Formalisation des interactions asynchrones

AFADL 2016

Florent Chevrou

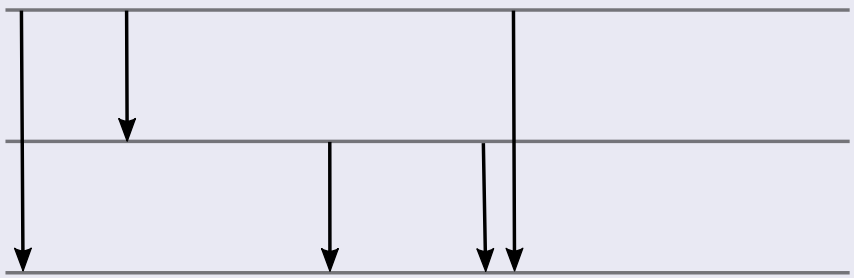
Encadrement : Aurélie Hurault et Philippe Quéinnec

IRIT/INP-ENSEEIHT – Équipe ACADIE – Université de Toulouse

7 juin 2016

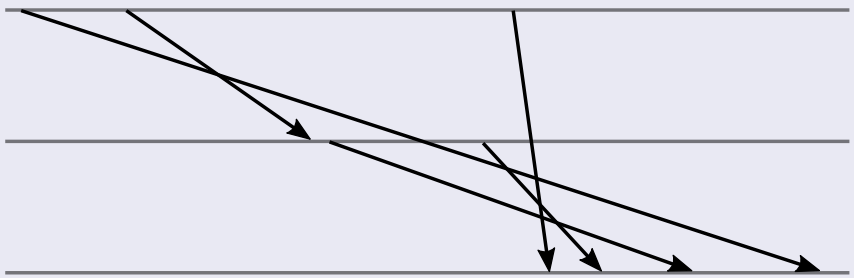
Communication point à point dans les systèmes distribués

Communication synchrone



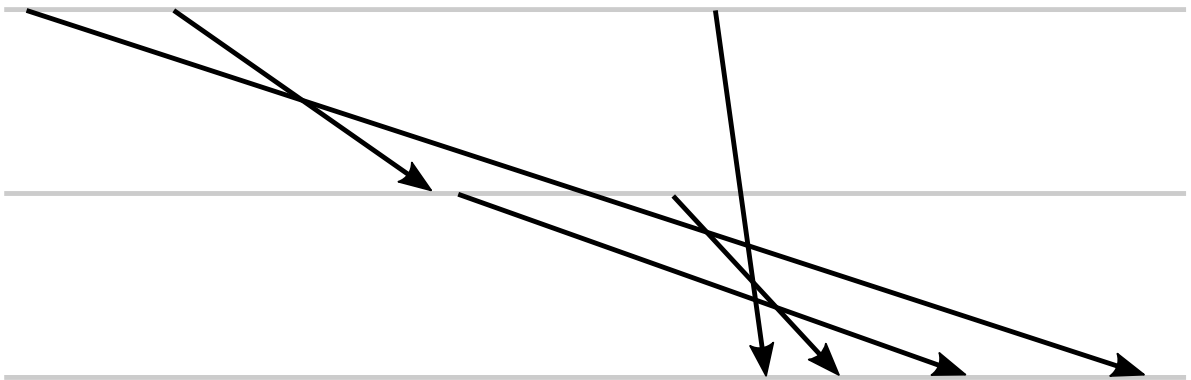
- *Rendez-vous* entre événements d'envoi et réception
- Un seul modèle

Communication asynchrone



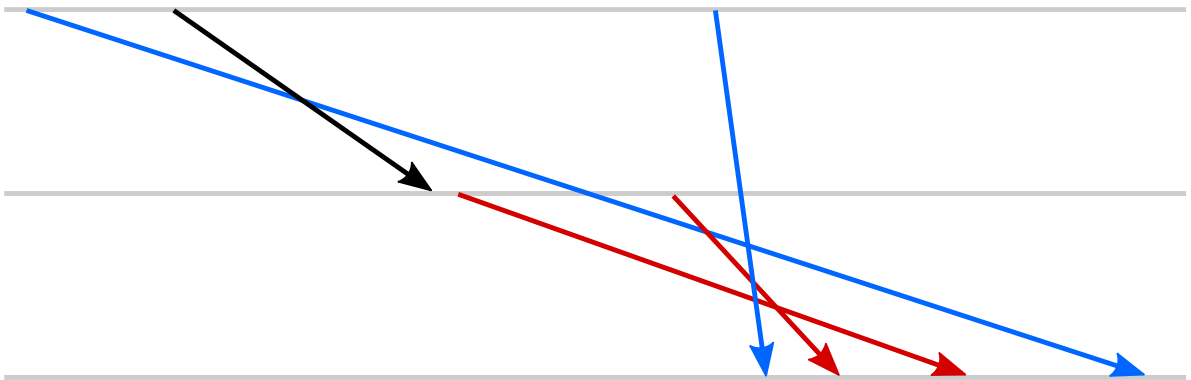
- Délai entre envoi et réception
- Nombreuses manières d'ordonner
- Compatibilité de pairs communiquants ?
- Hiérarchie

Illustration des modèles de communication



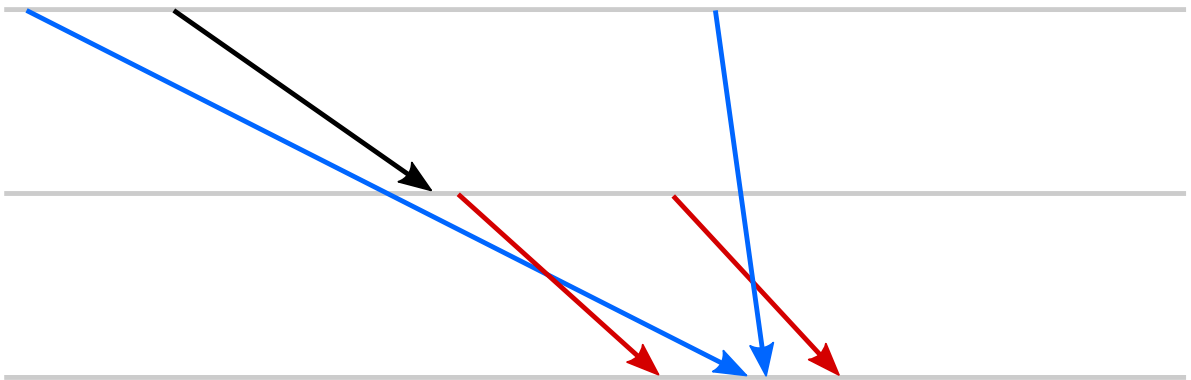
- **Asynchrone**
- FIFO 11
- Causal
- FIFO n1
- FIFO nn
- RSC

