Latence and fraîcheur pire cas sur systèmes avioniques modulaires intégrées

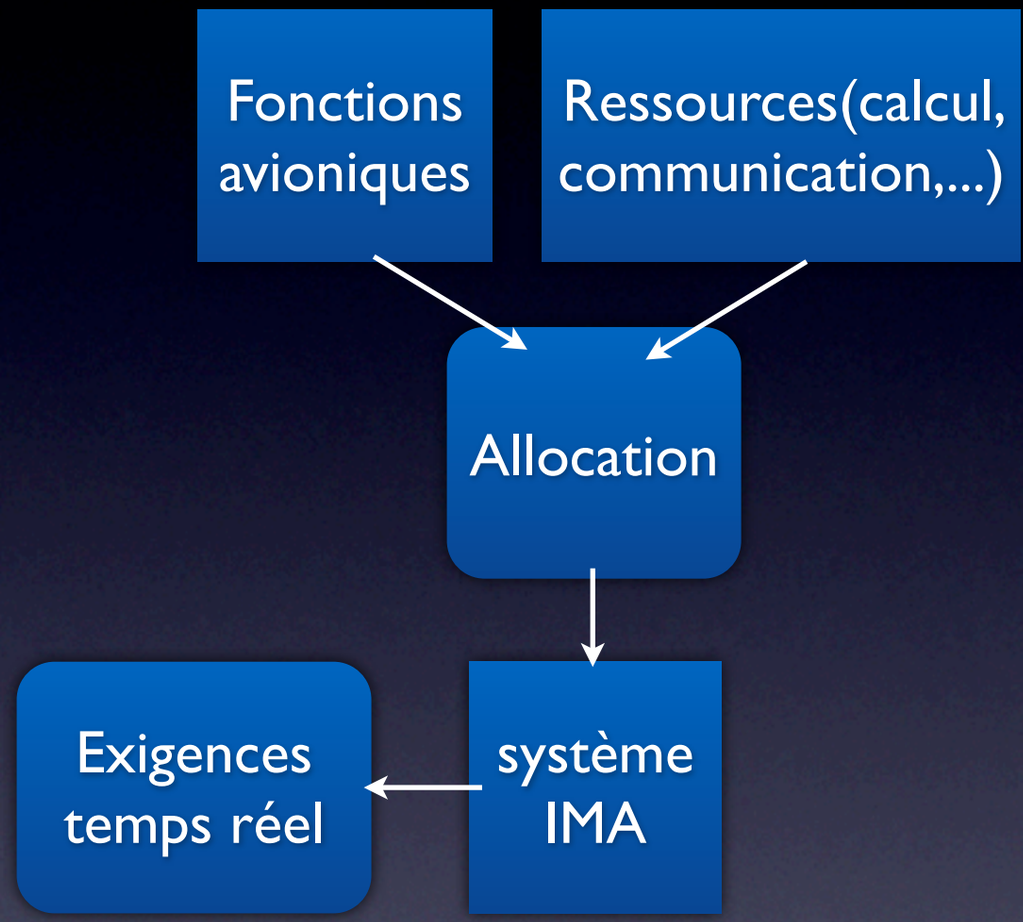
Michaël Lauer, Jérôme Ermont
Université de Toulouse - IRIT - ENSEEIHT - INPT

Frédéric Boniol, Claire Pagetti
ONERA

MSR 2011

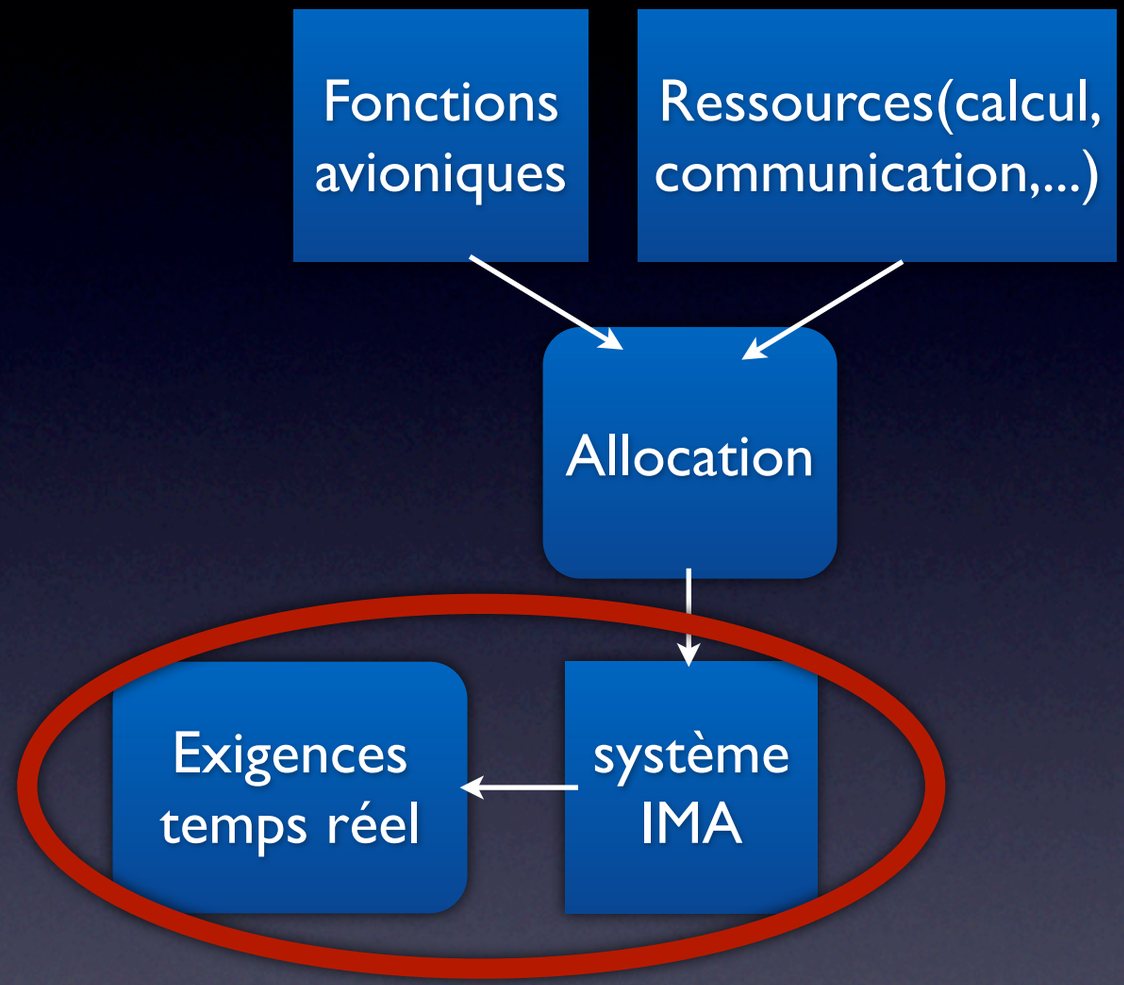
SATRIMMAP

- SAfety and Time cRItical Middleware for future Modular Avionics Platform
- Financement ANR (2008-2011)
- Airbus, CEA, IRIT, LAAS, ONERA, QoS Design



