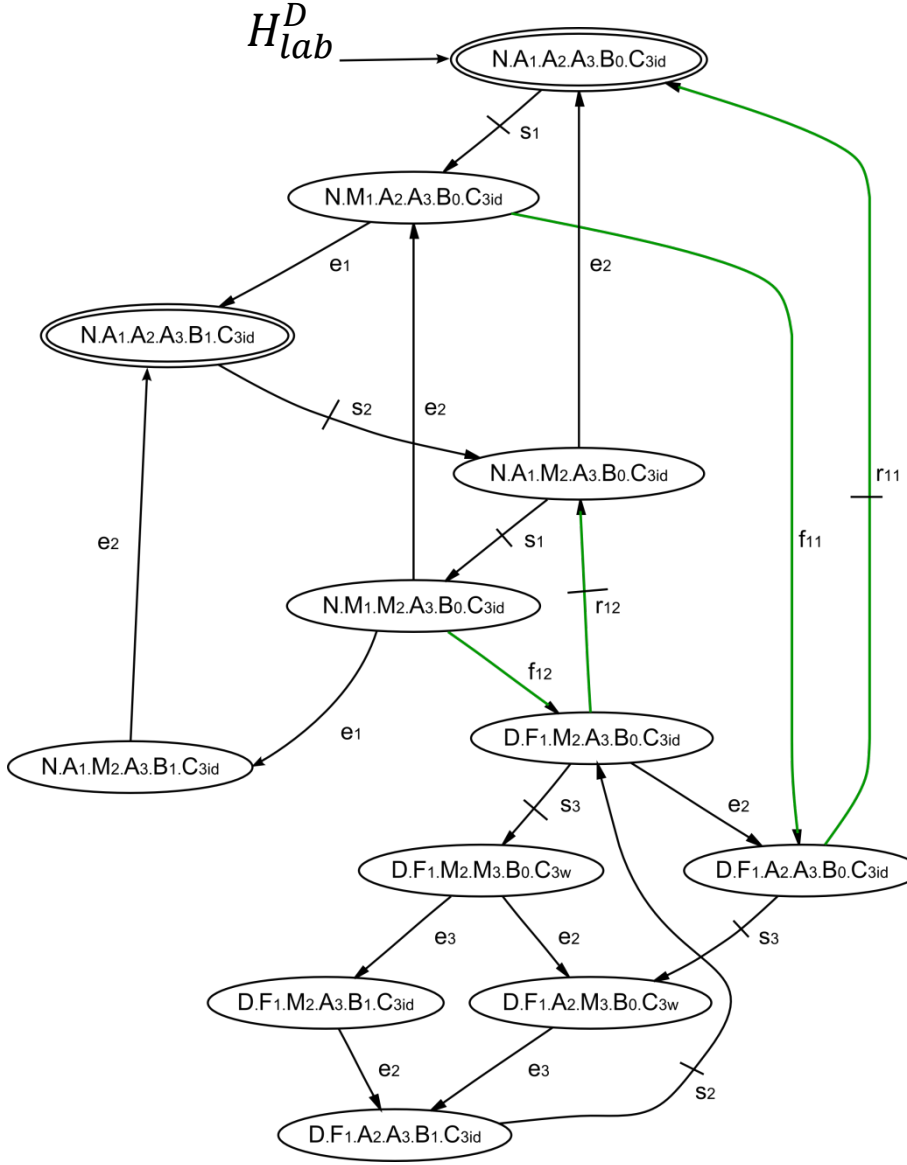
1. Formalisation du cahier des charges
   - Construction des modèles
   - Validation de la cohérence
2. Étude Intramodale
   - Construction des procédés sous contrôle interne
   - validation des spécifications intramodale
3. Étude Intermodale
   - Construction des procédés sous contrôle
   - validation des spécifications intramodale étendue et de commutation
4. Suivi de trajectoire
   - Suivi de trajectoire
   - Vérifications des commutations entre modes