Illustration des modèles de communication



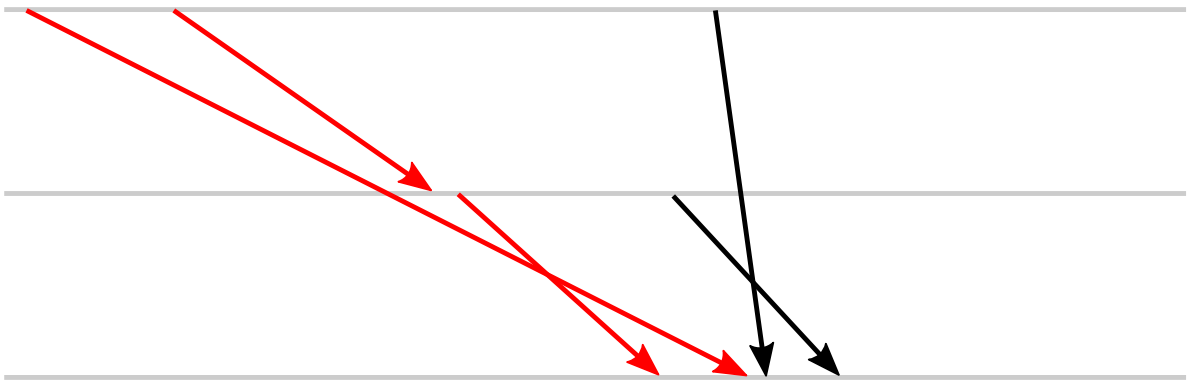
- **Asynchrone**
- FIFO 11
- Causal
- FIFO n1
- FIFO nn
- RSC

Illustration des modèles de communication



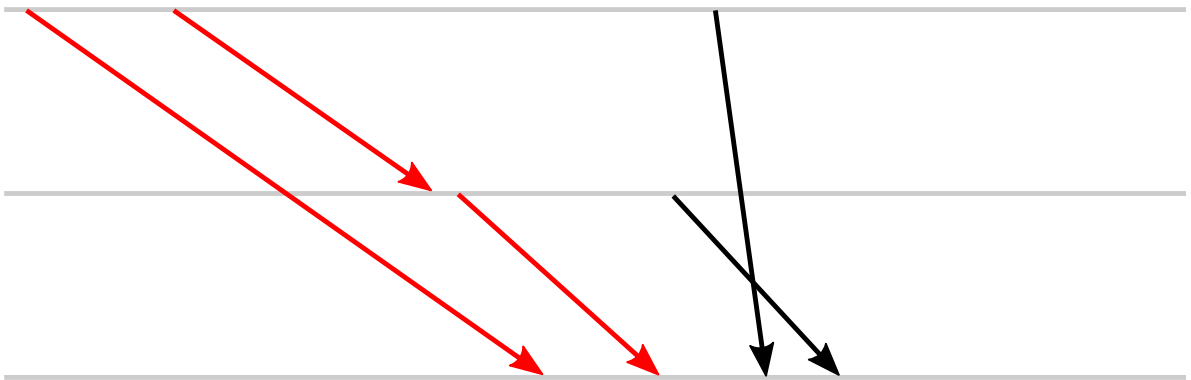
- Asynchrone
- **FIFO 11**
- Causal
- FIFO n1
- FIFO nn
- RSC

Illustration des modèles de communication



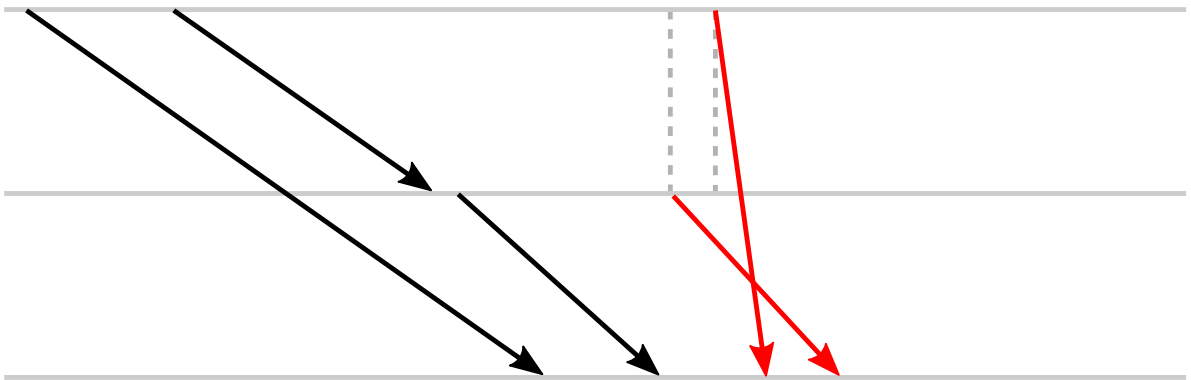
- Asynchrone
- **FIFO 11**
- Causal
- FIFO n1
- FIFO nn
- RSC

Illustration des modèles de communication



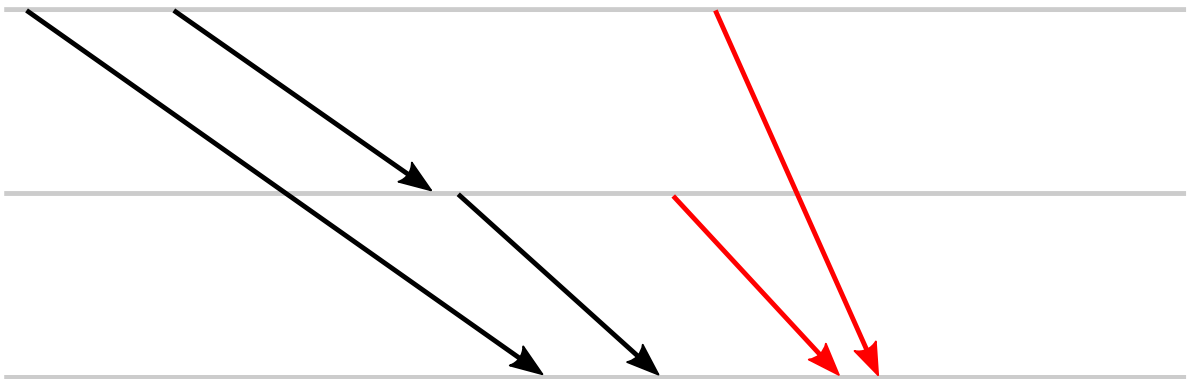
- Asynchrone
- FIFO 11
- **Causal**
- FIFO n1
- FIFO nn
- RSC