SATRIMMAP

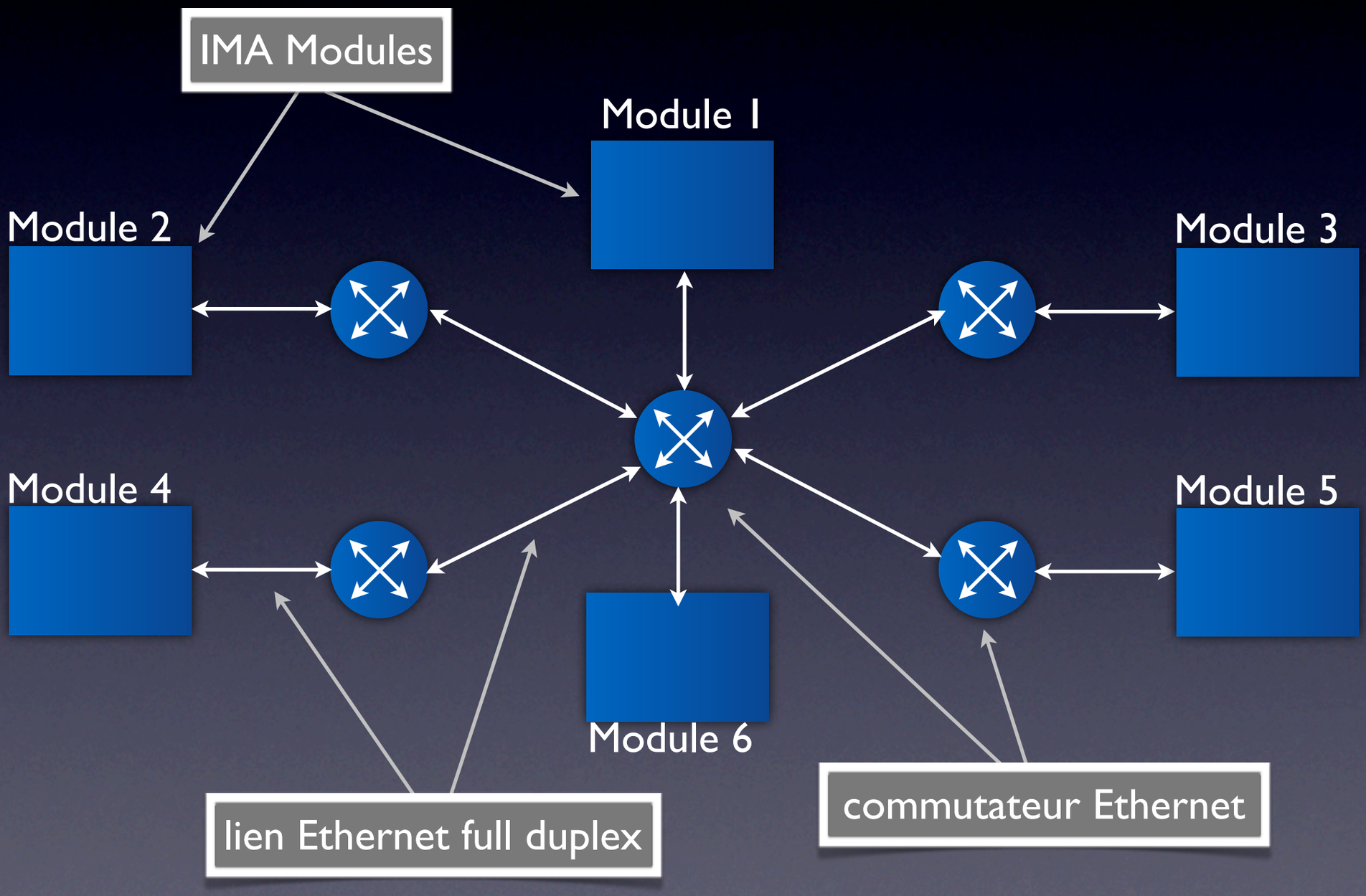
- SAfety and Time cRItical Middleware for future Modular Avionics Platform
- Financement ANR (2008-2011)
- Airbus, CEA, IRIT, LAAS, ONERA, QoS Design



Latence/fraîcheur sur systèmes IMA

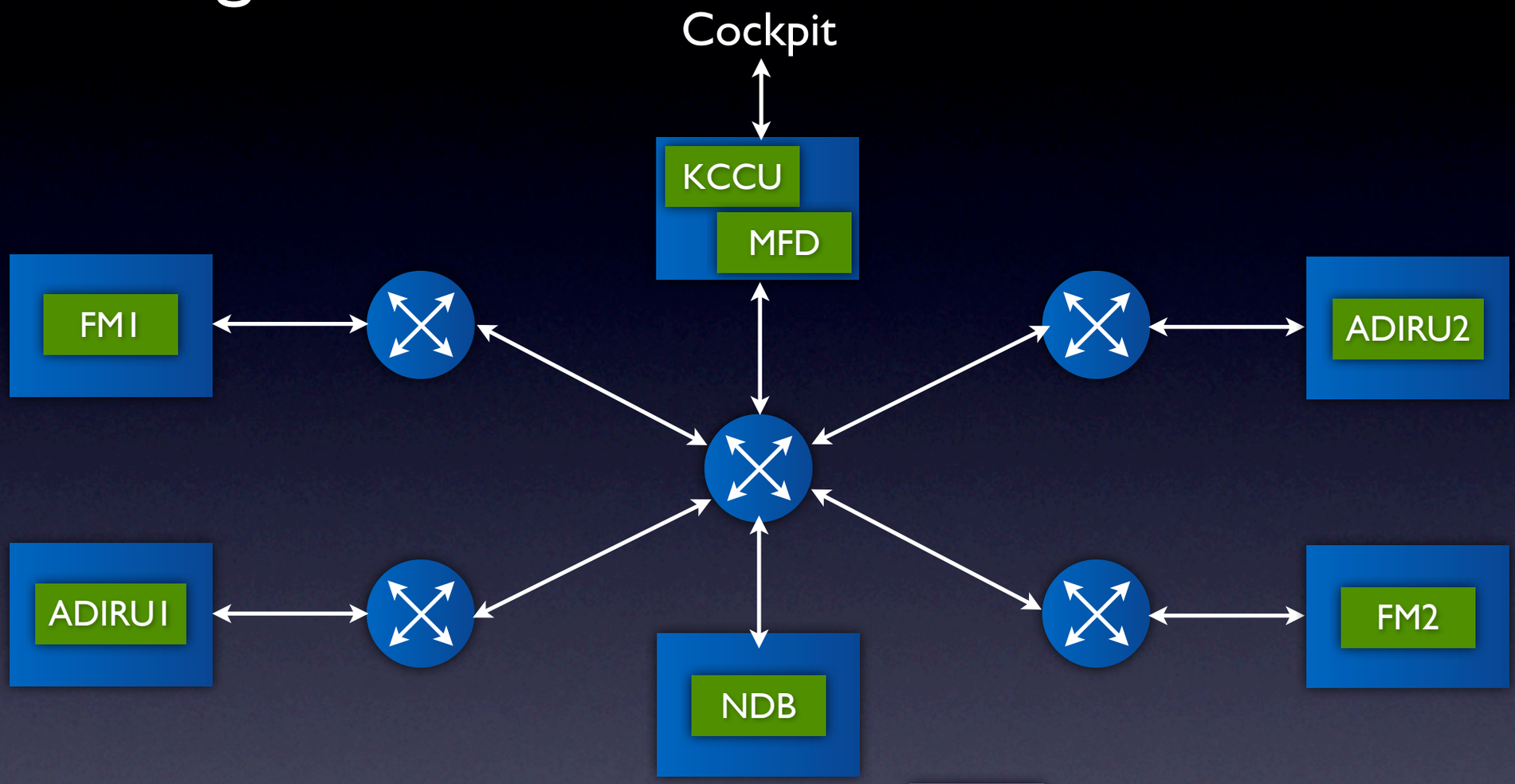
- Introduction
  - systèmes IMA
  - exigences temps réel
- Vérification des exigences
- Expérimentations
- Conclusion et perspectives