✓ Retour à l'étude intermodale



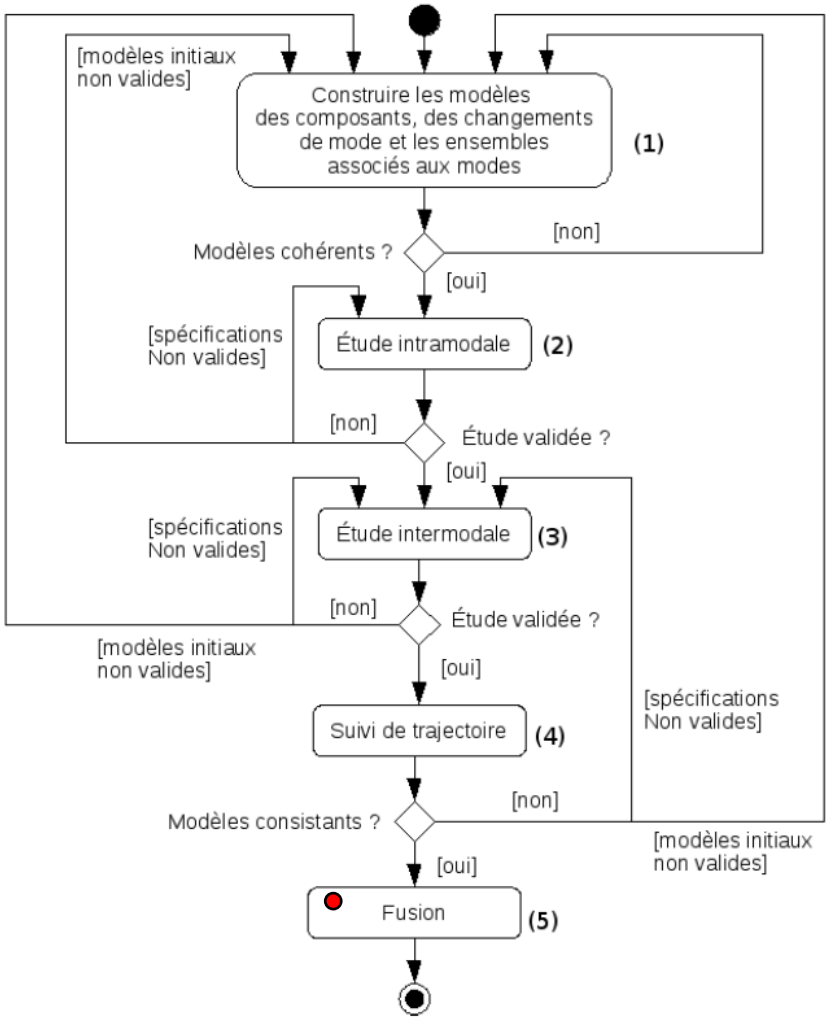
Modèles consistants





Fusion des états

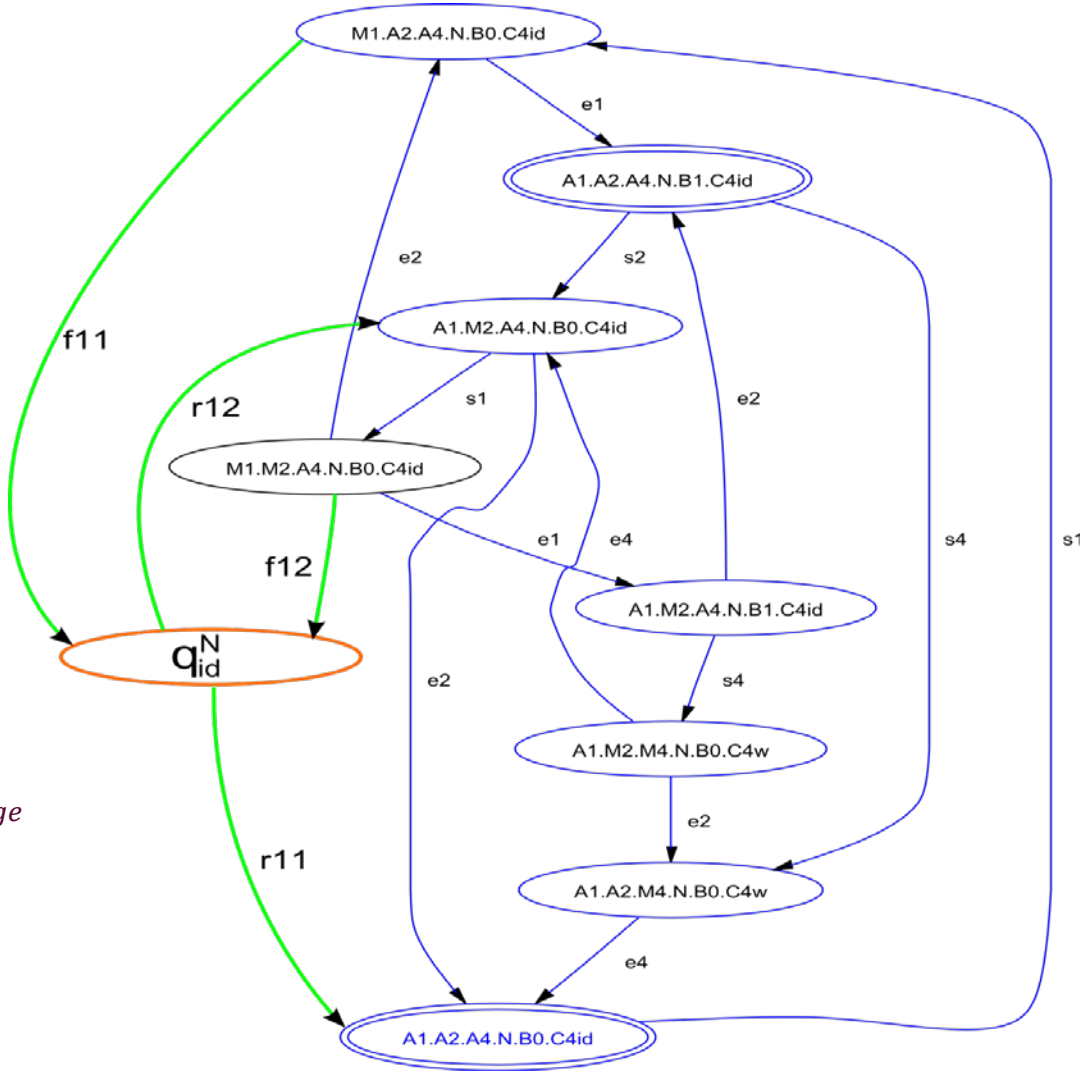
1. Formalisation du cahier des charges
   - Construction des modèles
   - Validation de la cohérence
2. Étude Intramodale
   - Construction des procédés sous contrôle interne
   - validation des spécifications intramodale
3. Étude Intermodale
   - Construction des procédés sous contrôle
   - validation des spécifications intramodale étendue et de commutation
4. Suivi de trajectoire
   - Suivi de trajectoire
   - Vérifications des commutations entre modes
5. Fusion d'états
   - regroupement des états non significatifs



