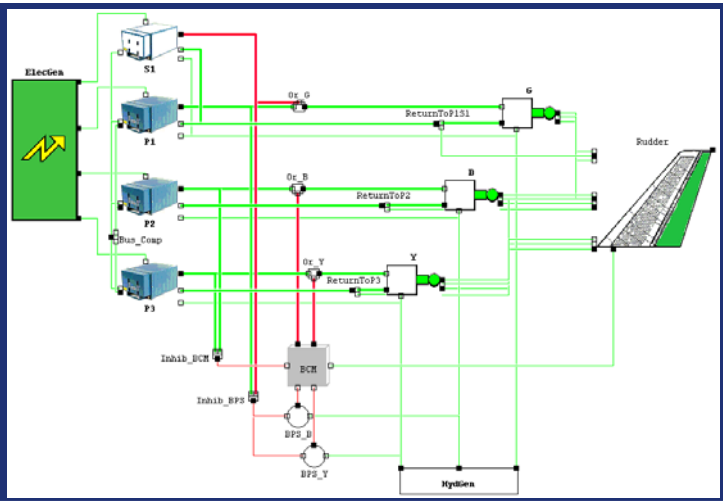
Présenté par

BERNARD Romain (Airbus, EAT)

Encadrants:
ZEITOUN Marc, GRIFFAULT Alain (LaBRI)
BIEBER Pierre (ONERA)
METGE Sylvain (Airbus, EADA)



Analyses de Sûreté de Fonctionnement multi-systèmes

Troisièmes Journées AltaRica - 2007

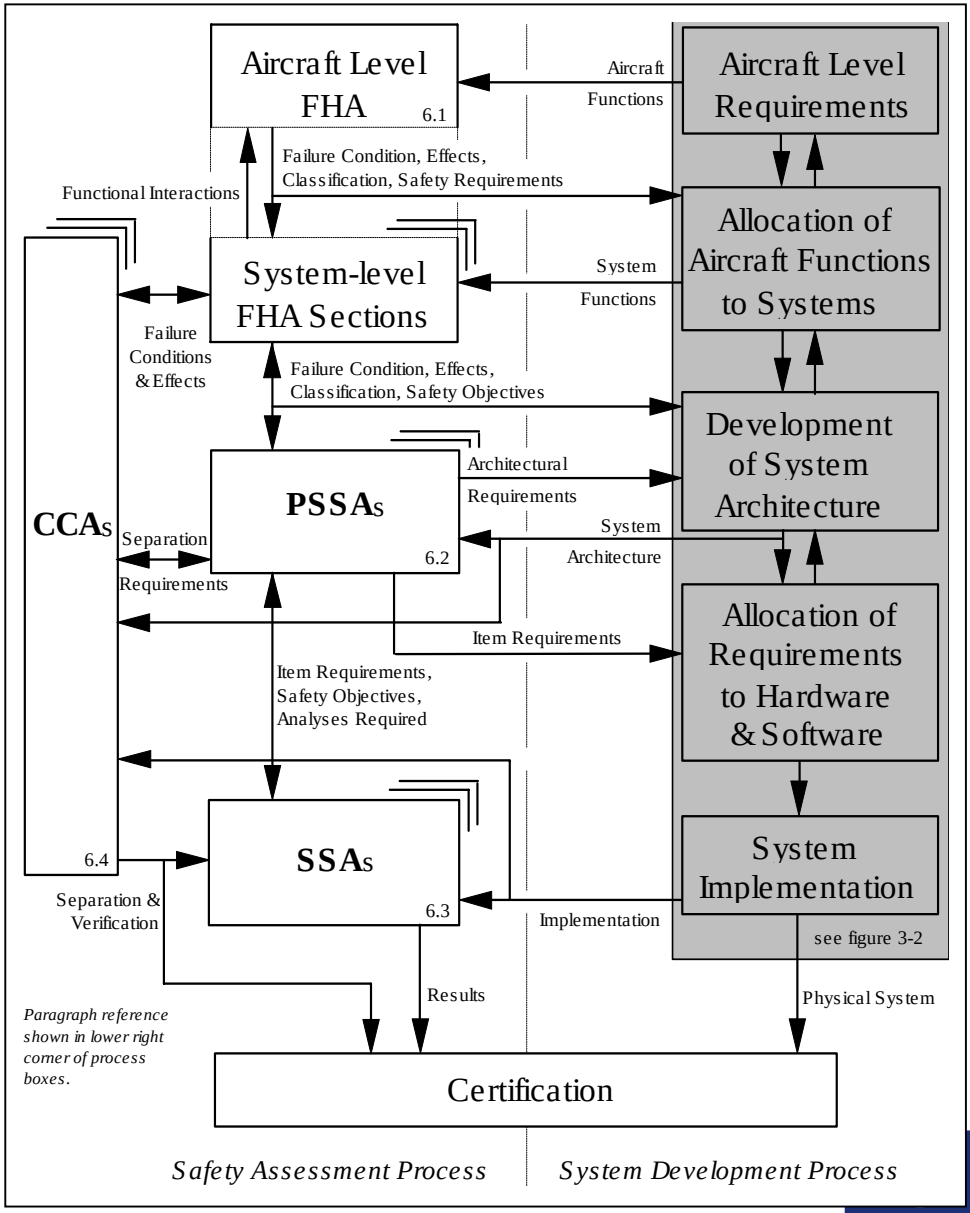
AIRBUS

Sommaire

1. Processus SdF actuel
2. Approche de modélisation
3. Cas d'étude
4. Raffinement
5. Conclusion

Évaluation de la sûreté de fonctionnement (SdF)

- Afin d'obtenir la Certification, Airbus doit prouver aux autorités que les exigences de sûreté de fonctionnement sont satisfaites.
- Le processus commence au niveau avion par l'identification des fonctions nécessaires, suivi par l'allocation des fonctions sur les systèmes de l'avion.
- Pour chaque fonction sont définies les situations redoutées , appelées Failure Conditions (FC).
- Les FC sont classifiées en fonction de la gravité des conséquences.
- Les ingénieurs SdF ont la responsabilité d'évaluer que chaque architecture de système proposée répond aux exigences liées à la classification de la FC.



Processus SdF actuel

Identification des fonctions Avion

Conception de l'architecture du système

Validation d'Architecture

Preliminary System Safety Assessment

Safety contribution

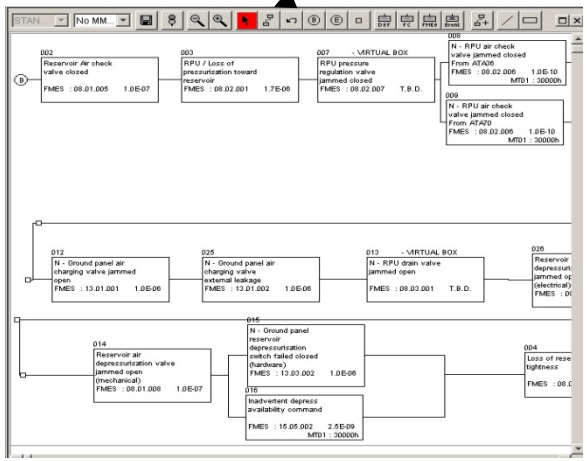
Functional **H**azard **A**ssessment

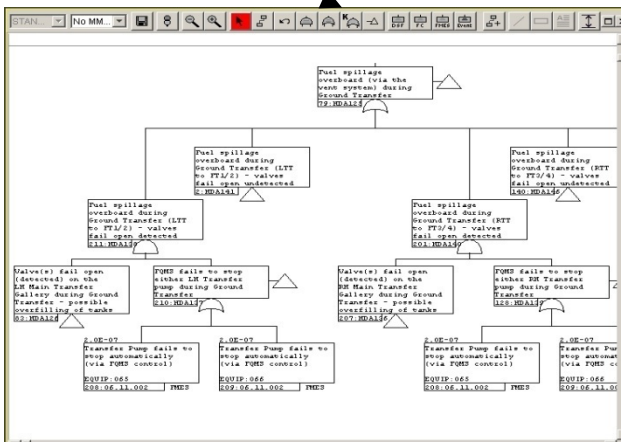
Description textuelle
+
Diagrammes d'architecture

Diagrammes de dépendances
Arbres de fautes (FT)

Coupes minimales
Quantification

1 2 3 4





Limitations identifiées

- Limitations des formalismes actuels:
  - Lisibilité difficile pour des non-spécialistes

  → validation par les concepteurs et communication impactées
  - Insuffisant pour comprendre le comportement d'un système:
    - Les aspects dynamiques, qui ont un effet sur le comportement du système, ne sont pas clairement mis en avant.

