

## Formalisation qualitative de scénarios critiques pour les systèmes dynamiques

Projet Féria

**Auteurs:** Bieber P., Castel C., Cholvy L., Demmou H.,  
Kehren C., Medjoudj M., Riviere N., Seguin C., Valette R.

## Cadre de travail

- **Domaine:** **conception** des systèmes embarqués critiques  
( **logiciels+matériels** )
- Point de vue discret et qualitatif
- Etude de la fiabilité et de la sécurité
- **Recherche** d'une démarche analogue aux arbres de  
défaillance quand celle-ci n'est pas appliquée

## Problématique

- **Objectif**
  - Étude de la fiabilité et de la sécurité des systèmes (complexes, hybrides mais avec forte composante discrète) comprenant des mécanismes de reconfigurations
  - Caractérisation et recherche de scénarios critiques menant à des situations redoutées.
- **Problème**
  - Méthodes classiques de sûreté de fonctionnement inefficaces
  - Explosion combinatoire des états, difficulté d'une recherche exhaustive
- **Solution?**
  - Recherche d'une démarche analogue aux arbres de défaillance permettant la prise en compte du comportement dynamique

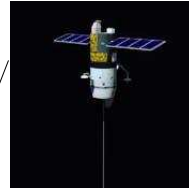
## Plan

- **Motivation-Buts**
- **Exemple illustratif de la démarche**
- **Définition d'un scénario critique**
- **Caractérisation par Logique Temporelle Linéaire (LTL)**
- **Caractérisation par logique linéaire de Girard**
- **Conclusion**

## Motivations et buts

- **Recherche d'une démarche analogue** aux arbres de défaillance
  - permettant la prise en compte du comportement dynamique
- **Arbres de défaillance**
  - Impliquant premier  $\leftrightarrow$  Coup minimal
  - L'ordre d'occurrence des événements pas pris en compte (Ex:  $F1;F2;R1 \neq F1;R1;F2$ )
- **Problème**
  - Comment prendre en compte l'ordre (dynamique)?
  - Minimalité
  - Complétude
  - Comment construire un scénario.

## Illustration: 2 Satellites + 1 Station Sol

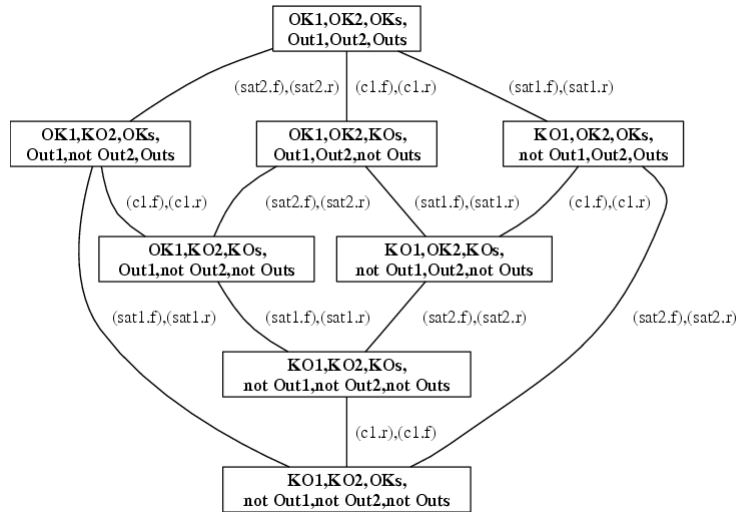


Défaillances  
Réparations



La constellation fonctionne si  
 • Les stations sol ok  
 • Au moins 1 satellite ok

→ Outs

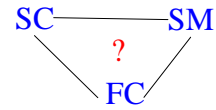


## Constat

Pour l'événement redouté: **enpermanence Outs=false**

- **Existence d'une infinité de séquences d'événements conduisant à cette condition de panne**
  - fs,fs;rs;fs,fs;rs;fs;rs;fs,...
- **Important: après fs, rs n'apparaît plus**
- **Autre scénario: f1;f2,ouf2;f1**
  - l'ordre n'est pas important => ordre partiel

## Scénariocritique(SC)



• **Définition** : pour FC (cas de panne) et SM (modèle du système)

- SC/FC et SM = un représentant de chemins, extraits de SM, allant d'un état à un autre FC est vraie
- Exemple: fs, rs, fs; f1, f2; ....

• **Besoins** (par analogie avec la notion de coupe et d'impliquant) :

- Représentation complète: tous les scénarios doivent être exprimés
- Scénarios pertinents: information nécessaire et suffisante
- Scénarios concis-compacts

## Approches

• **Modèles du système**

- Automates → LTL
- Réseau de Petri → Logique linéaire de Girard

• **Hypothèses**

- Système déterministe
- Une seule transition tirée à la fois
- Changement de valeur d'une variable d'entrée → événement

## ApprocheLTL

► Opérateurs **booléens classiques** : and, or, -->, ...