Illustration des modèles de communication



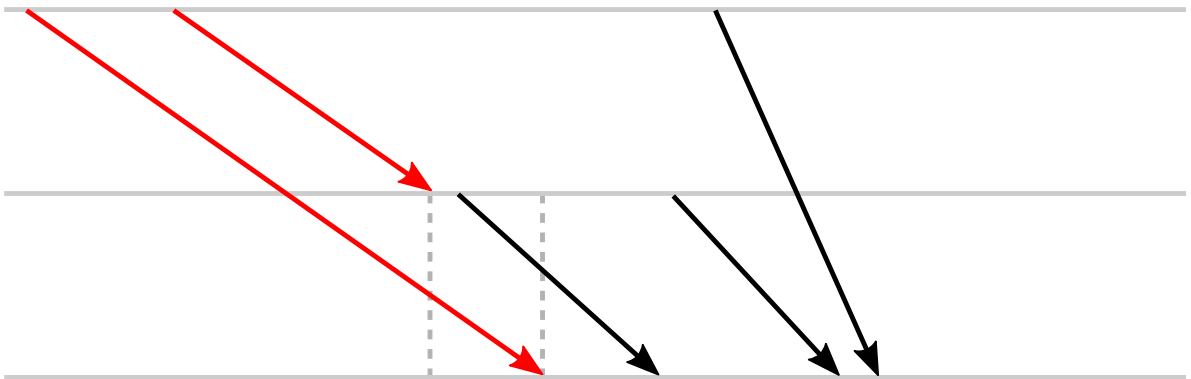
- Asynchrone
- FIFO 11
- **Causal**
- FIFO n1
- FIFO nn
- RSC

Illustration des modèles de communication



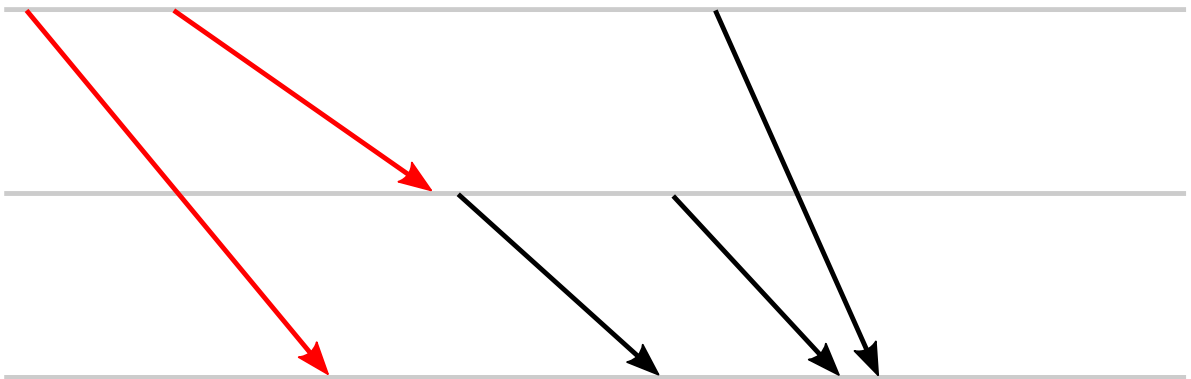
- Asynchrone
- FIFO 11
- Causal
- **FIFO n1**
- FIFO nn
- RSC

Illustration des modèles de communication



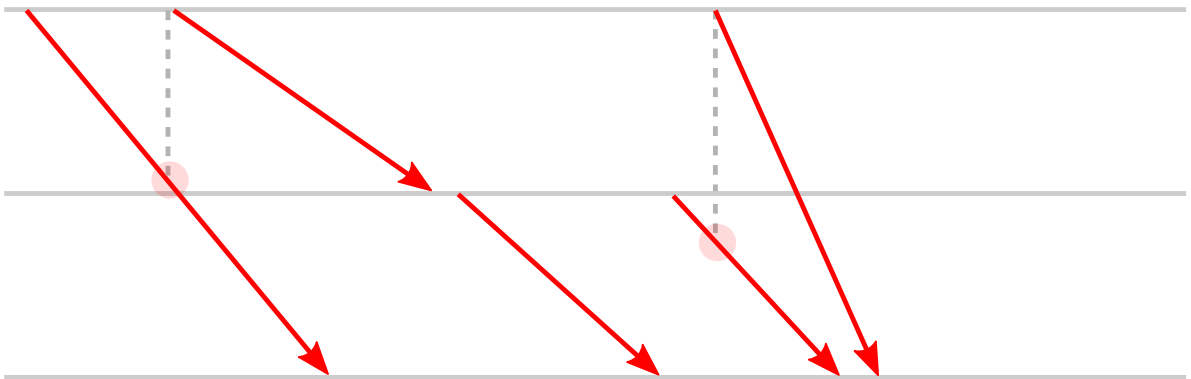
- Asynchrone
- FIFO 11
- Causal
- **FIFO n1**
- FIFO nn
- RSC

Illustration des modèles de communication



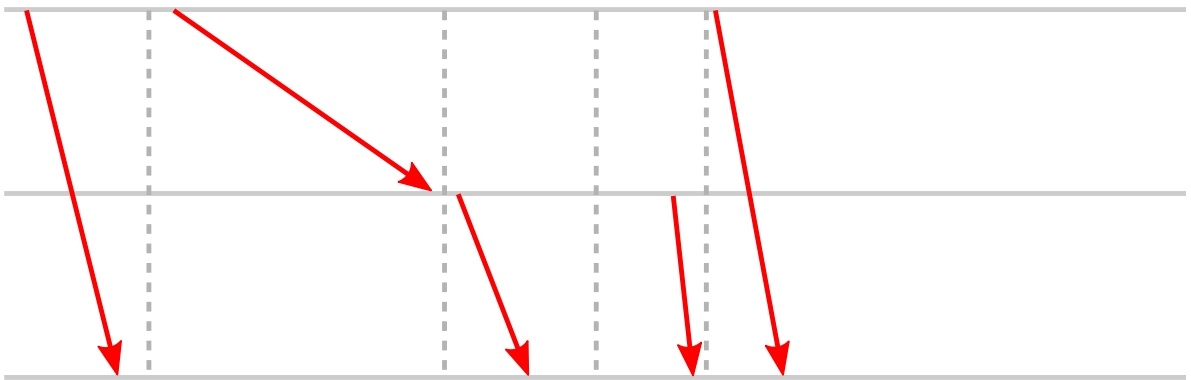
- Asynchrone
- FIFO 11
- Causal
- FIFO n1
- **FIFO nn**
- RSC