- Limitations liées à l'évolution des architectures avion:
  - Les architectures sont de plus en plus complexes et intégrées

  → analyse exhaustive de plus en plus coûteuse
  - Les architectures peuvent évoluer

  → chaque analyse doit être vérifiée manuellement et éventuellement mise à jour

Sommaire

1. Processus SdF actuel
2. Approche de modélisation
   - Modèles de propagation de pannes
   - AltaRica
3. Cas d'étude
4. Raffinement

Modèles de propagation de pannes

- Les modèles de propagation de pannes (MPP) se focalisent sur:
  - Les occurrences, la propagation et les conséquences d'une défaillance
  - La détection d'erreurs
  - Les reconfigurations
- Dans le but de supporter les analyses de SdF:
  - Les MPP ne considèrent pas les valeurs réelles
  - Les MPP discrétisent les valeurs qui dénotent un état (d'une donnée, d'un composant...) suivant les modes de panne possibles:
    - correct : la valeur réelle est égale à la valeur nominale
    - perdu : la valeur réelle est très éloignée de la valeur nominale
    - erroné : la valeur réelle diffère légèrement de l'attente

Langage AltaRica : illustration

Description tabulaire d'un nœud AltaRica

State	Type	Initial Value
Status	{correct, erroneous, lost}	Correct

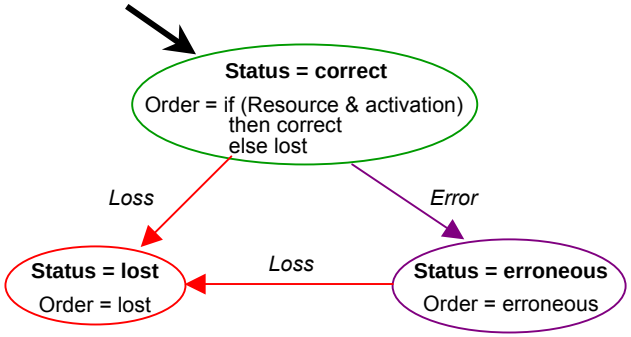
Flow	Type	Direction
Resource	Boolean	In
Activation	Boolean	In
Order	{correct, erroneous, lost}	Out

Event	Law	Law parameters
Loss	Constant	1e-4
Error	Constant	1e-5

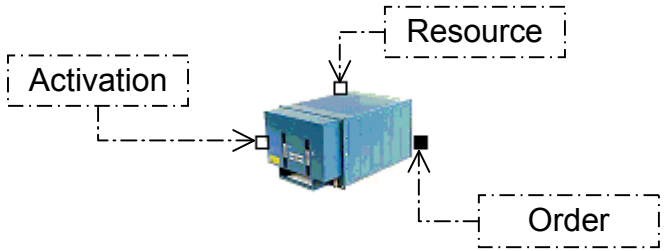
Event	Guard	New affectations
		Status
Loss	Status != lost	lost
Error	Status = correct	erroneous

Assertion	Case	Value
Order	Resource and Activation and Status = correct	correct
	Resource and Activation and Status = erroneous	erroneous
	Else	lost