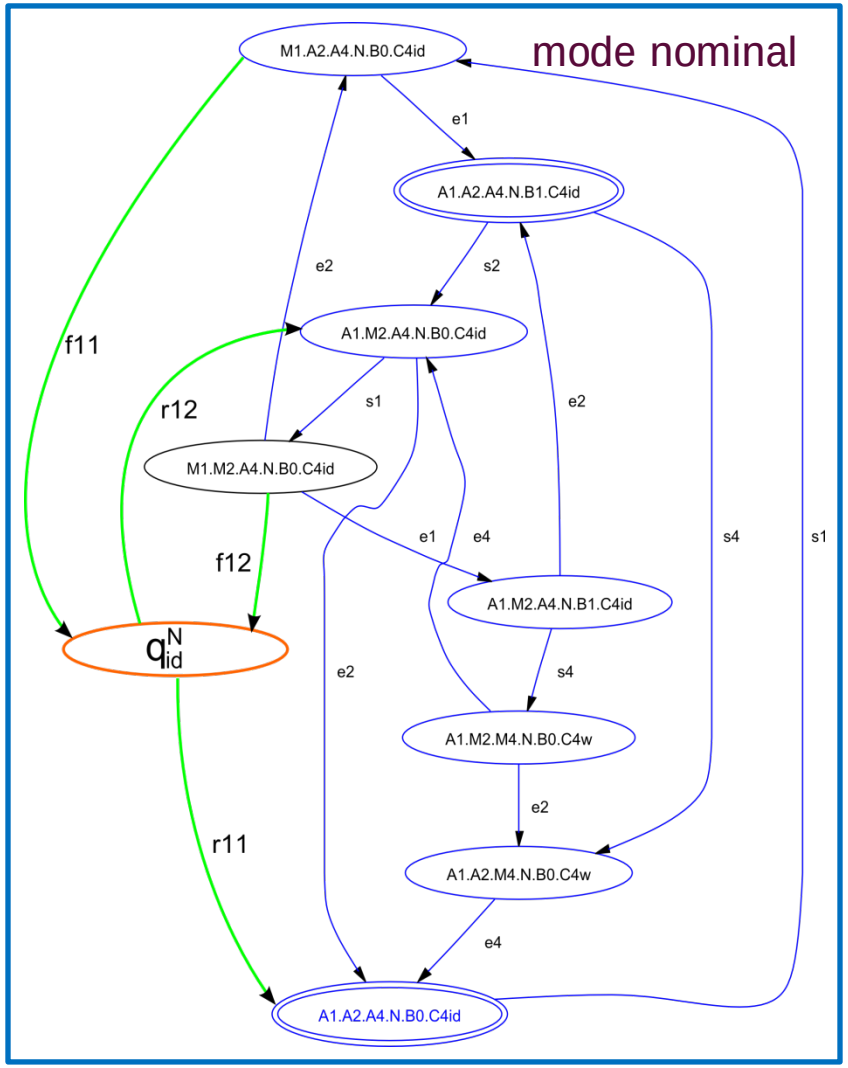
Fusion des états non significatifs

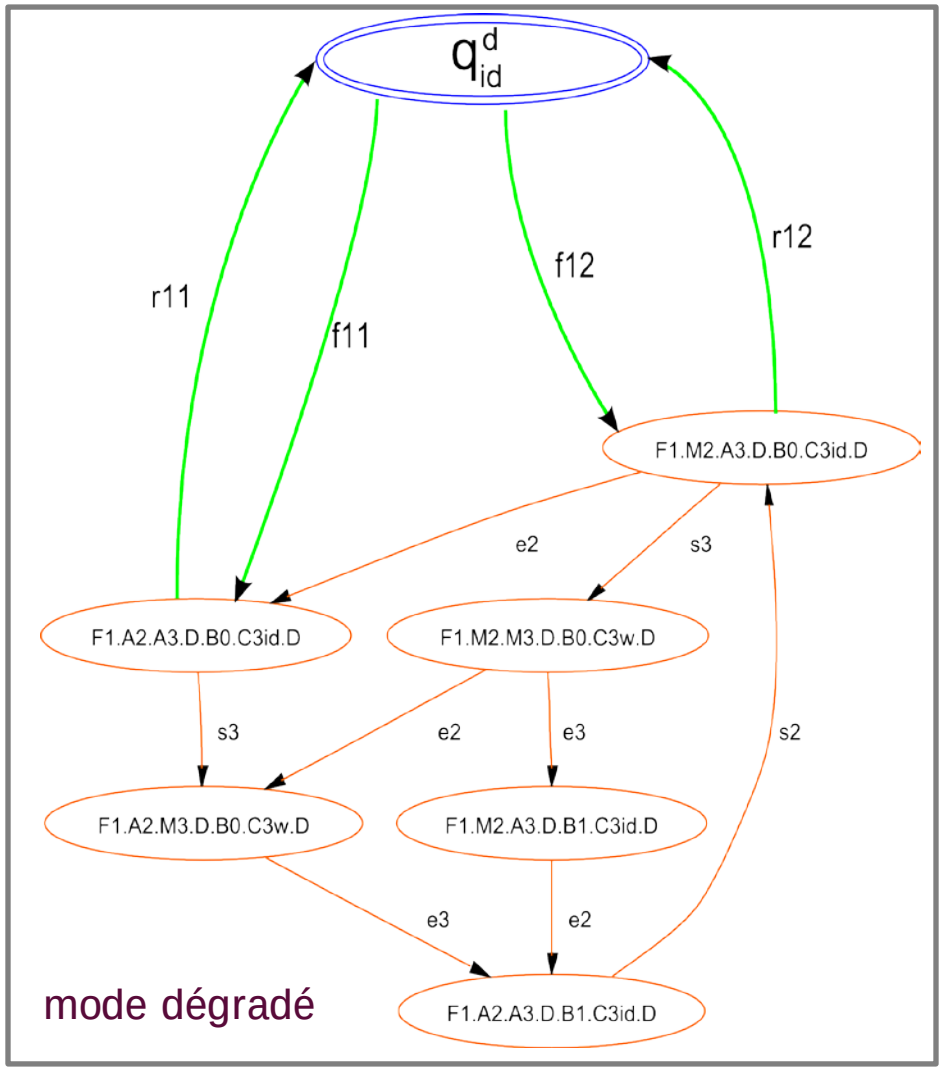
- Un modèle par mode
  - Chaque modèle représente le comportement interne et les commutations admissibles dans le mode concerné