Systèmes IMA : matériel



Systèmes IMA : calcul

Système de gestion de vol



Partitions :
(Arinc 653)

KCCU	Keyboard and Cursor Control Unit
MFD	MultiFunctional Display
FM	Flight Manager
ADIRU	Air Data Inertial Reference Unit
NDB	Navigation DataBase

Systèmes IMA : calcul

Système de gestion de vol

Cockpit

Ordonnancement statique des partitions:

MAjor time Frame (MAF)

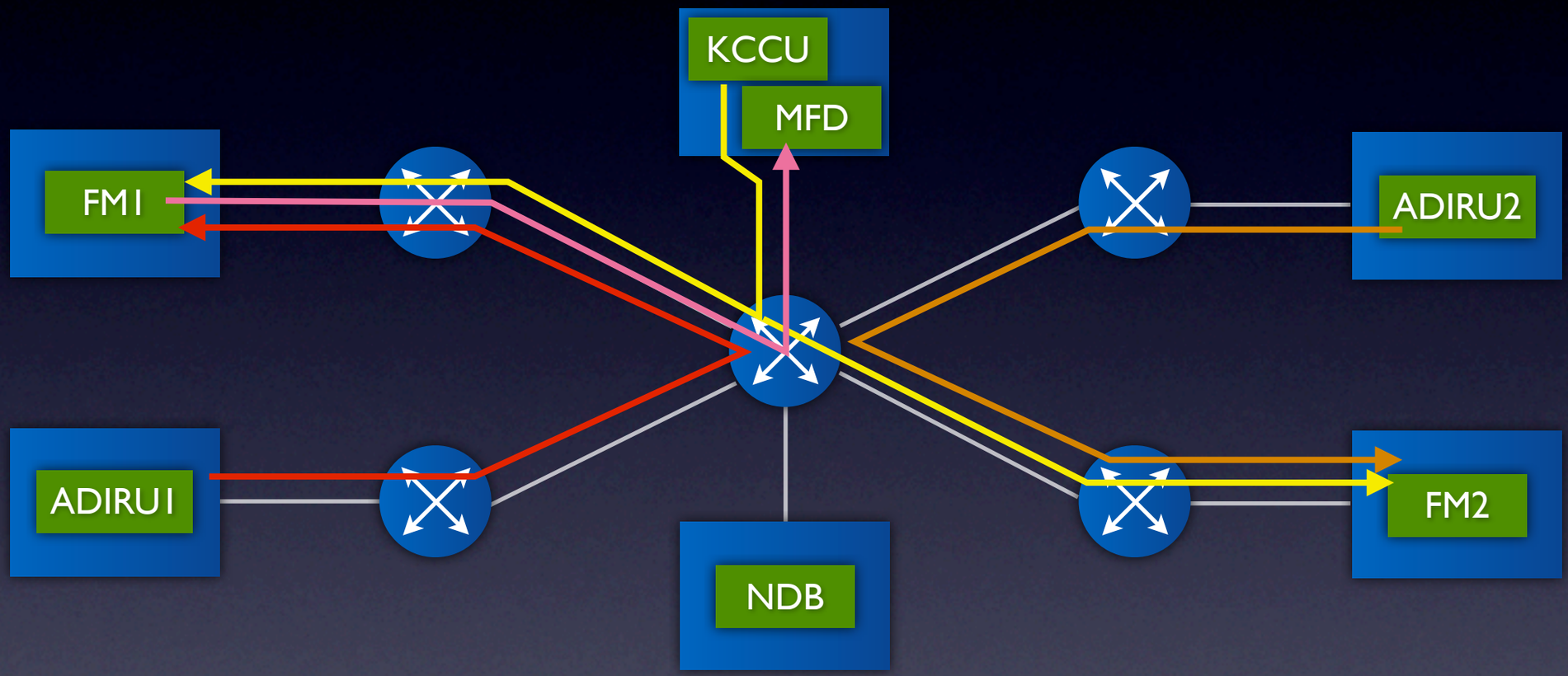
Module 1

trol Unit

	MFD	MultiFunctional Display
Partitions : (Arinc 653)	FM	Flight Manager
	ADIRU	Air Data Inertial Reference Unit
	NDB	Navigation DataBase

Systèmes IMA : communication

Système de gestion de vol



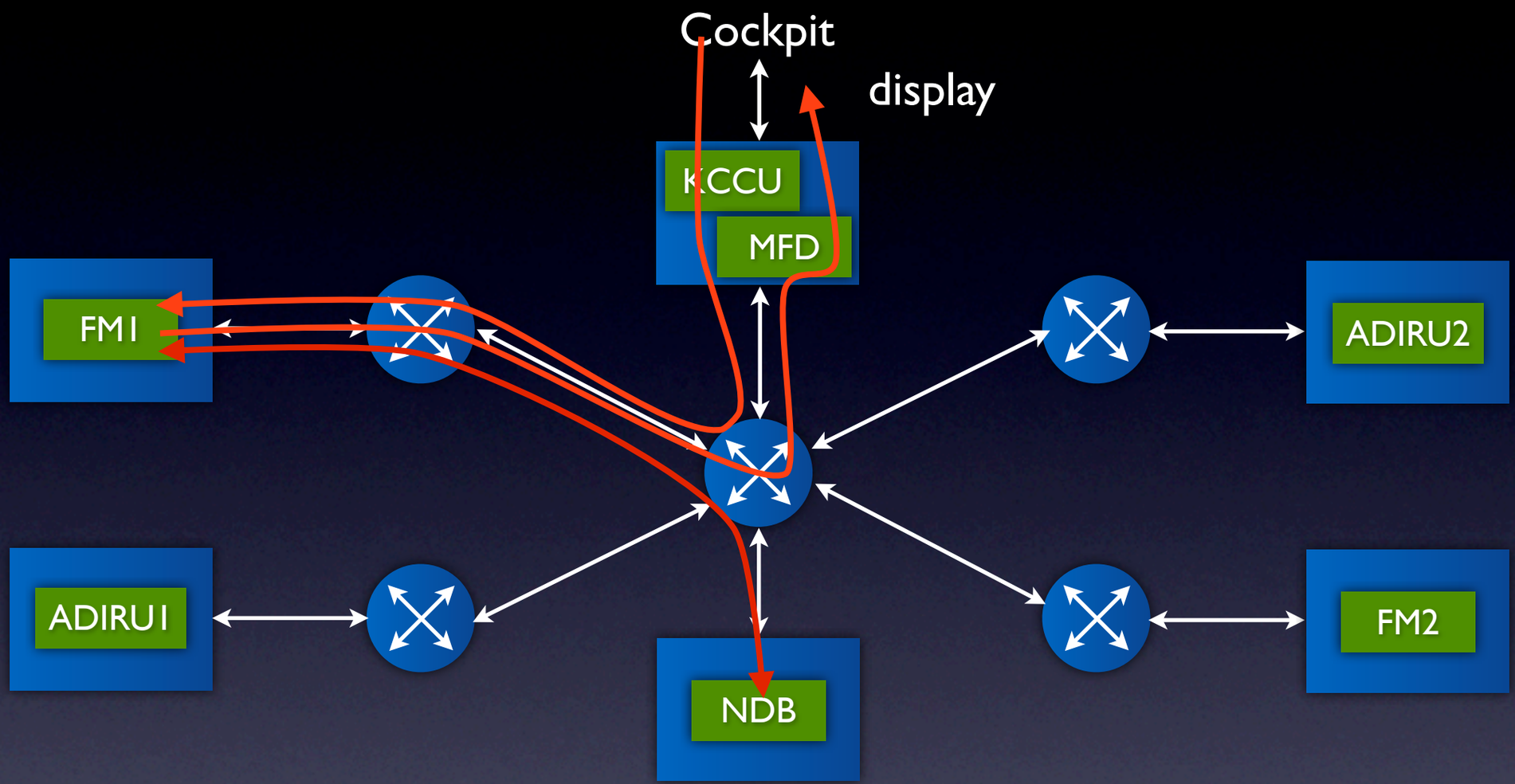
Virtual Links :
(Arinc 664/AFDX)