Automate correspondant

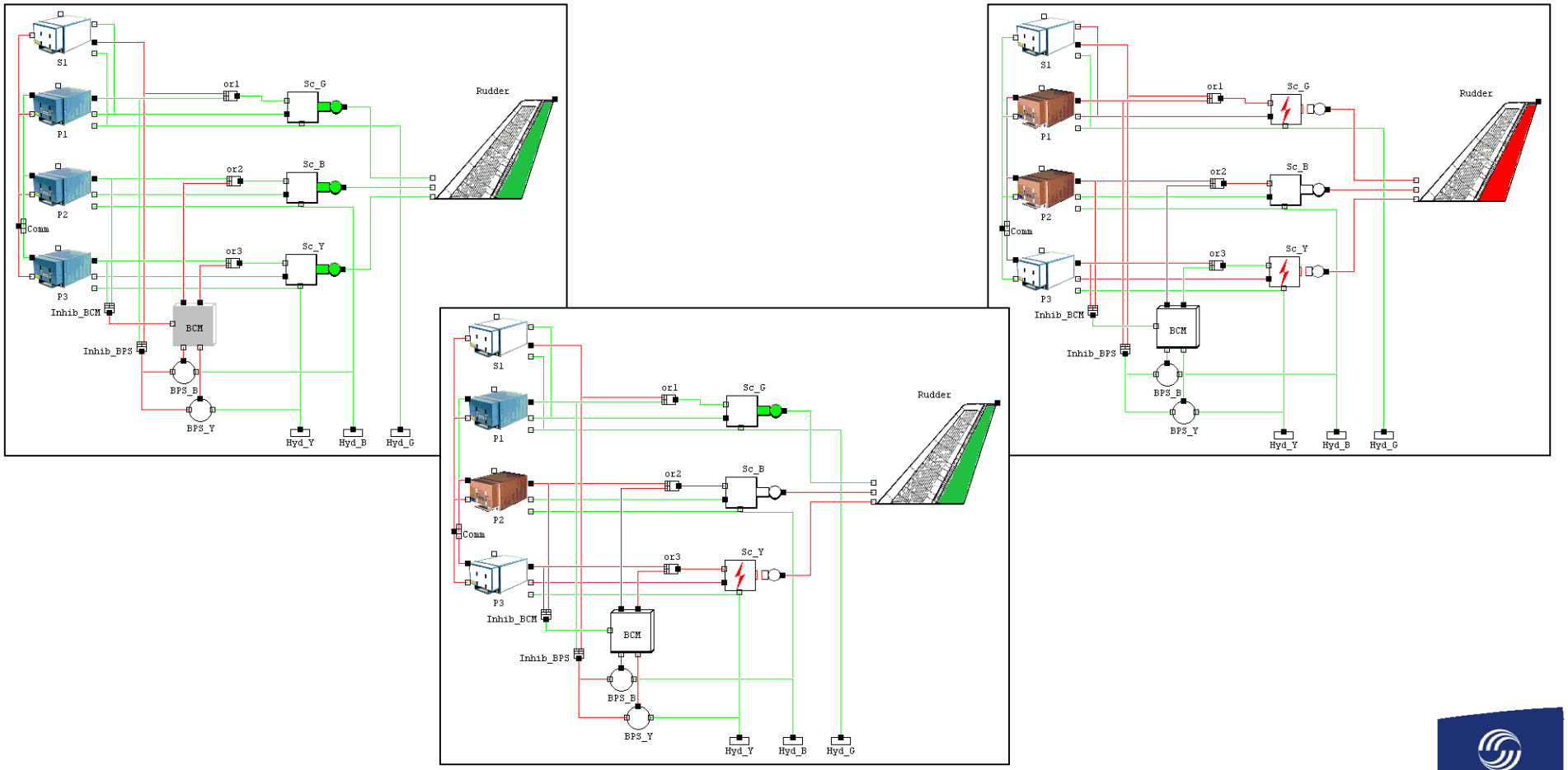


Représentation graphique du nœud AltaRica



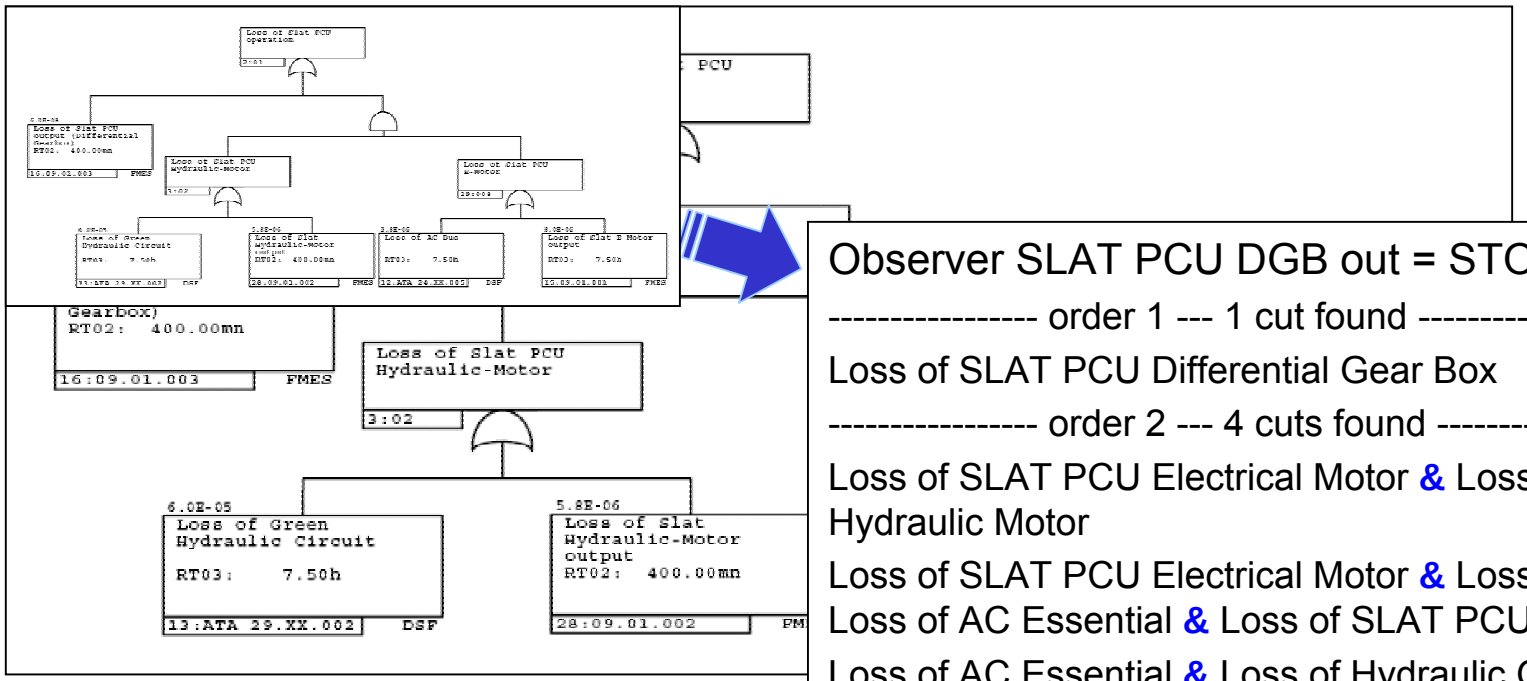
Outils d'analyse

- *Simulation interactive:*
  - animation de la représentation graphique, évolution des icônes des composants et des couleurs de liens après tirage d'un évènement



Outils d'analyse

- *Simulation interactive*
- *Génération d'arbre de faute*:
  - analyse exhaustive pour un événement redouté spécifié
    → Calcul des coupes minimales et des probabilités



Observer SLAT PCU DGB out = STOPPED:

---------- order 1 --- 1 cut found ----------

Loss of SLAT PCU Differential Gear Box

---------- order 2 --- 4 cuts found ----------

Loss of SLAT PCU Electrical Motor **&** Loss of SLAT PCU Hydraulic Motor

Loss of SLAT PCU Electrical Motor **&** Loss of Hydraulic Green

Loss of AC Essential **&** Loss of SLAT PCU Hydraulic Motor

Loss of AC Essential **&** Loss of Hydraulic Green

……

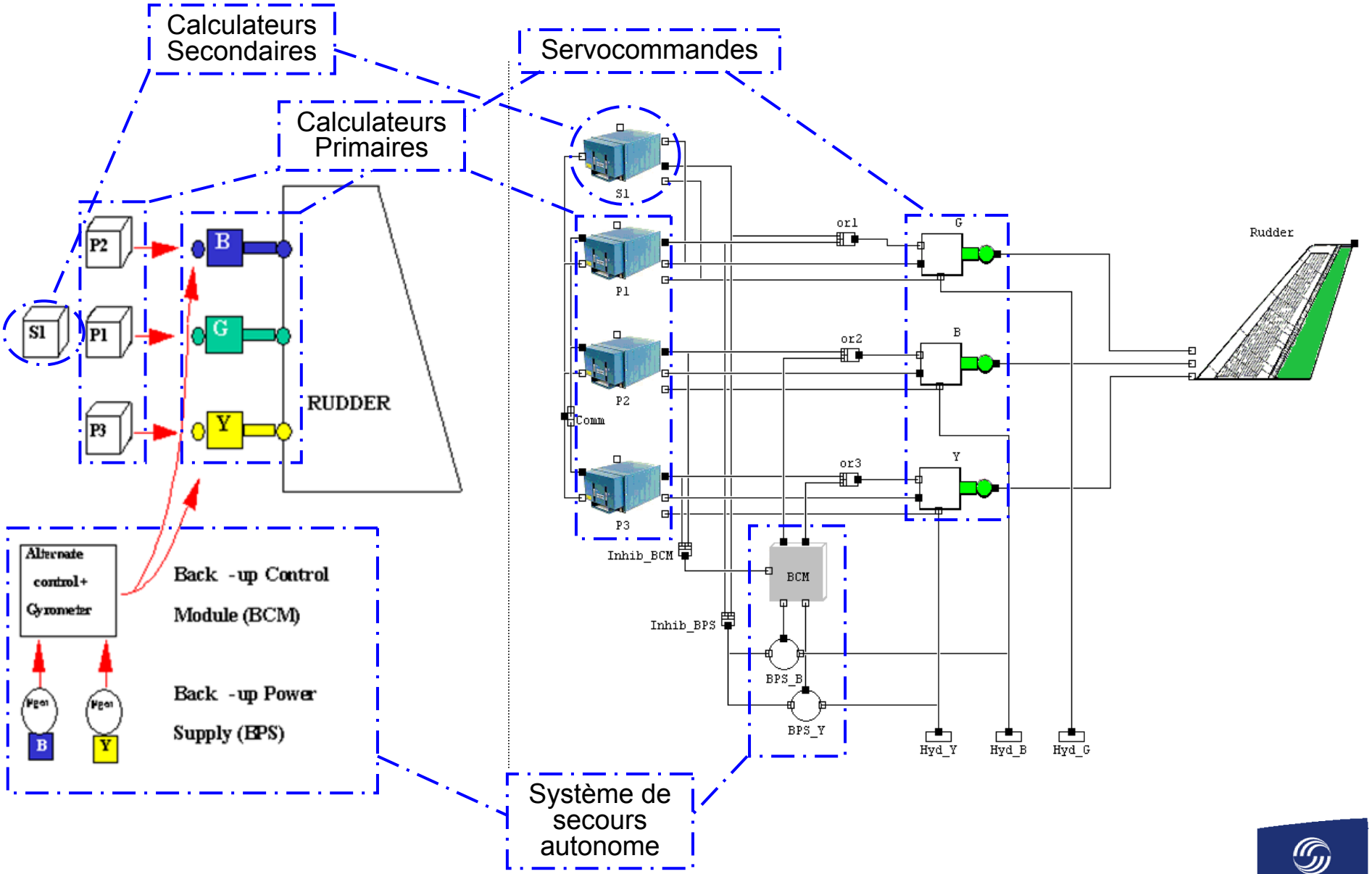
Outils d'analyse

- *Simulation interactive*
- *Génération d'arbre de faute*
- *Génération de séquences*:
  - calcul exhaustif des séquences (enchaînement d'événement) conduisant à un événement redouté spécifié
- *Model-checking*:
  - Analyse de modèle cherchant un contre-exemple à une propriété donnée (MecV, SMV)
- *Simulation stochastique*

Sommaire

1. Processus SdF actuel
2. Approche de modélisation
3. Cas d'étude
   - Modèle Rudder « mono-système »
   - Modèle Rudder « multi-systèmes »
   - Du découpage fonctionnel à l'architecture système
4. Raffinement
5. Conclusion