Illustration des modèles de communication



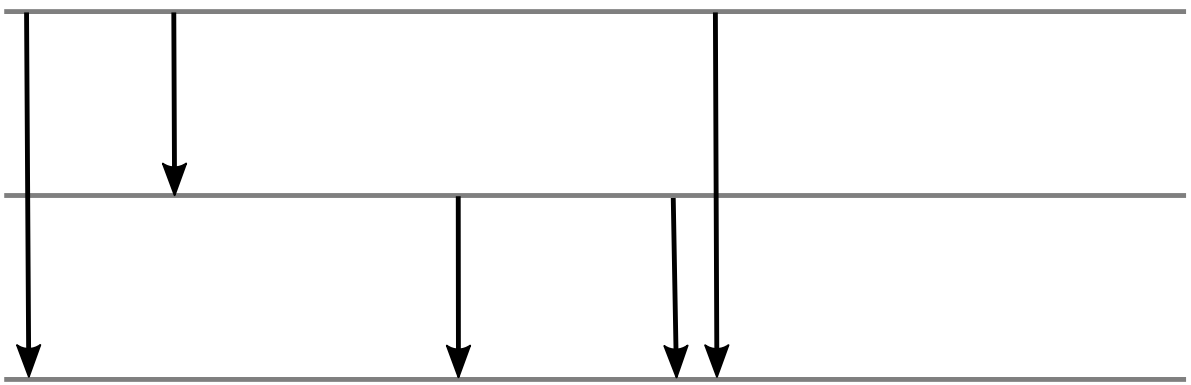
- Asynchrone
- FIFO 11
- Causal
- FIFO n1
- **FIFO nn**
- RSC

Illustration des modèles de communication



- Asynchrone
- FIFO 11
- Causal
- FIFO n1
- FIFO nn
- **RSC**

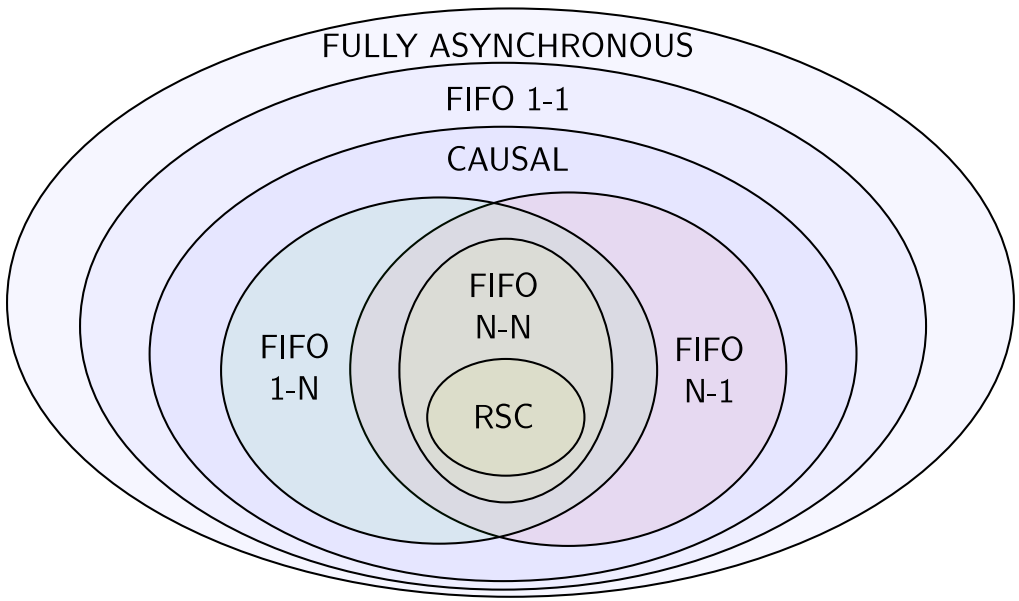
Illustration des modèles de communication



- Asynchrone
- FIFO 11
- Causal
- FIFO n1
- FIFO nn
- RSC
- **Synchrone**

Hiérarchie

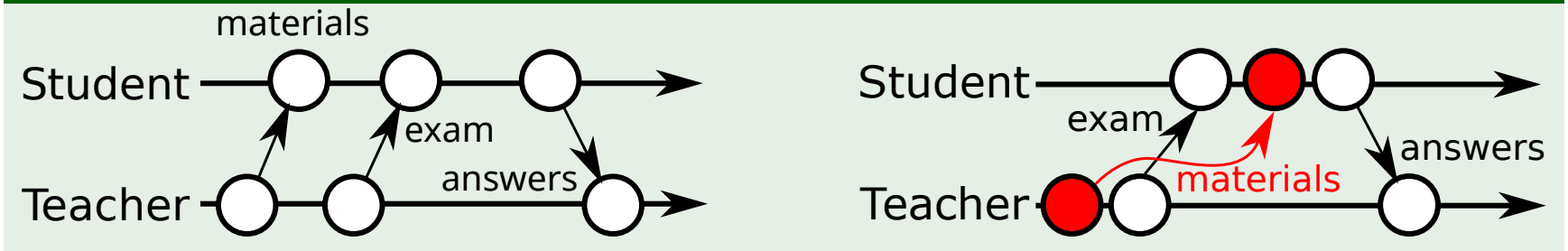
- Inclusions des exécutions distribuées possibles dans les modèles
- $\text{M1} \subseteq \text{M2} \triangleq \forall \sigma : \text{M1} \models \sigma \Rightarrow \text{M2} \models \sigma$



- Preuves qui découlent de l'inclusion des ordres qui définissent les modèles de communication
- Mécanisation des preuves : raffinements