VL_1
VL_2
VL_3
VL_4

Latence/fraîcheur sur systèmes IMA

- Introduction
  - systèmes IMA
  - exigences temps réel → Latence, Fraîcheur
- Vérification des exigences
- Expérimentations
- Conclusion et perspectives

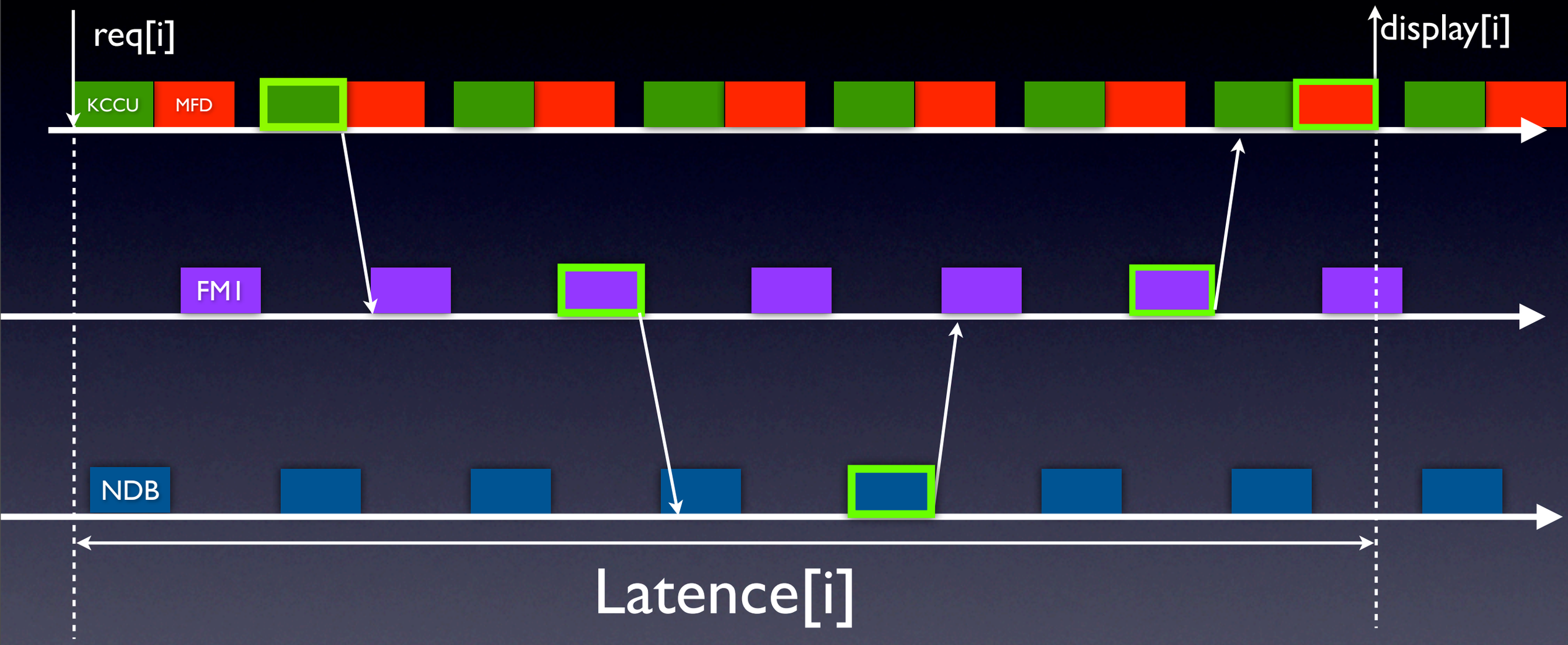
Exigence de latence



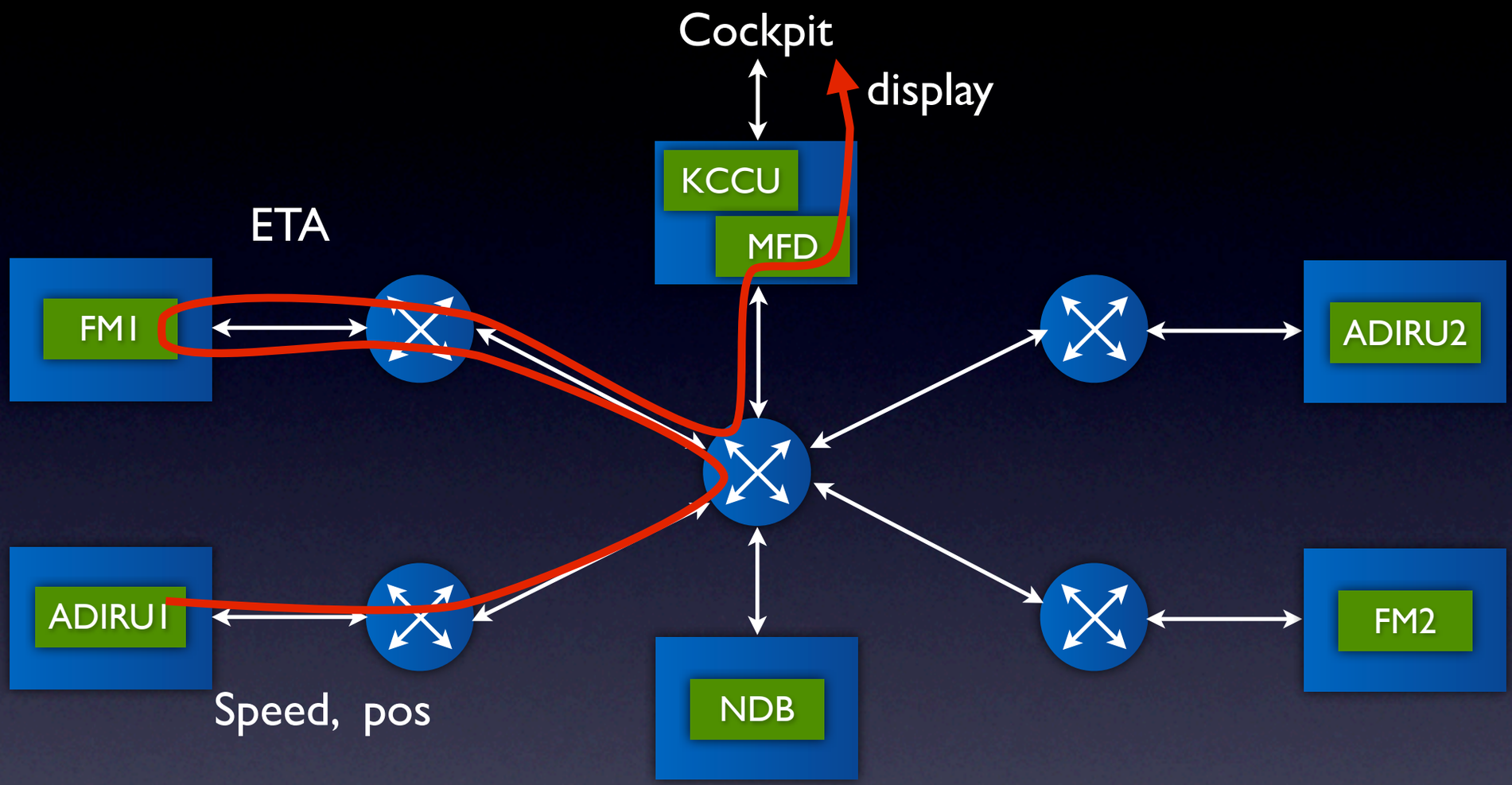
Chaîne fonctionnelle:

$$\underbrace{pilot \rightarrow KCCU \rightarrow FM1 \rightarrow ND \rightarrow FM1 \rightarrow MFD \rightarrow pilot}_{latency \leq 700ms}$$