- Procédure:
  a. Détermination de l'ensemble des états à fusionner : $Y_{mer}^{M_j} \subset Y_{lab}^{M_j}$
  b. Tous les états de $Y_{mer}^{M_j}$ sont remplacés par un état inactif $y_{id}^{M_j}$
  c. Si $y_{0,lab}^{M_j} \subset Y_{mer}^{M_j}$, alors $y_{0,merge}^{M_j} = y_{id}^{M_j}$
  d. Si $Y_{m,lab}^{M_j} \cap Y_{mer}^{M_j} \neq \emptyset$, alors $y_{id}^{M_j} \in Y_{m,merge}^{M_j}$



Modèles finaux : un par mode





Comparaison entre deux approches

- Équivalence de comportements entre l'approche centralisée et l'approche modale

- Objectif : $H_{cent} = \|_{M_j \in \mathcal{M}} H^{M_j}$

$H_{cent} = G_{cent} \parallel E_{cent}$

$H^{M_j} = G^{M_j} \parallel E^{M_j}$

$G_{cent} = G^{\mathcal{M}} \parallel (\|_{C_i \in \mathcal{C}} G^{C_i}$

$E_{cent} = \|_l E^l$

$G^{M_j} = G^{\mathcal{M}} \|_{C_k \in \mathcal{C}^{M_j}} G^{C_k}$

$E^{M_j} = \|_k \left(E^{k,M_j}\right)$

$G_{cent} \parallel E_{cent} = \|_{M_j \in \mathcal{M}} (G^{M_j} \parallel E^{M_j})$

Comparaison entre deux approches: un par mode

- Équivalence de comportements des procédés: $G_{cent} = \|_{M_j \in \mathcal{M}} (G^{M_j})$
  - ✓ Vrai si $\mathcal{C} = \bigcup_{M_j \in \mathcal{M}} \mathcal{C}^{M_j}$

- Équivalence de spécifications: $E_{cent} = \|_{M_j \in \mathcal{M}} (E^{M_j})$
  - ✓ Vrai si spécifications indépendante du mode
  - ✖ Si dépendante du mode : impossible à dire sans une vérification

$$E_{cent} == (E^{M_1} \| E^{M_2} \| E^{M_3} \| \cdots \| E^{M_j})$$

- En considérant plusieurs spécifications : $\|_k E^k = \|_k (\|_{M_j \in \mathcal{M}} E^{k,M_j})$

Conclusion

- **Démarche d'aide à la conception**
  - ✓ Modèles sûrs par construction
  - ✓ Validation étape par étape des modèles obtenus
  - ✓ Complètement définies
- **Commutations sûres entre modes**
  - ✓ Suivi de trajectoire entre modèles
  - ✓ Caractérisation des trajectoires de commutations
  - ✓ Identification des commutations problématiques pour aider à leur résolution
- **Démarche mathématiquement définie**
  - ✓ Démontrer les propriétés de sécurité des modèles
  - ✓ Automatiser la démarche pour traiter des systèmes de grandes tailles

Perspectives

- **Réduire la complexité** *(lors de l'étude intermodale)*
  - Abstraction de modèles
- **Automatisation complète de la démarche**
  - Difficulté à calculer le langage d'un automate
  - Algorithme de suivi de trajectoire n'utilisant pas les langages
- **Extension sur l'automate de mode**
  - Niveau hiérarchique
- **Démarche d'aide à la détermination des modes d'un système**
  - Extension de la démarche en amont

Ampère
Unité Mixte de Recherche CNRS
Génie Électrique, Électromagnétisme, Automatique, Microbiologie environnementale et Applications

Commutations sûres de modes pour les systèmes à événements discrets

Présentée par : **Gregory FARAUT**

MERCI

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE
Lyon 1
INSA LYON