Système de commande Rudder



Étude Rudder: présentation

- FC : Loss of control of the rudder (Hazardous)
- Modélisation incrémentale

1. Modèle initial :
   - Comportement binaire: correct ou perdu
   - Modèle statique: l'ordre des défaillances n'influence pas la configuration atteignable

     ex. "Perte de A" puis "Perte de B" = "Perte de B" puis "Perte de A"

2. Modèle enrichi :
   - Comportement erroné ajouté au modèle initial
   - Modèle dynamique: la chronologie des défaillances influence la configuration atteignable

     ex. "Perte de surveillance (MON)" puis "erreur (COM) " ≠ "erreur (COM)" puis " Perte de surveillance (MON)"

Modèle initial: objectifs & outils

- Le modèle initial permet de:
  - Valider les reconfiguration principales
  - Effectuer une analyse préliminaire sur un nombre réduit de modes de panne

- Le modèle enrichi permet de:
  - Définir le comportement du système en cas d'erreur
  - Définir des règles de surveillance utilisant des retours de capteurs

Architecture Command/Monitoring

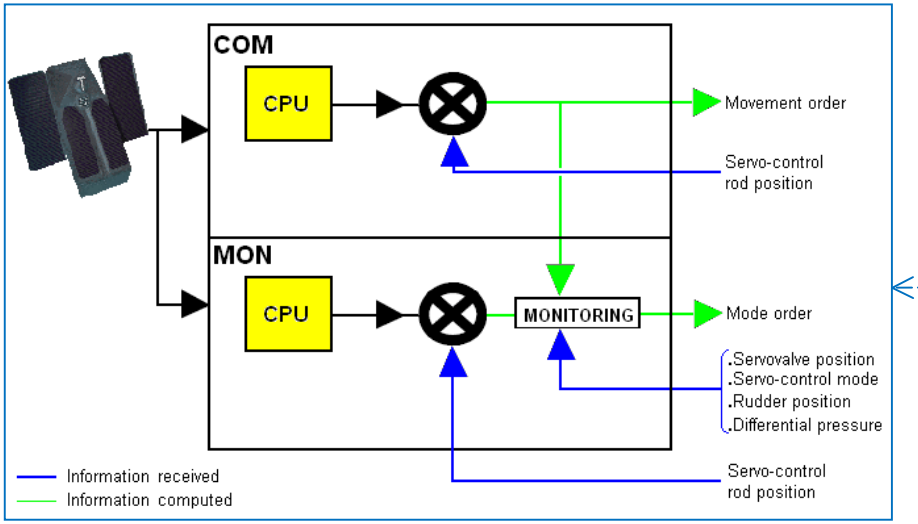
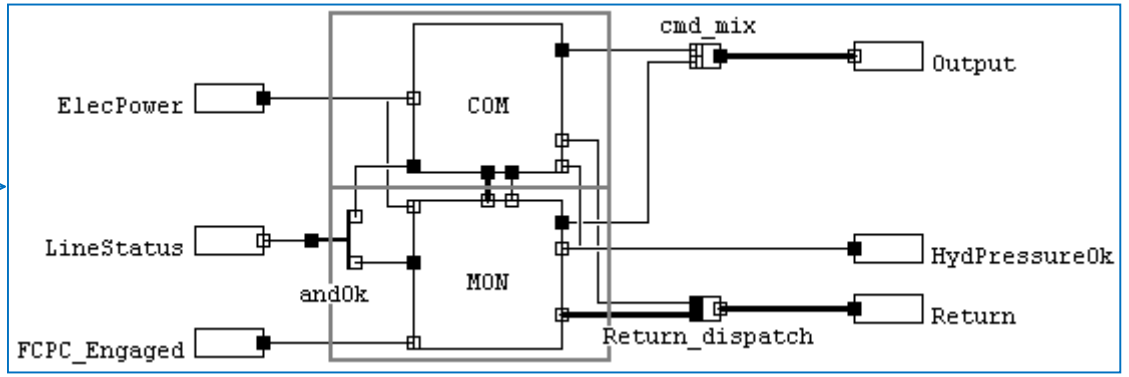


Schéma descriptif de l'architecture command/monitoring (COM/MON)