Exigence de latence



Exigence de fraîcheur

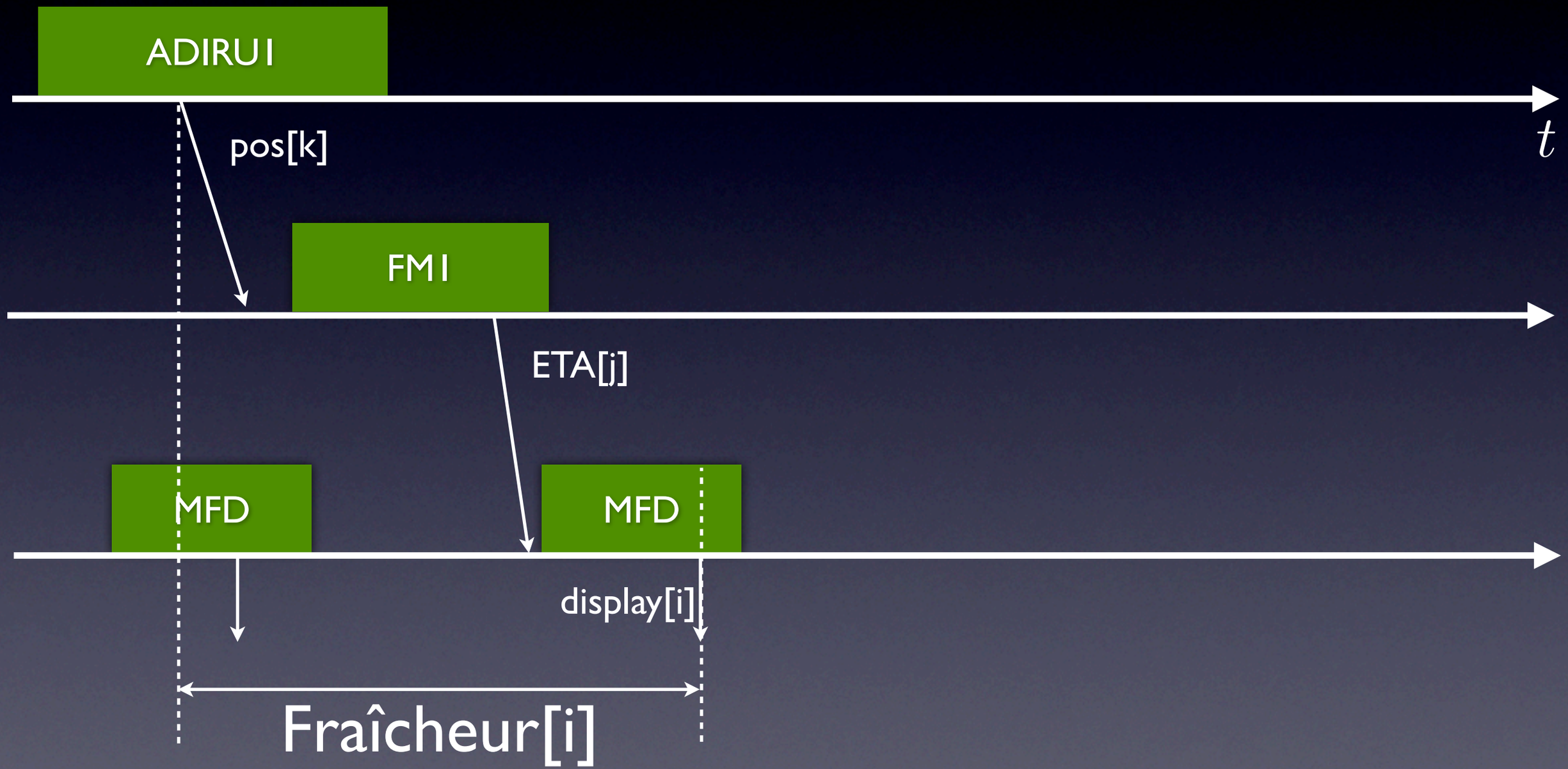


Chaîne fonctionnelle :

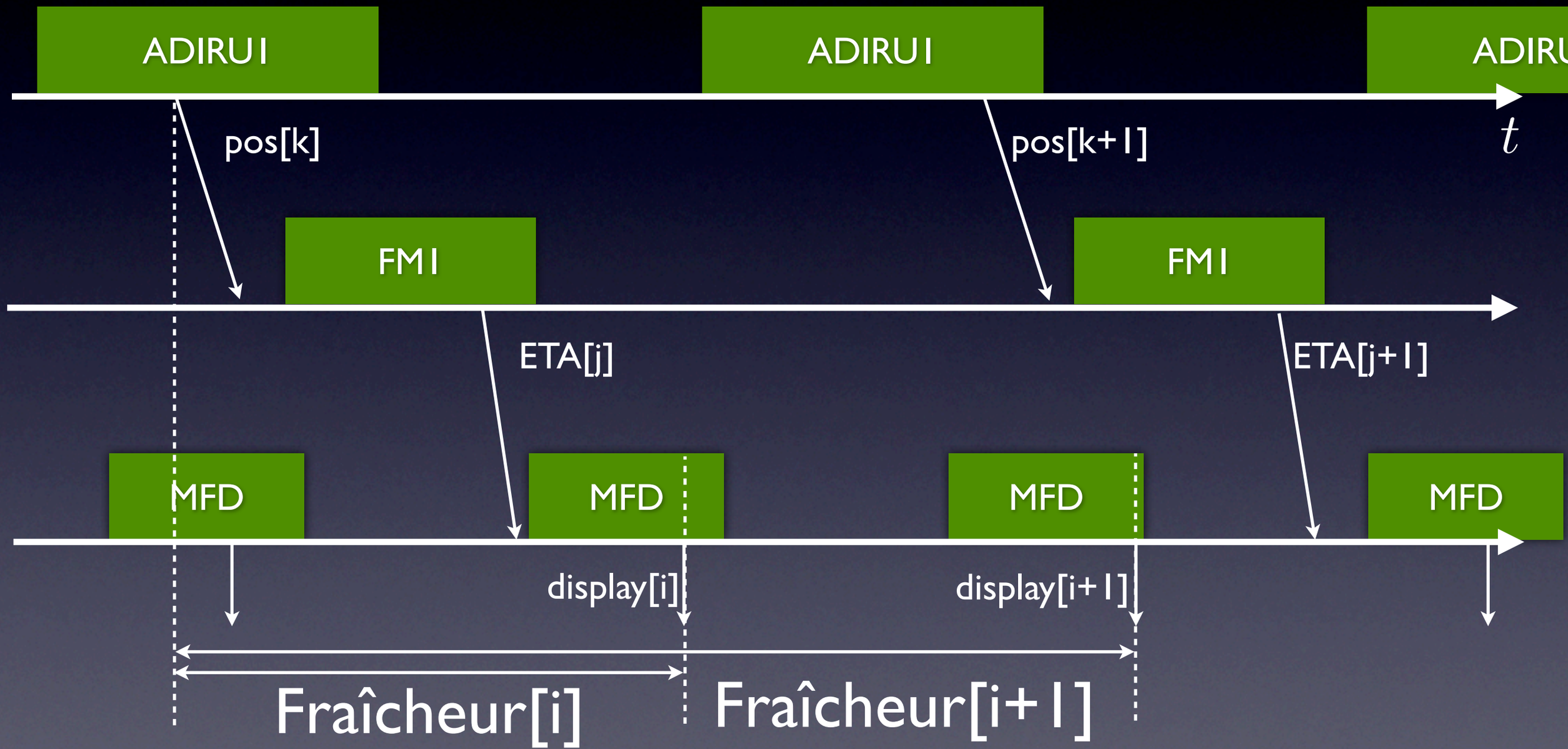
$$\underbrace{ADIRU1 \rightarrow FM1 \rightarrow MFD \rightarrow pilot}_{freshness \leq 500ms}$$