Conséquences sur la compatibilité de pairs

Exemple de violation de l'ordre FIFO

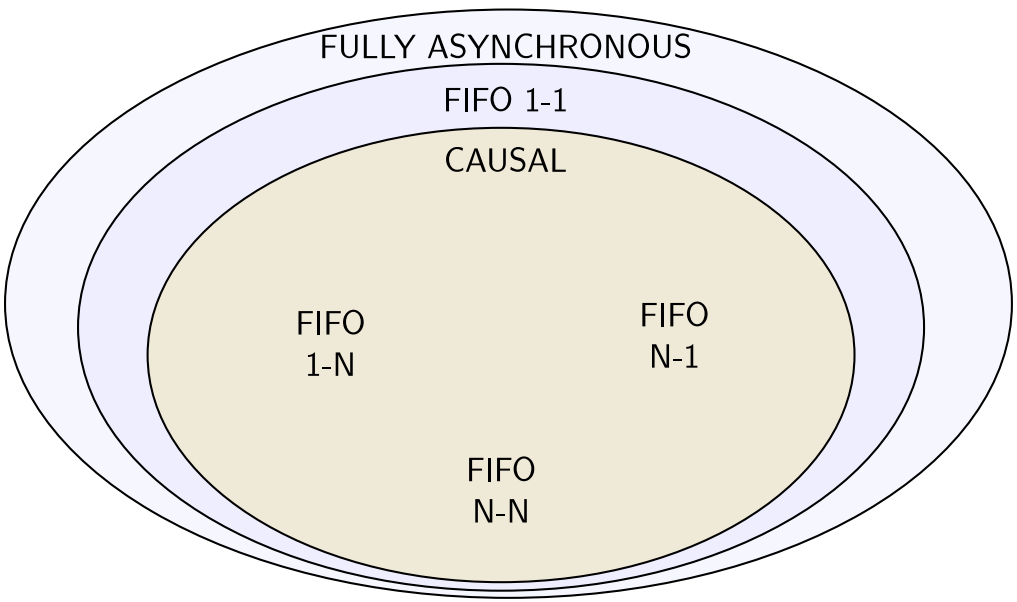


Différentes propriétés de compatibilité

- Pas de réception inattendue
- Terminaison
- Absence d'interblocage
- Pas de messages indéfiniment en transit
- ...

Hiérarchie point de vue système et compatibilité

- $M1 \subseteq M2 \triangleq \forall S$:
  S incompatible sous M1 $\Rightarrow$ S incompatible sous M2
- Conjecture pour la terminaison et l'absence de réception inattendue :



- Intérêt : substituabilité par les modèles formellement simples

Caractéristiques

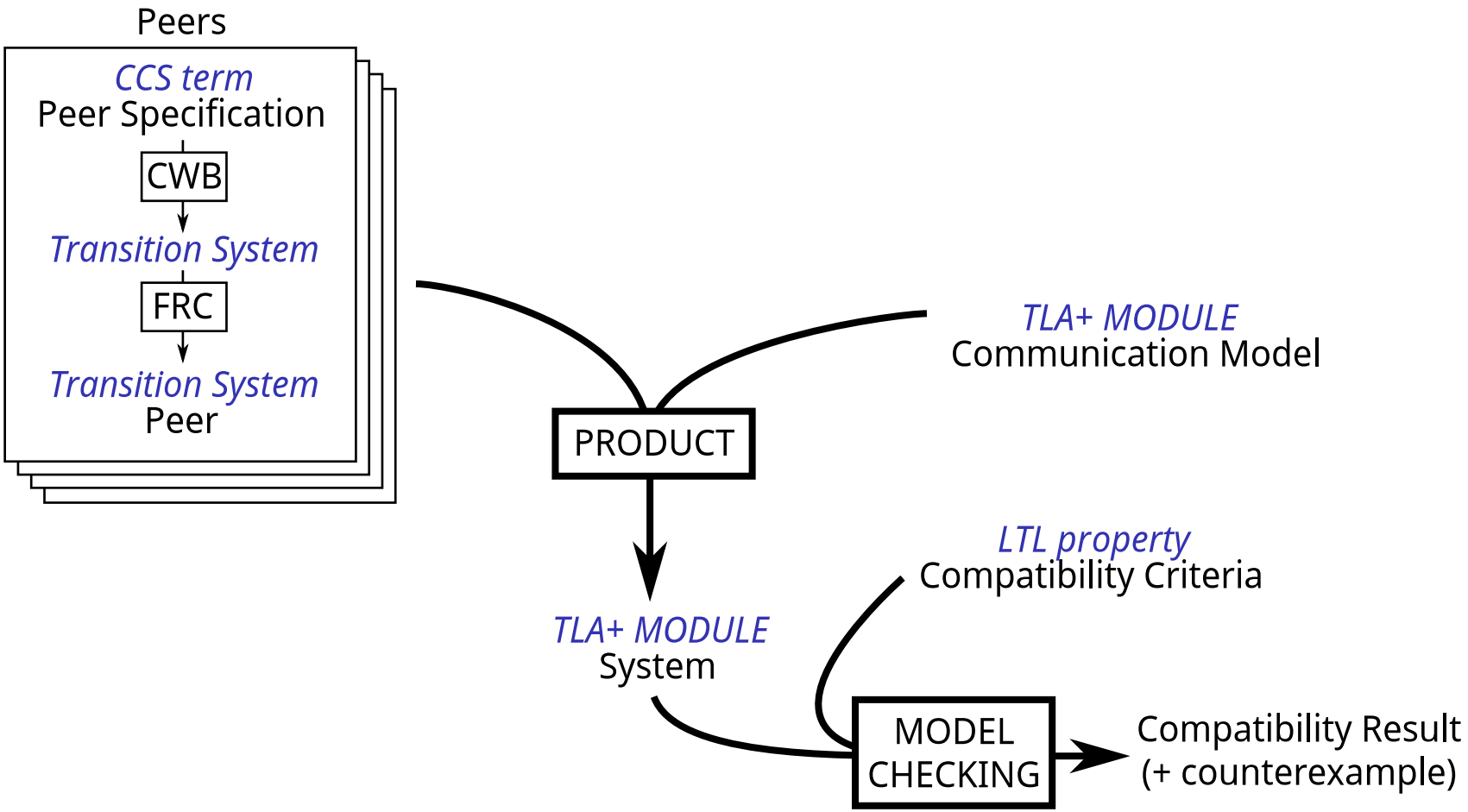
Modélisation avec TLA+

- Spécification des modèles de communication unifiée, basée sur les histoires de messages, et distribuée
- Abstraction des destinataires par canaux multiémetteurs/multidestinataires
- Découpage en groupes de canaux associés à différents modèles (propriétés d'ordre)

Méthode

- Pairs spécifiés par systèmes de transition
- Modularité
- Chaîne automatisée
- Critère de compatibilité : propriété LTL
- **Model checking** (TLC)

Chaîne d'actions



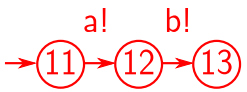
Exemple de module généré

MODULE *composition*

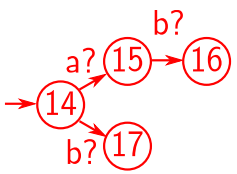
EXTENDS *Naturals*, *peermanagement*
CONSTANTS *N*
VARIABLES *net*
$Vars \triangleq \langle peers, net \rangle$
$Com \triangleq$ INSTANCE *causal* WITH *CHANNEL* $\leftarrow$ {"a", "b"}