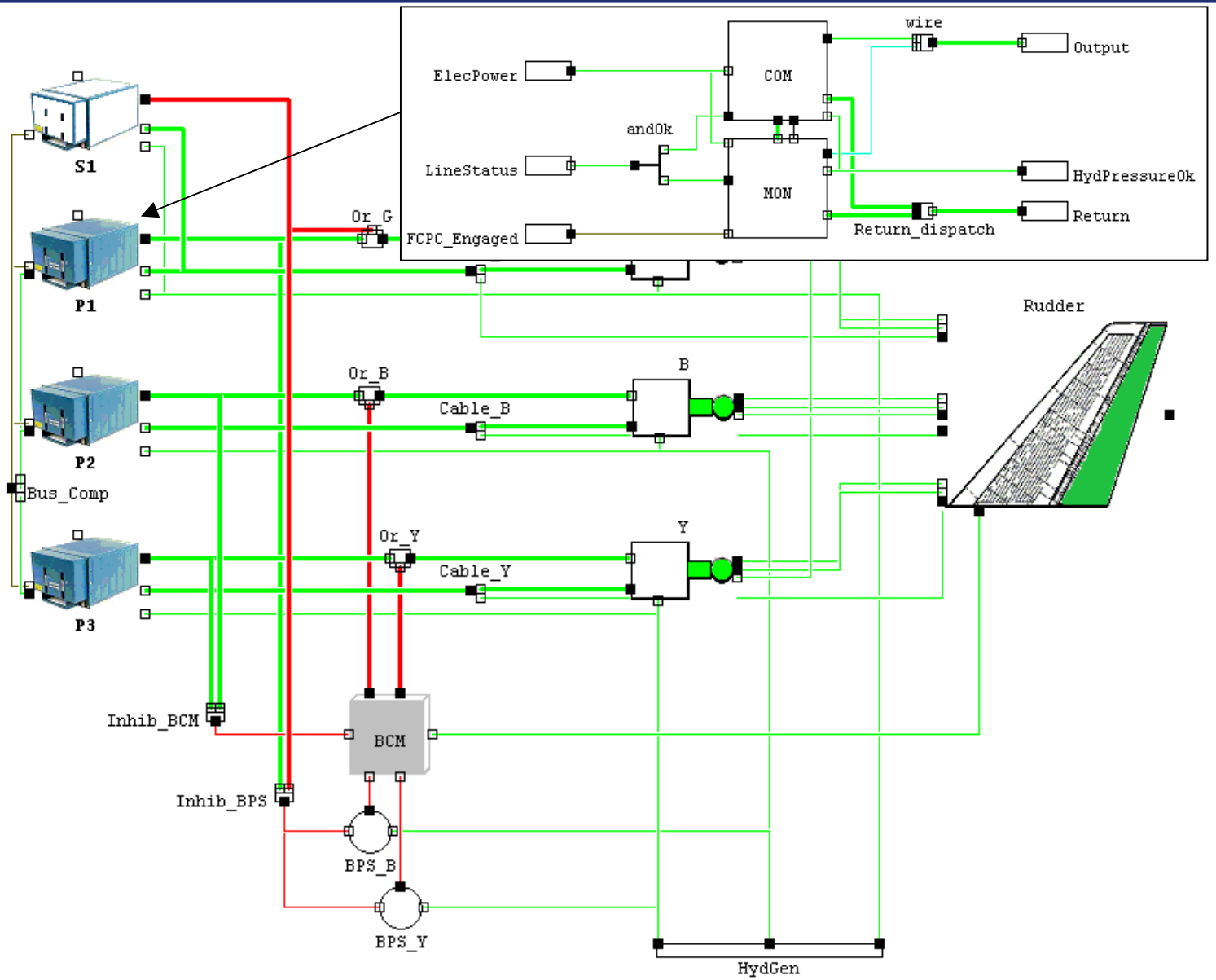
Composant AltaRica COM/MON



Exemple de détection du composant MON

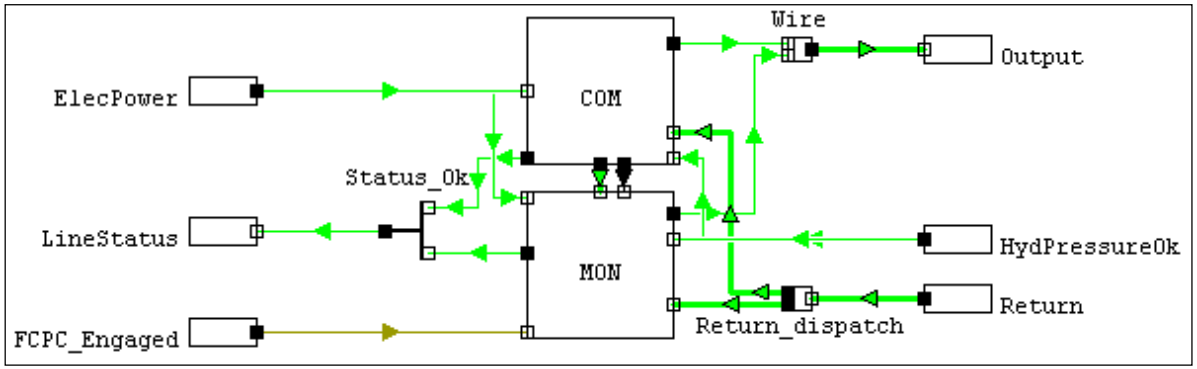
Event	Guard	New affectations
		Status
Update	Available and InputFromCom != MonOrder	lost

Architecture Command/Monitoring



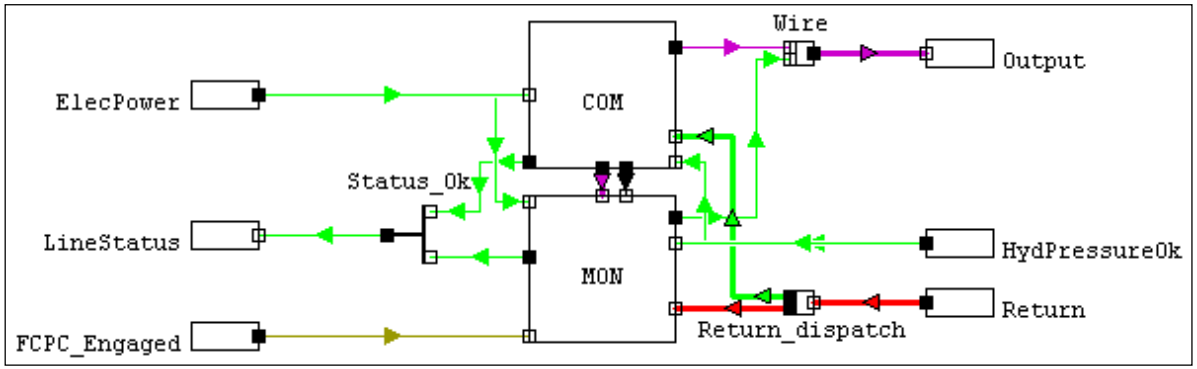
COM/MON: occurrence d'erreur & détection

Situation nominale



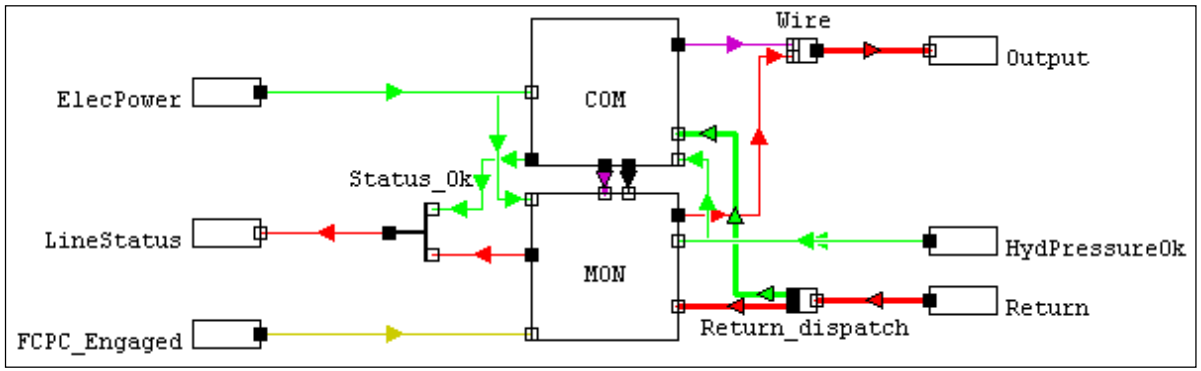
Erreur COM, **avant** détection par MON:

- Ordre erroné envoyé par le COM
- Au moins un retour incorrect



Erreur COM, **après** détection par MON:

- Ordre de passivation envoyé par le MON
- MON communique au système la perte de tout le calculateur



Études multi-systèmes: motivations

- Les cas d'études réalisés ont démontré l'intérêt des modélisation mono-système.
- Mais le processus d'analyse SdF s'intéresse à des problématiques multi-systèmes.

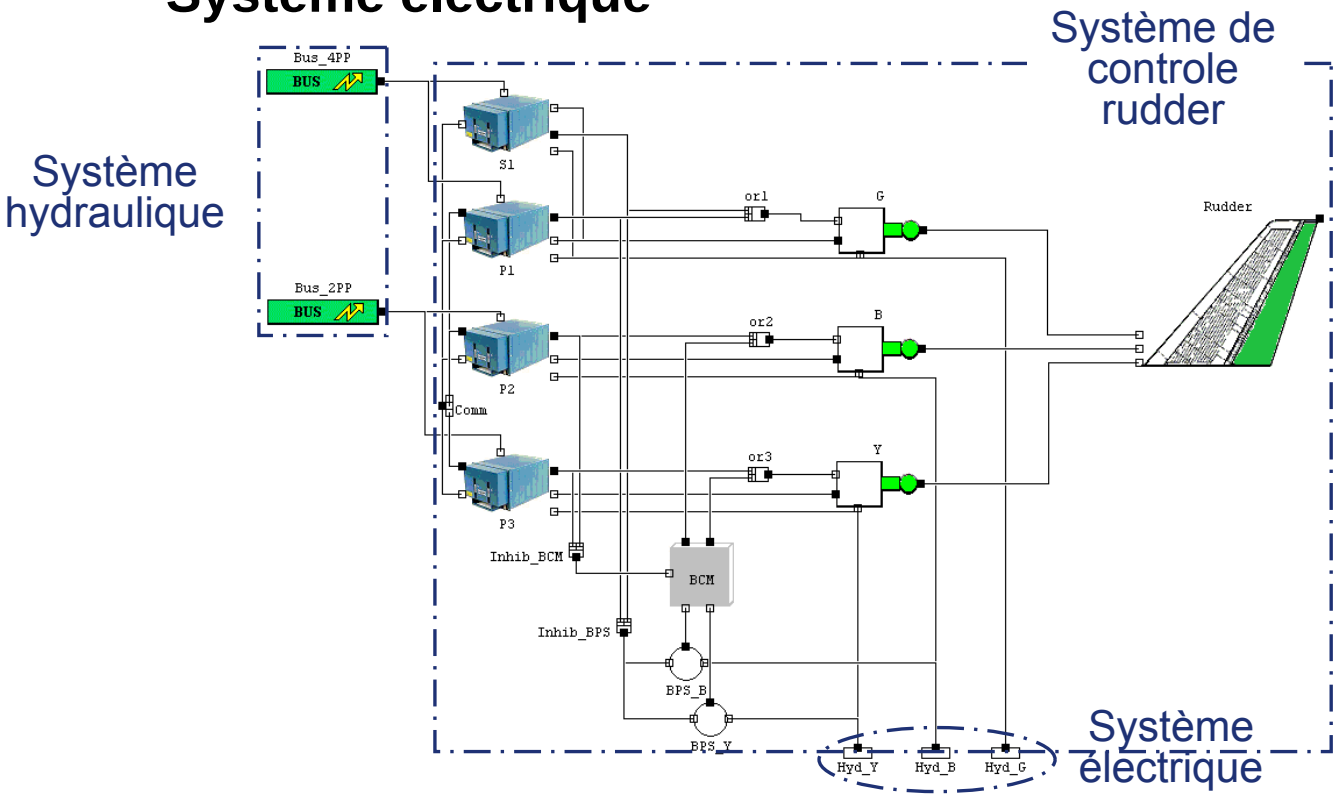
  → ***Nécessité d'étudier des modélisations multi-systèmes***