► propriétés des états instantanés

► Opérateurs **temporels**

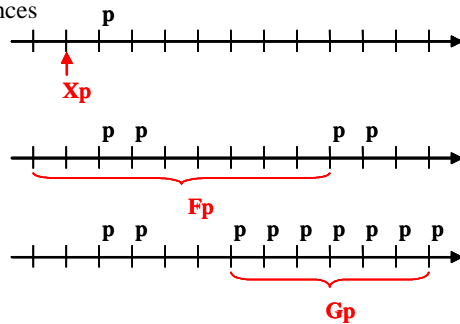
► propriétés des séquences

► Next p: Xp

► Finally p: Fp

► Globally p: Gp

► p Until q: pUq



## ApprocheLTL: notion de conséquence

- **Satisfaction** d'une formule temporelle **p** par une séquence si la propriété est vraie dans le premier état

$$- (S1, S2, S3, \dots) \models p \iff p \text{ vrai dans } S1$$

- **Conséquence logique**

$$- p \models q: \text{est conséquence logique de } p \text{ si toutes les séquences qui satisfont } p \text{ satisfont } q$$

## Propriétés des scénarios

**Un scénario ( $SC_i$ ), une condition de défaillance ( $FC_k$ )**

**= formule de LTL**

- **Causalité d'un scénario:**  
 $SC_i$  cause  $FC_k$  dans  $SM$  si
  - $SC_i, SM \models FC_k$
- **Condition nécessaire de minimalité:**  
 $SC_i$  minimal pour  $FC_k$  dans  $SM$  alors
  - pour tout  $SC_j$  si  $SC_j, SM \models FC_k$  et  $SC_i \models SC_j$  alors  $rs_{SC_j} = SC_i$
- **Complétude des scénarios**
  - $FC_k, SM \models SC_1 \vee SC_2 \vee \dots \vee SC_m$

## Illustration

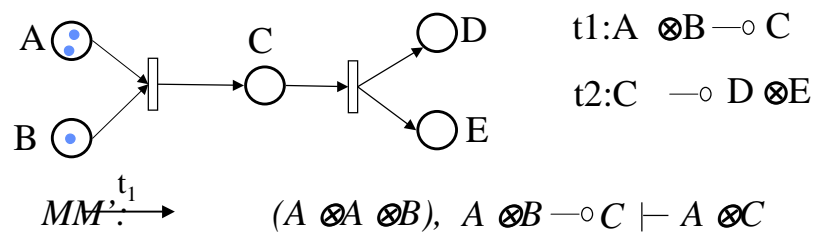
- **SM:** Modèle du système décrit par un **automate**
- **FC:** Perte permanente du service de la station sol
  - $F(G(\text{not Outs}))$
- **SC1:** une défaillance de la station sol n'est plus suivie d'une réparation
  - $F(fs \text{ and not Frs})$
- **SC2:** défaillance des deux satellites sans réparation
  - $F(f1 \text{ and not Fr1}) \text{ and } F(f2 \text{ and not Fr2})$

**Vérification par SMV**

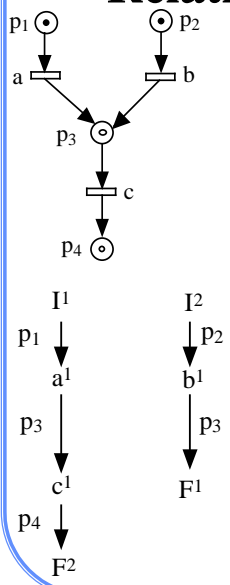
## Relation réseau de Petri-Logique linéaire

• **Représentation d'un réseau de Petri en logique linéaire**

- Un marquage est un monôme en «FOIS»  $\otimes$
- Basées sur des instances de franchissement de transitions
- Un franchissement d'une séquence est un séquent



## Relation réseau de Petri-Logique linéaire



$$\frac{\frac{\frac{p_3(b^1) \vdash p_3(F^1) \quad p_4(c^1) \vdash p_4(F^2)}{p_3(a^1) \vdash p_3(c^1) \quad p_3(b^1), p_4(c^1) \vdash p_3(F^1) \otimes p_4(F^2)}{p_2(I^2) \vdash p_2(b^1) \quad p_3(a^1), p_3(b^1), p_3 \multimap p_4 \vdash p_3(F^1) \otimes p_4(F^2)}}{p_1(I^1) \vdash p_1(a^1) \quad p_3(a^1), p_2, p_2 \multimap p_3, p_3 \multimap p_4 \vdash p_3(F^1) \otimes p_4(F^2)}}{p_1(I^1), p_2(I^2), p_1 \multimap p_3, p_2 \multimap p_3, p_3 \multimap p_4 \vdash p_3(F^1) \otimes p_4(F^2)}$$