$Init \triangleq Com!Init \wedge peers = \langle 11, 14 \rangle$

$t1(peer) \triangleq trans(peer, 11, 12) \wedge Com!send(peer, \text{"a"})$
$t2(peer) \triangleq trans(peer, 12, 13) \wedge Com!send(peer, \text{"b"})$

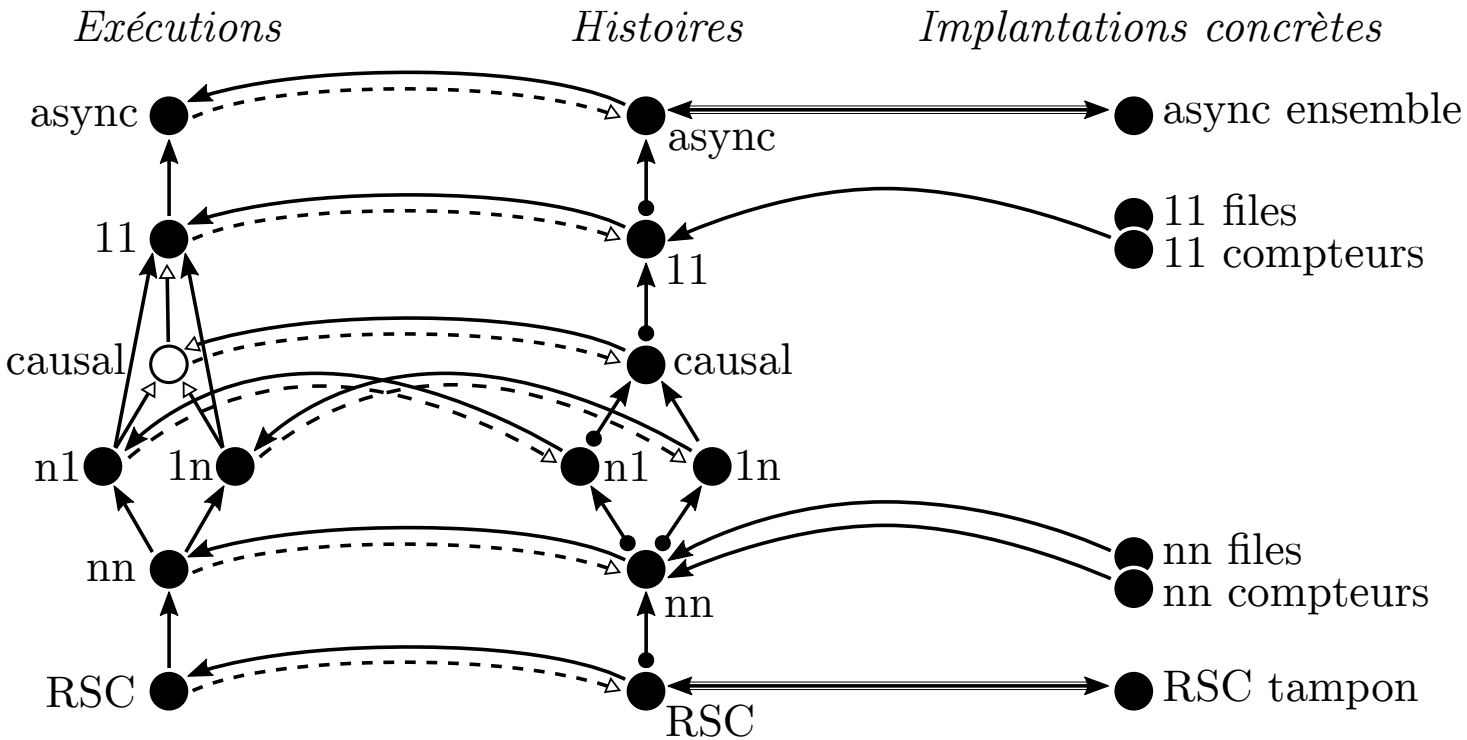


$t3(peer) \triangleq trans(peer, 14, 15) \wedge Com!receive(peer, \text{"a"}, \{\text{"b"}, \text{"a"}\})$
$t4(peer) \triangleq trans(peer, 15, 16) \wedge Com!receive(peer, \text{"b"}, \{\text{"b"}\})$
$t5(peer) \triangleq trans(peer, 14, 17) \wedge Com!receive(peer, \text{"b"}, \{\text{"b"}, \text{"a"}\})$



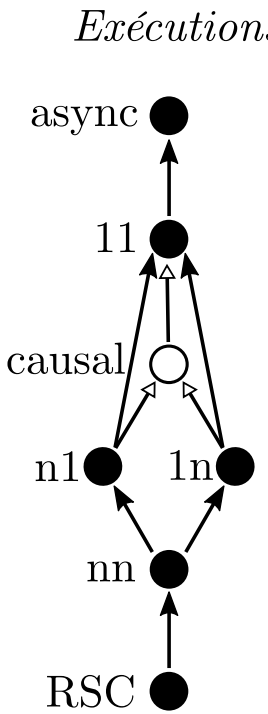
$Fairness \triangleq \forall i \in 1 \,..\, N : ($
$\mathrm{WF}_{Vars}(t1(i)) \wedge \mathrm{WF}_{Vars}(t2(i)) \wedge \mathrm{WF}_{Vars}(t3(i)) \wedge \mathrm{WF}_{Vars}(t4(i)) \wedge \mathrm{WF}_{Vars}(t5(i)))$
$\wedge \mathrm{WF}_{Vars}(Com!internal \wedge$ UNCHANGED $peers)$
$Next \triangleq \exists i \in 1 \,..\, N : (t1(i) \vee t2(i) \vee t3(i) \vee t4(i) \vee t5(i)) \vee (Com!internal \wedge$ UNCHANGED $peers)$
$Spec \triangleq Init \wedge \Box[Next]_{Vars} \wedge Fairness$

Aperçu des relations



spécification manuelle ○ raffine (preuve manuelle) ⟶ sous hypothèses - - - -
spécification (Event-B ou TLA+) ● raffine (preuve Event-B) ⟶ identité ⟺
raffine (Event-B et TLA+) ●⟶