- Enjeux:
  - Étudier les dépendances inter-systèmes au plus tôt dans le développement (dès le niveau avion)
  - Lier les niveaux avion/système/équipement pour assurer la cohérence des allocations d'exigences

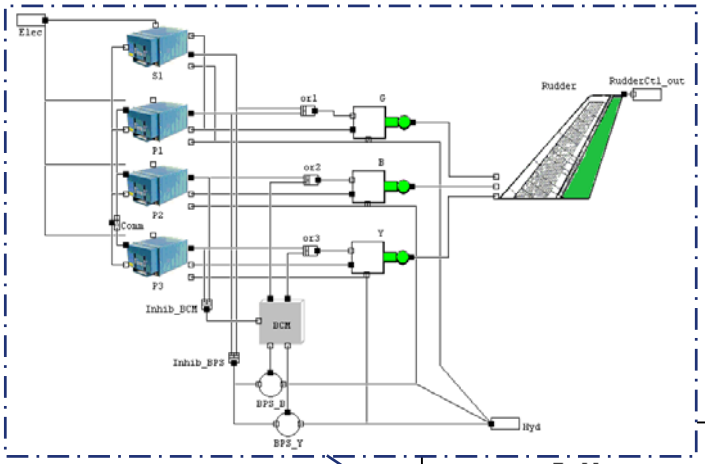
- Objectif:
  - supporter les analyses multi-systèmes avec des modèles AltaRica

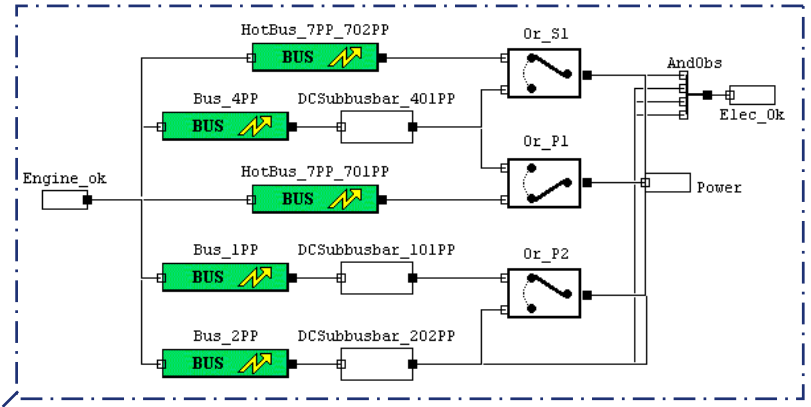
Modèle AltaRica: Rudder Mono-système

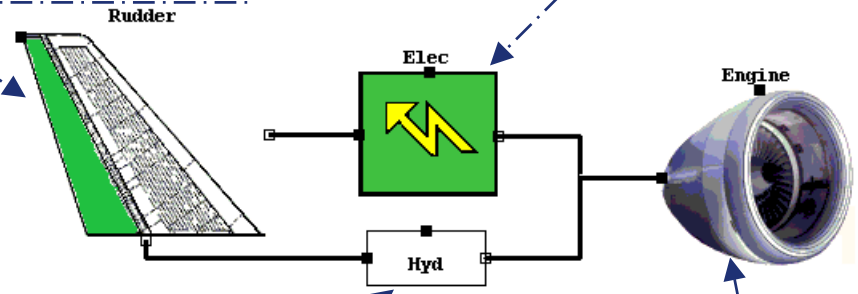
- **Modèle initial décomposé en plusieurs modèles:**
  - **Système de contrôle**
  - **Ressources:**
    - **Système hydraulique**
    - **Système électrique**

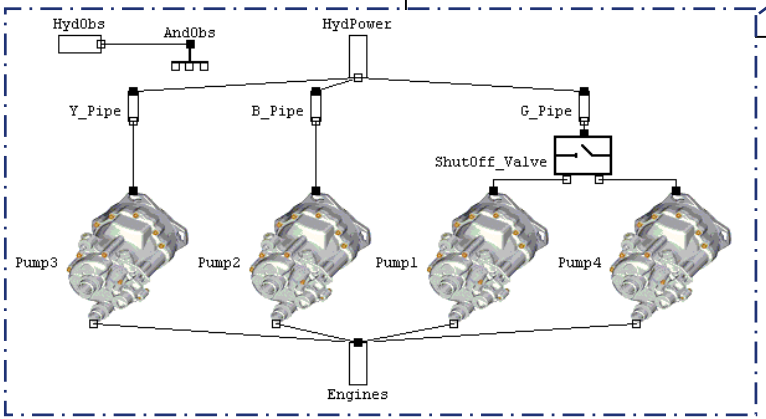


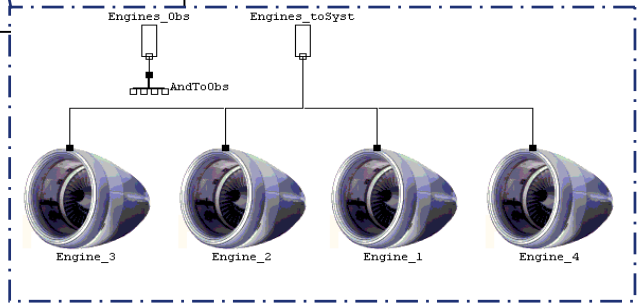
Modèle AltaRica: Rudder Multi-systèmes







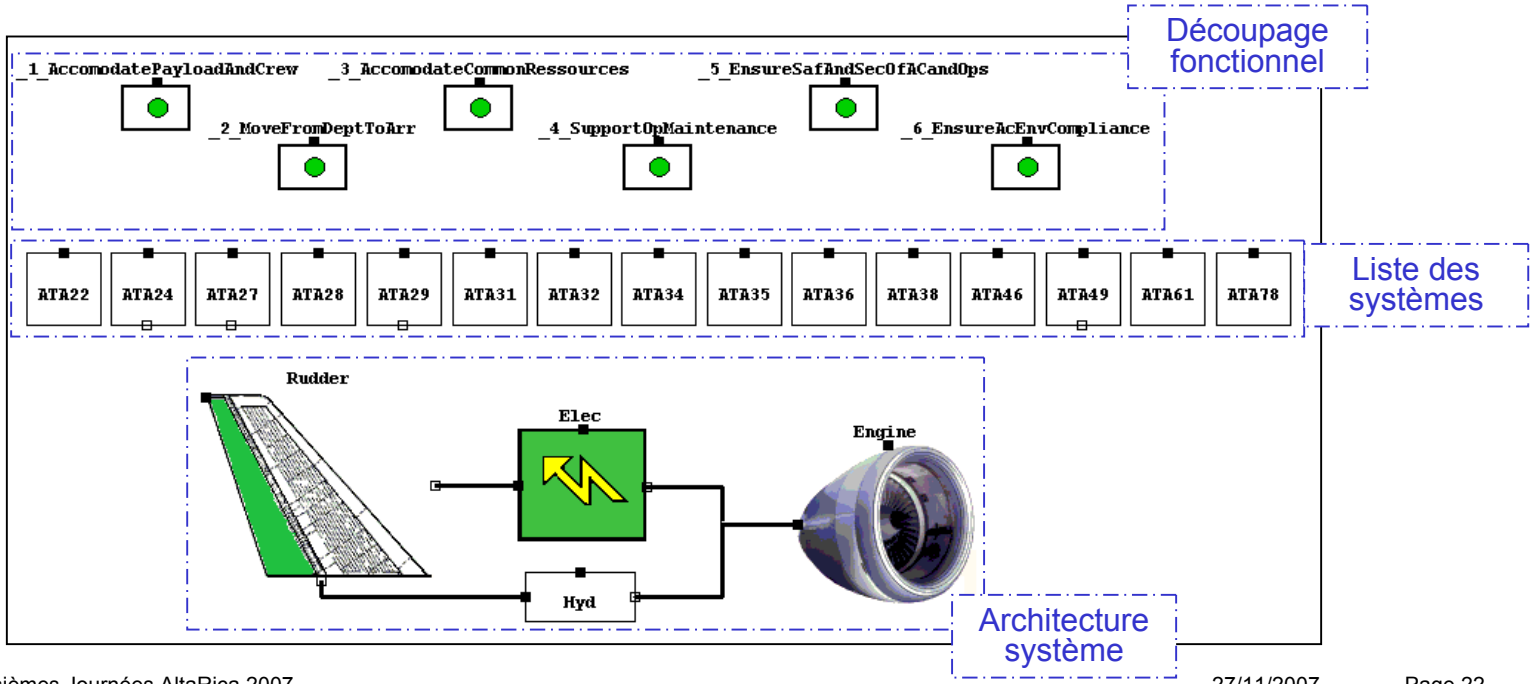




Liens fonctions -> systèmes

- Découpage fonctionnel:
  - Liste les fonctions nécessaires
  - Alloue fonctions aux systèmes