$c^1$   
 $b^1$   
 $a^1$

$$p_1(I^1) \otimes p_2(I^2), p_1 \multimap p_3, p_2 \multimap p_3, p_3 \multimap p_4 \vdash p_3(F^1) \otimes p_4(F^2)$$

Preuve: a; b; c

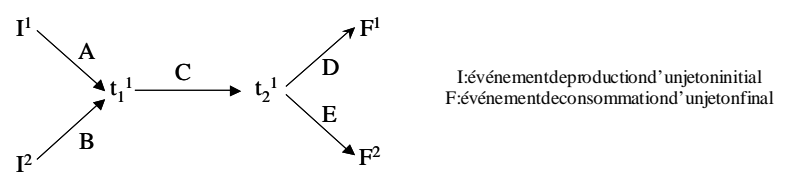
# Relation réseau de Petri-Logique linéaire

## § Construction d'un **arbre de preuve** du séquent

- Procédure simple (utilisation de deux règles)
- Taille de l'arbre proportionnelle au nombre de franchissements dans le séquent

## § Construction d'un **graphe de précedence**

- Relations de **causalité** entre les instances de franchissement de transitions



# Approche: RdP+LL

Premierscénario:

$$Ok_s, f_s, fail_2 \vdash F$$

$$(CS_1 \wedge SM) \vdash FC_1$$

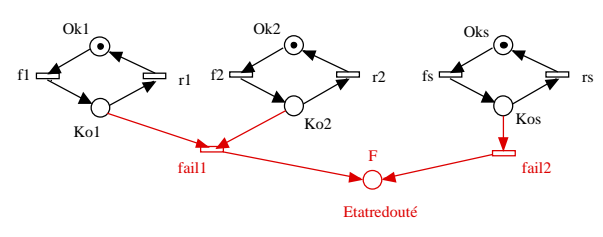
$$f_s, fail_2 \vdash (Ok_s \multimap F)$$

Deuxièmescénario:

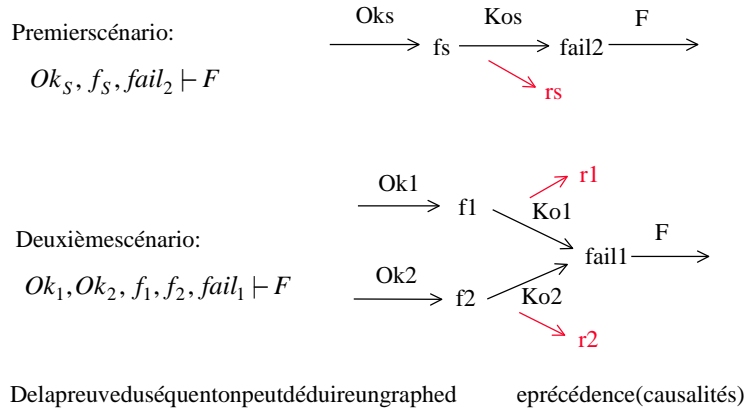
$$Ok_1, Ok_2, f_1, f_2, fail_1 \vdash F$$

$$(CS_2 \wedge SM) \vdash FC_2$$

$$f_1, f_2, fail_1 \vdash (Ok_1 \otimes Ok_2 \multimap F)$$



## Approche:RdP+LL



## Approche-RdP+LL

- **Conditionsuffisante**  $l_i \vdash (M_o \multimap M_f)$
- **Conditionnécessaire**  
 $\forall l_i, l_i \vdash (M_o \multimap M_f) \quad l_k, l_k \vdash (M_o \multimap M_f)$  estnécessaire si:  $\forall l_i, \exists l_c, l_i = l_k \otimes l_c$   
 celaestnormalementlaconséquence dufaitque  $\exists M_c, l_c \vdash (M_c \multimap M_c)$   
 telque  $l_k = l_{k1} \otimes l_{k2} \quad l_{k1} \vdash (M_o \multimap M_c)$  et  $l_{k2} \vdash (M_c \multimap M_f)$
- **Complétudedede:**  $L = \{l_1, \dots, l_i, \dots, l_n\}$   
 $\forall l_k, l_k \vdash (M_o \multimap M_f) \quad \exists l_i \in L, \exists l_c, l_k = l_i \otimes l_c, l_i \vdash (M_o \multimap M_f)$

## Conclusion

- **Unbesoin**
  - modéliser des ordres partiels d'événements et
  - raisonner sur la causalité des événements
- **Deux approches de représentation de scénarios ont été proposées**
  - Logique temporelle linéaire:
    - » Scénarios exprimables dans le langage de la logique temporelle
    - » Démarche visant l'extension des implicants premiers à la logique temporelle
  - Logique linéaire pour les réseaux de Petri
    - » Exploitation des preuves des équivalents pour construire des scénarios
- **Perspectives**
  - Notion de minimalité et forme canonique des scénarios
  - Automatiser la construction des scénarios critiques