ETA: Estimated Time of Arrival

Exigence de fraîcheur



Exigence de fraîcheur



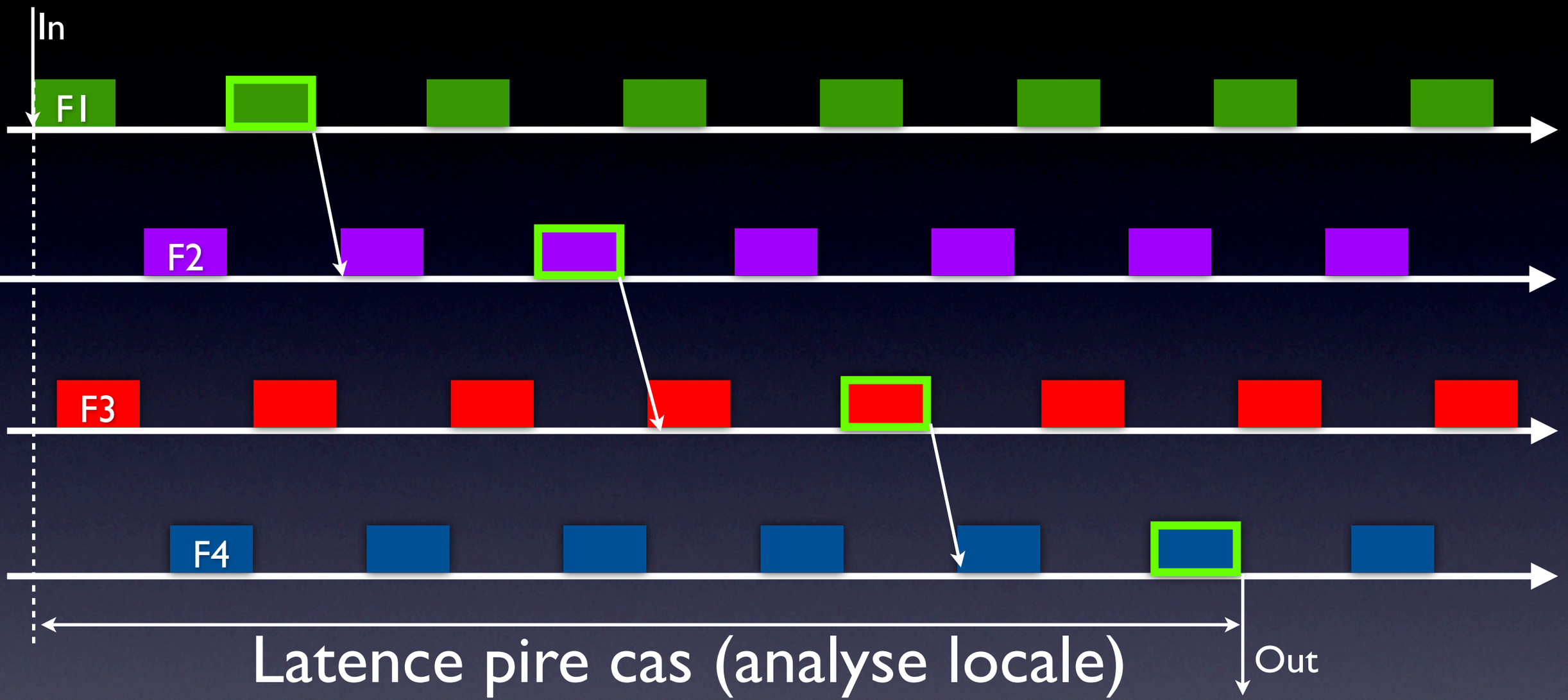
Latence/fraîcheur sur systèmes IMA

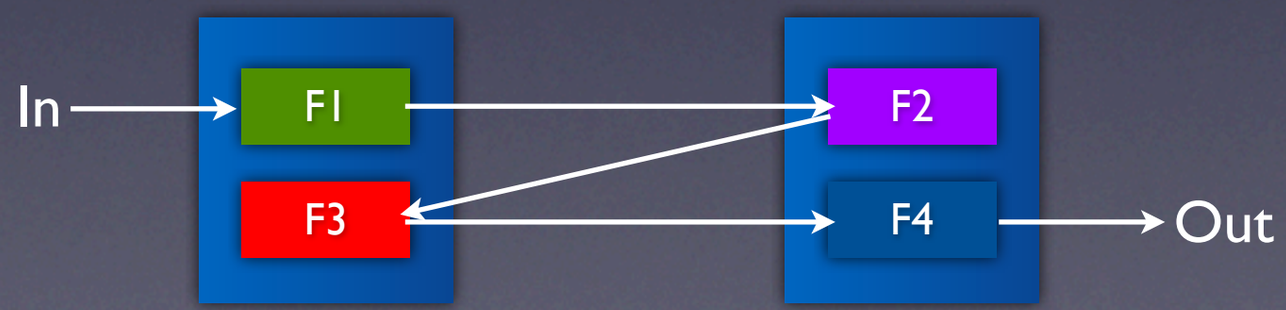
- Introduction
- Vérification des exigences
  - Formalisation : *tagged signal model*
  - Vérification : programmation linéaire
- Expérimentation
- Conclusion et perspectives

Etat de l'art

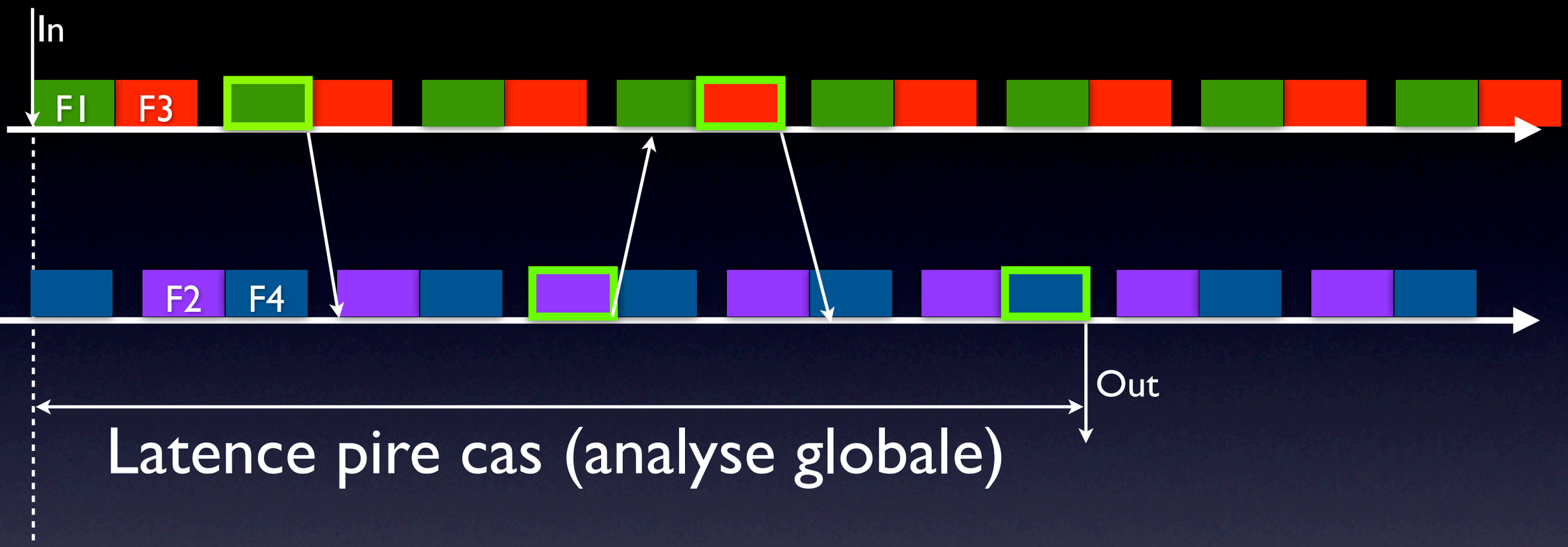
- Network calculus (J.Y. LeBoudec), approche par trajectoire (S. Martin) : latence pire cas dans les réseaux
- Automates temporisés + model-checking (F. Carcenac) : passage à l'échelle KO
- Real-time Calculus (L. Thiele) : passage à l'échelle OK, uniquement latence, analyse locale des composants => pessimisme