BASIC FUNCTIONS	MAIN FUNCTIONS	FUNCTIONS	DETAILED FUNCTIONS AND COMMENTS	INVOLVED SYSTEMS
2 MOVE FROM DEPARTURE TO ARRIVAL	02.02 CONTROL AIRCRAFT	02.02.02	02.02.02.01 Control direction on ground	27A / 32B / 70A
			02.02.02.02 Control roll	27A
			02.02.02.03 Control yaw	27A
			02.02.02.04 Control yaw trim	27A



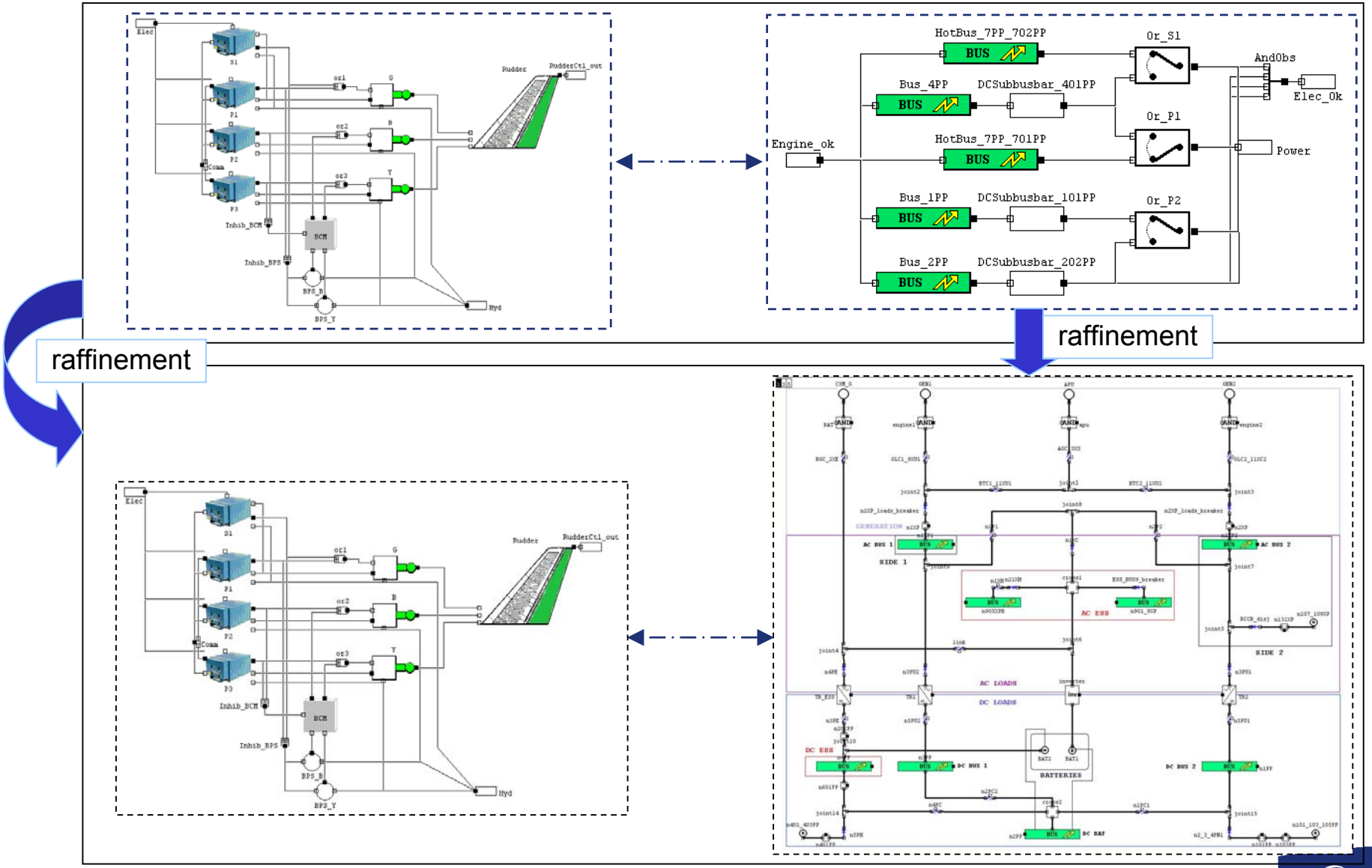
Sommaire

1. Processus SdF actuel
2. Approche de modélisation
3. Cas d'étude
4. Raffinement
5. Conclusion

Raffinement: introduction

- Approche de conception: enrichissement progressif de la spécification/description/modélisation
- Définir une relation de raffinement:
  - Définir des liens entre un modèle « abstrait » et un modèle « concret »
  - Établir une formule mathématique et les propriétés associées
- Démarche:
  - Étudier un système « abstrait » dont on déduit des propriétés
  - Extraire un sous-système, dit « abstrait » et le détailler
  - S'assurer que la relation de raffinement existe entre le sous-système détaillé (« concret ») et le sous-système initial
  - En déduire des propriétés sur le sous-système « concret »

Raffinement: application



Raffinement AltaRica

- Existant:
  - Une seule relation de raffinement a été définie pour le langage AltaRica: la *bisimulation*

  → 2 systèmes en bisimulation permettent de réaliser exactement les mêmes actions
  - Démonstration réalisée pour le langage AltaRica (LaBRI) avec priorité

- Les contraintes de la bisimulation sont trop fortes et cette relation ne peut s'appliquer à ces cas industriels.

- Questions:
  - Quelles relations?
  - Quel langage? (AltaRica LaBRI total/restreint, A.R. Data Flow…)

Raffinement AltaRica

- Objectif: définir des relations moins contraignantes et applicables aux architectures avion pour supporter le développement des modèles et les analyses.

- *Simulation simple*

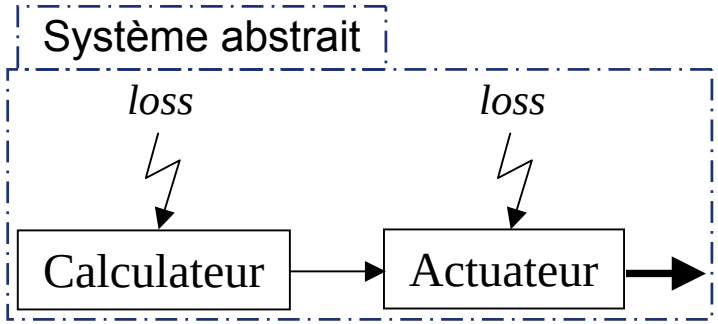
  → toute action du système « abstrait » peut être réalisée par le système « concret »

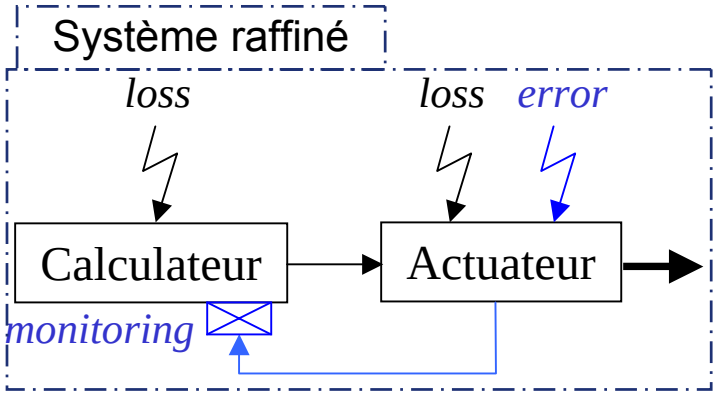
  - Relation définie et compositionalité démontrée pour un langage sans priorité sur les événements