Aperçu des relations

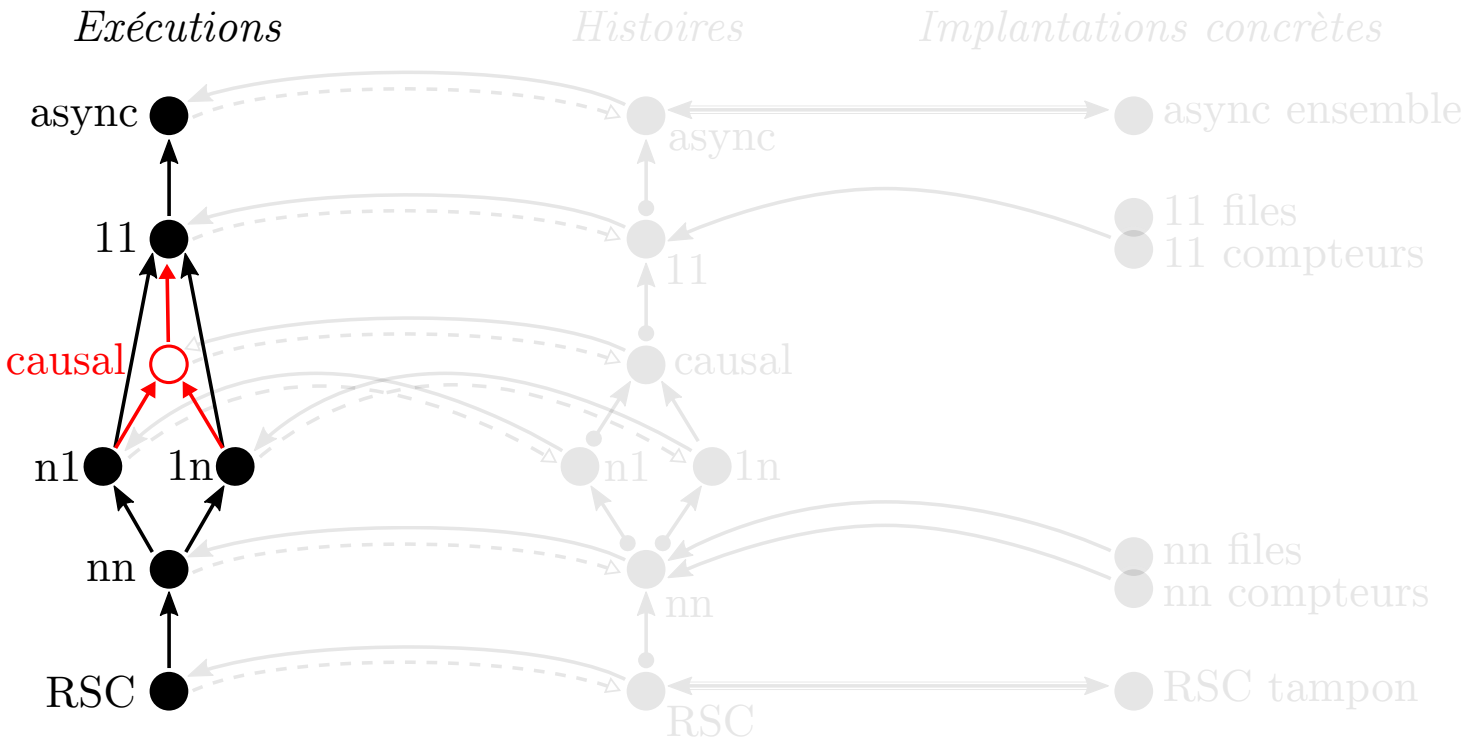


Exécution : séquence d'événements (envoi, réception)

Modèle de communication : ordre sur les événements

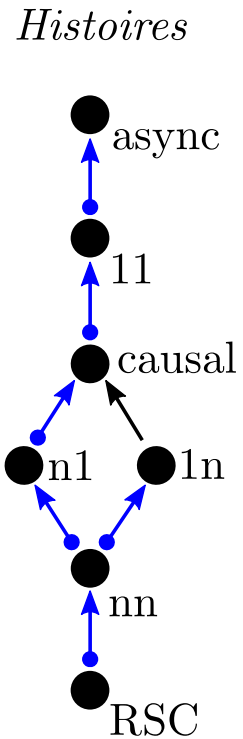
spécification manuelle ○
spécification (Event-B ou TLA+) ●
raffine (preuve manuelle) ⟶▷
raffine (preuve Event-B) ⟶
raffine (Event-B et TLA+) ●⟶
sous hypothèses - - - -
identité ⟺

Aperçu des relations



spécification manuelle ○ raffine (preuve manuelle) → sous hypothèses - - - -
spécification (Event-B ou TLA+) ● raffine (preuve Event-B) → identité ⟺
raffine (Event-B et TLA+) ●→