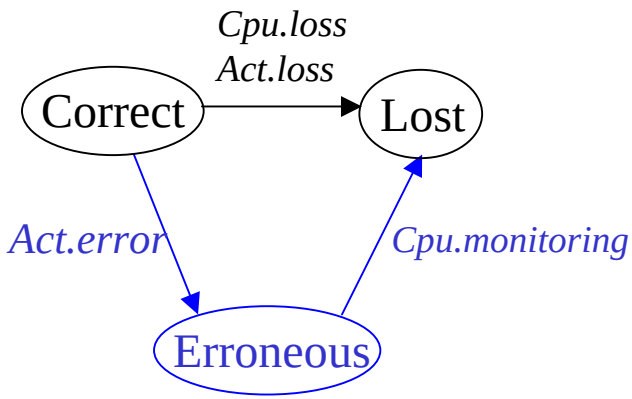
- *Équivalence observationnelle*

  → les actions du système « abstrait » sont équivalentes à des enchaînements d'actions du système « concret »

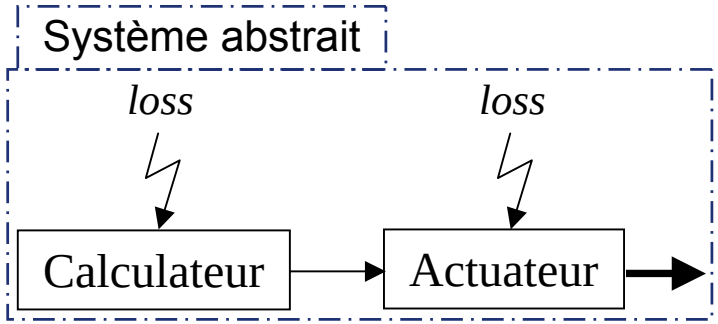
Raffinement AltaRica: illustration

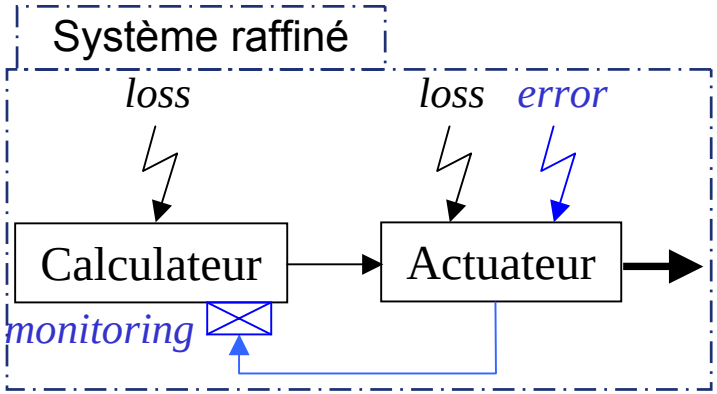


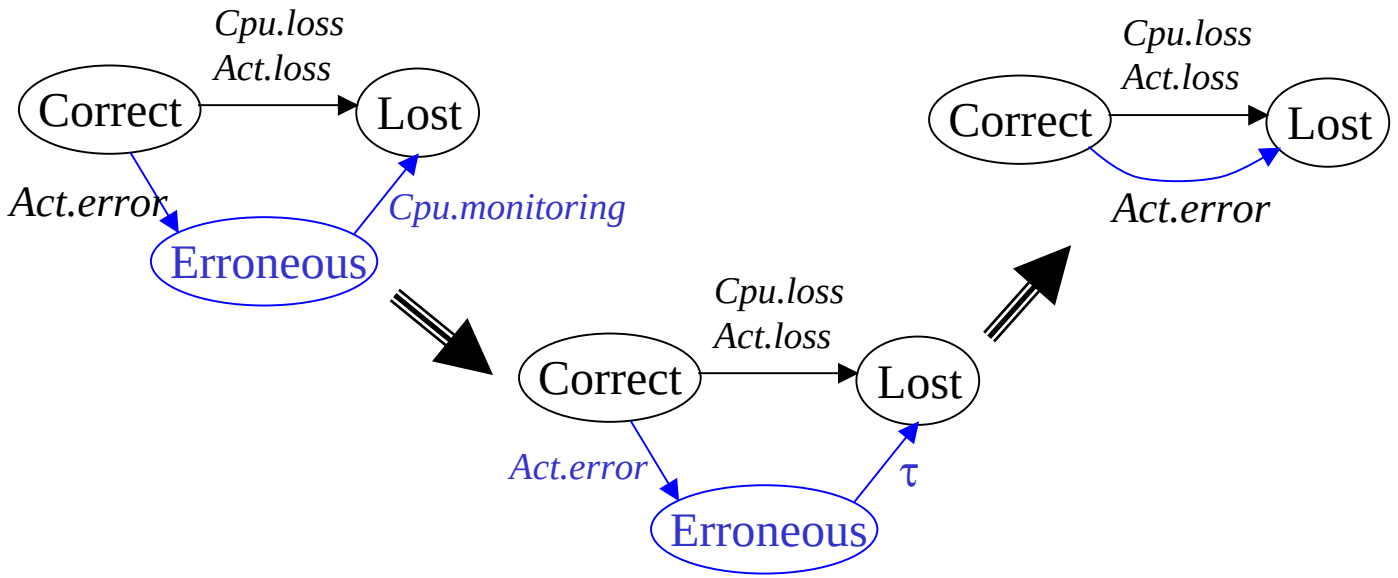




Équivalence observationnelle







Sommaire

1. Processus SdF actuel
2. Approche de modélisation
3. Cas d'étude
4. Raffinement
5. Conclusion

Conclusion

- Raffinement
  - Équivalence observationnelle: étude en cours
  - Simulation observationnelle: à creuser si équivalence observationnelle inappropriée
  - Étude des outils supports: MecV, génération de séquences
- Manipulations sur des exemples en AltaRica LaBRI et AltaRica DataFlow à réaliser
- Réflexion sur intégration de modèles multi-systèmes dans le processus à creuser

Possible future process

Design Documents

- System Description Document
- Architecture Diagram

Engineer Interpretation

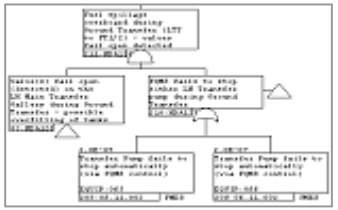
Informal Safety Engineer Expertise

System Behaviour Understanding

Engineer Judgement

Safety Analysis Results

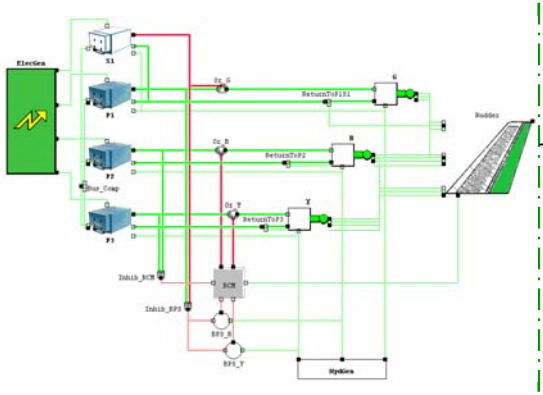
Dependance Diagram



Fault Tree

Formalization

Formal Model



Computer Performed Generation

Safety Analysis Results

Exhaustive Minimal Cut Sets

Feared Event: Rudder Control Lost

-------- order: 3 --- 10 cuts found ------

Loss of Yellow Hydraulic & Loss of Blue Hydraulic & Loss of Green Hydraulic

Loss of Green Servo control & Loss of Yellow Servo control & Loss of Prim 2

Loss of Yellow Servo control & Loss of Prim 2 & Loss of Green Hydraulic

Loss of Yellow Hydraulic
& Loss of Blue Servo control
& Loss of Green Servo control

Loss of Yellow Hydraulic
& Loss of Blue Servo control
& Loss of Green Hydraulic

Loss of Yellow Hydraulic
& Loss of Green Servo control
& Loss of Blue Hydraulic