Aperçu des relations

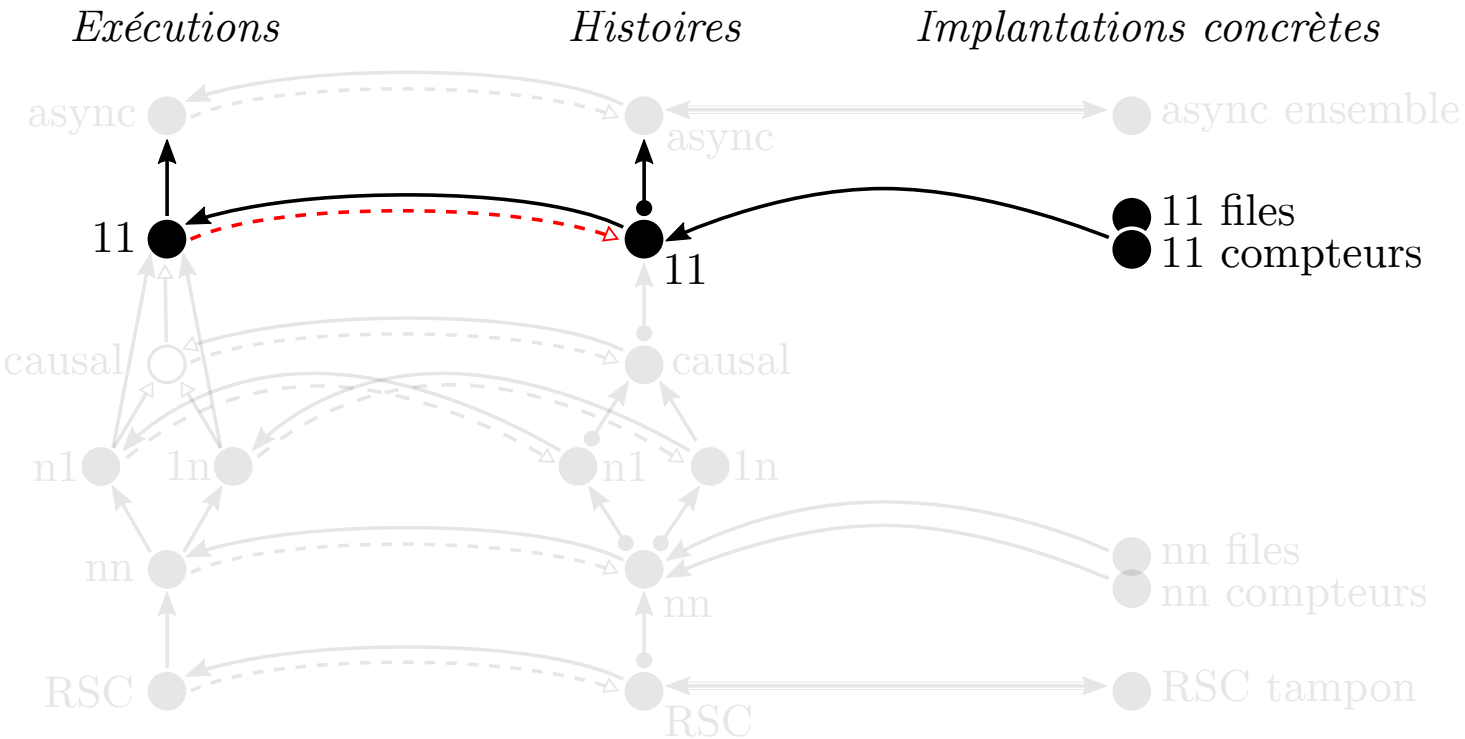


Histoire d'un message : ensemble des messages dont il dépend

Modèle de communication : garde sur les événements en fonction des histoires

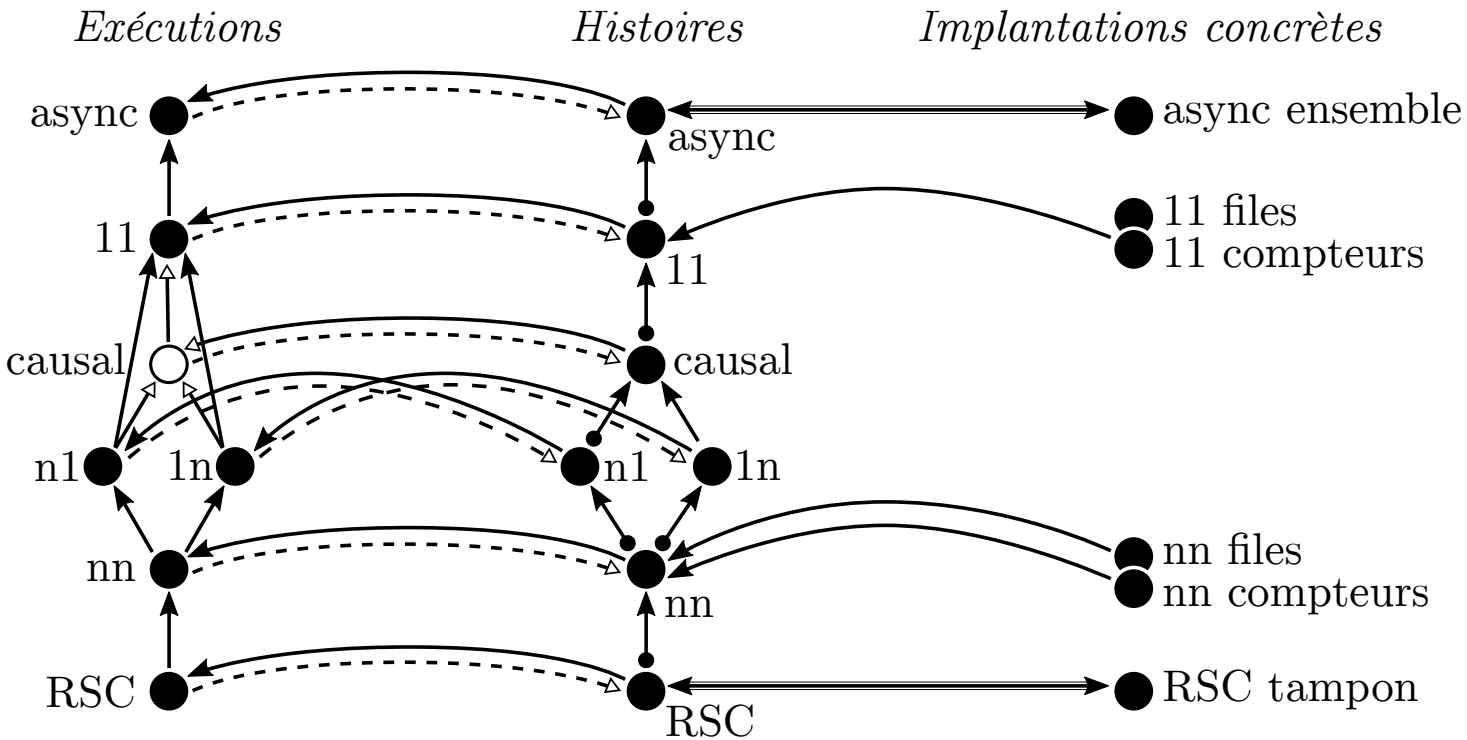
spécification manuelle ○
spécification (Event-B ou TLA+) ●
raffine (preuve manuelle) ⟶▷
raffine (preuve Event-B) ⟶
raffine (Event-B et TLA+) ●⟶
sous hypothèses - - - -
identité ⟺

Aperçu des relations



spécification manuelle
spécification (Event-B ou TLA+)
raffine (preuve manuelle)
raffine (preuve Event-B)
raffine (Event-B et TLA+)
sous hypothèses
identité

Aperçu des relations



spécification manuelle ○ raffine (preuve manuelle) ⟶ sous hypothèses - - - -
spécification (Event-B ou TLA+) ● raffine (preuve Event-B) ⟶ identité ⟺
raffine (Event-B et TLA+) ●⟶

Conclusion

- Étude des modèles de communication
  - Dans l'absolu
  - Pour la compatibilités de compositions de pairs
- Mise en évidence des substituabilités
- Framework de vérification automatisée (model checking)
- Approches de spécification unifiées
- Mécanisation des preuves de raffinements avec TLA$^+$ Proof System et Event-B
- Perspectives :
  - Parfaire et enrichir l'état des lieux des relations
  - Communication point à point $\rightarrow$ Diffusion

Conclusion

- Étude des modèles de communication
  - Dans l'absolu
  - Pour la compatibilités de compositions de pairs
- Mise en évidence des substituabilités
- Framework de vérification automatisée (model checking)
- Approches de spécification unifiées
- Mécanisation des preuves de raffinements avec TLA$^+$ Proof System et Event-B
- Perspectives :
  - Parfaire et enrichir l'état des lieux des relations
  - Communication point à point $\rightarrow$ Diffusion

Merci de votre attention

Questions ?