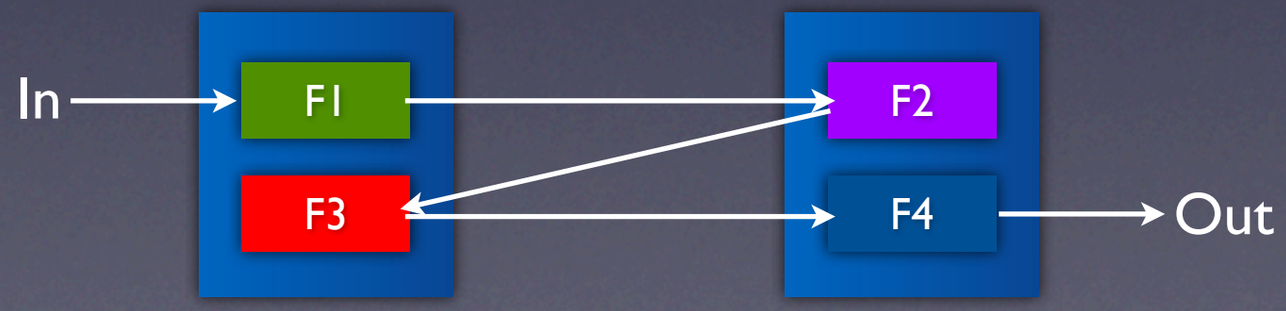
Analyse pire cas : locale vs globale



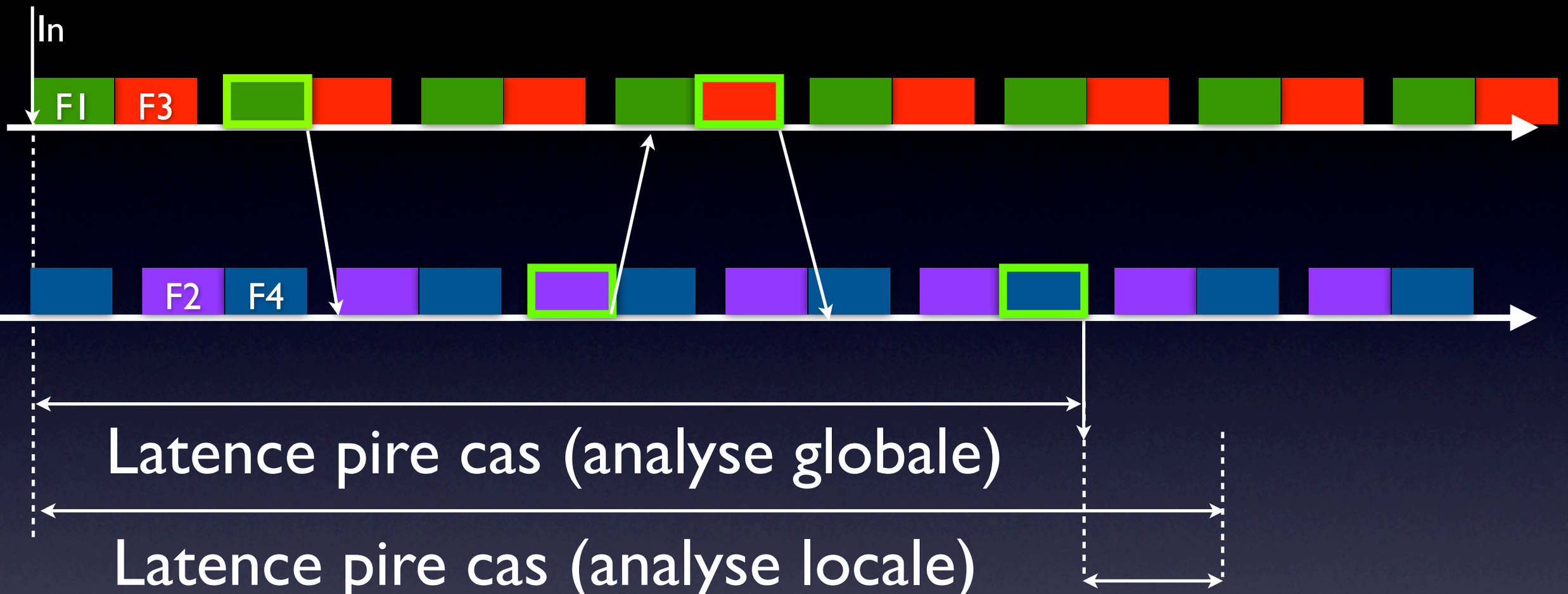


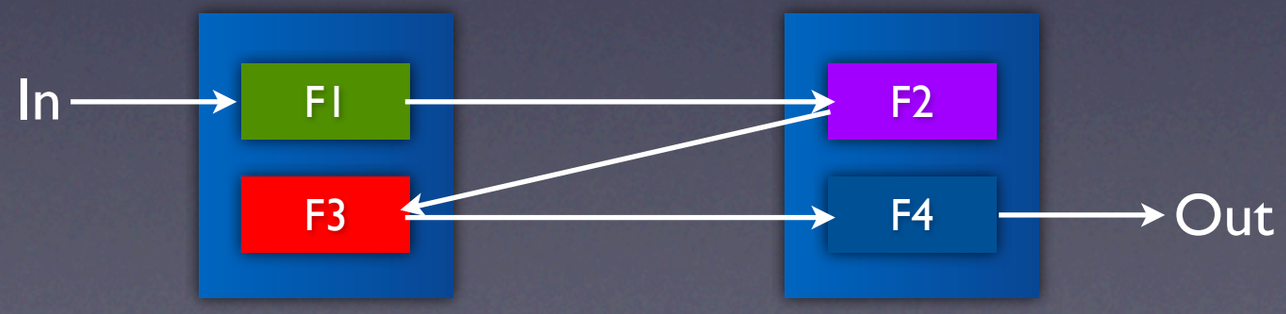
Analyse pire cas : locale vs globale





Analyse pire cas : locale vs globale

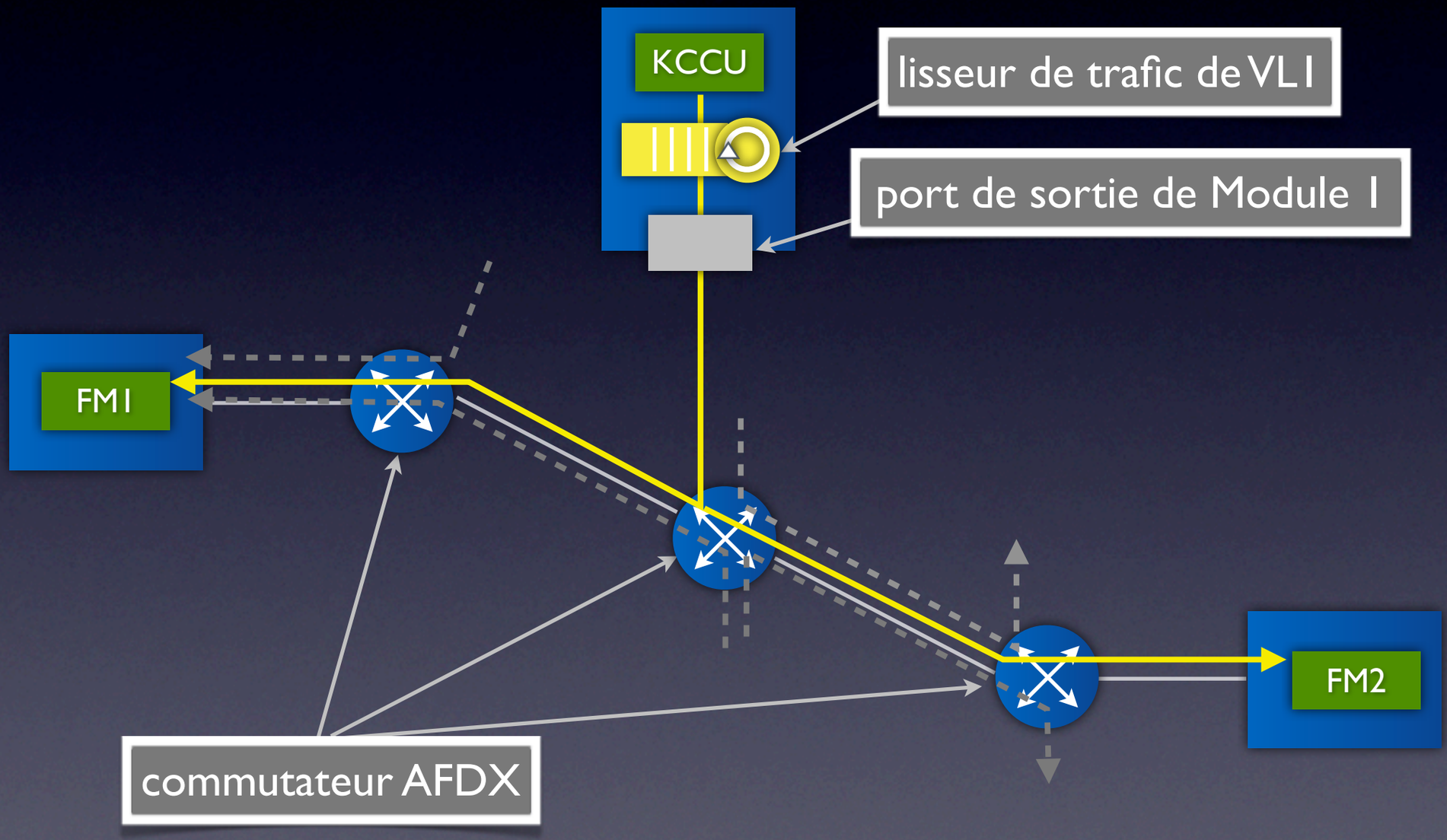




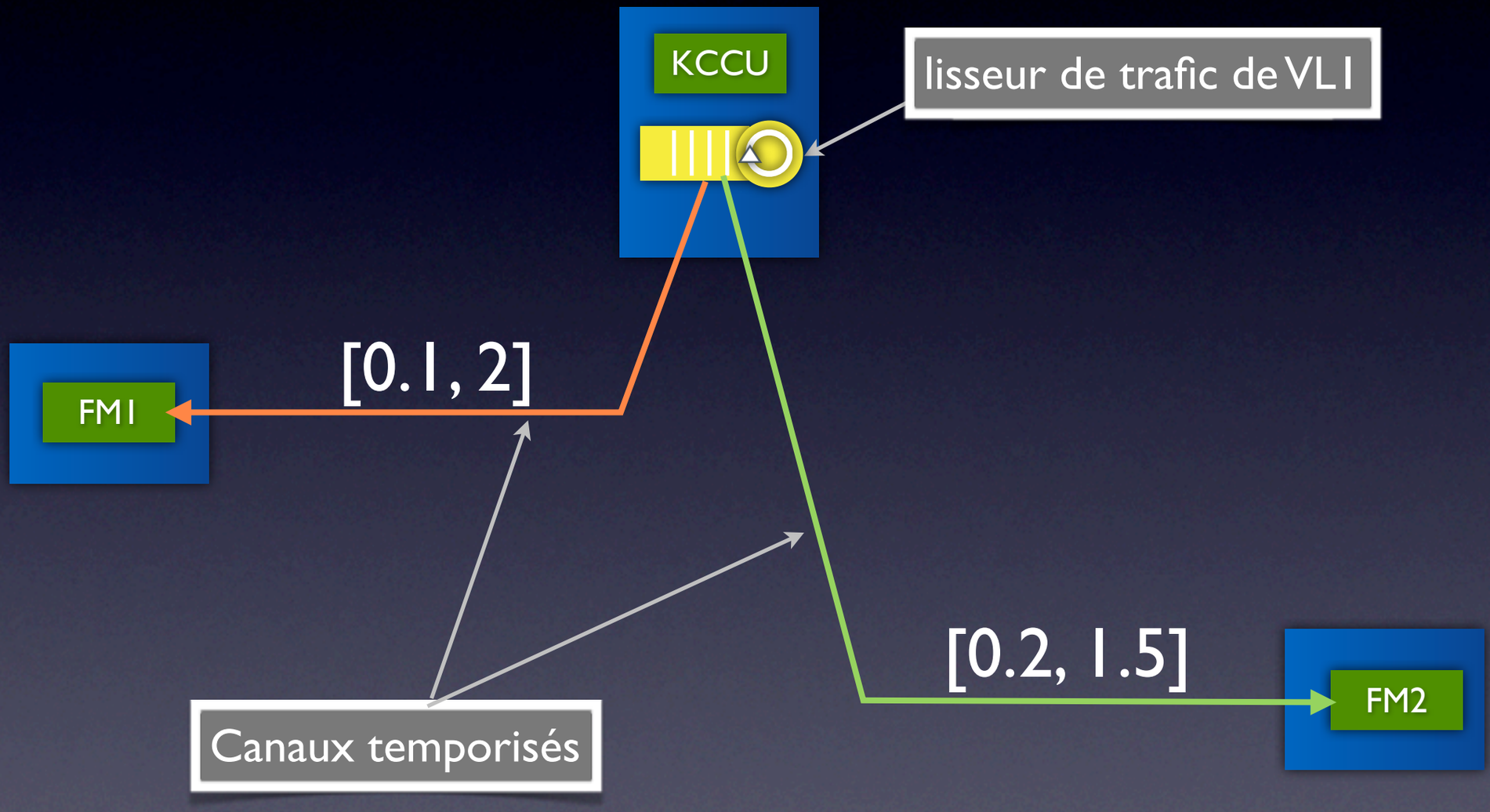
Méthode

1. Abstraction du réseau avec des *canaux temporisés* (approche par trajectoire)
2. Formalisation avec le *tagged signal model* [Lee & Sangiovanni-Vincentelli 96]: comportement temporelle + dépendances entre événements
3. Vérification : solution optimale d'un programme linéaire

Abstraction du réseau



Abstraction du réseau



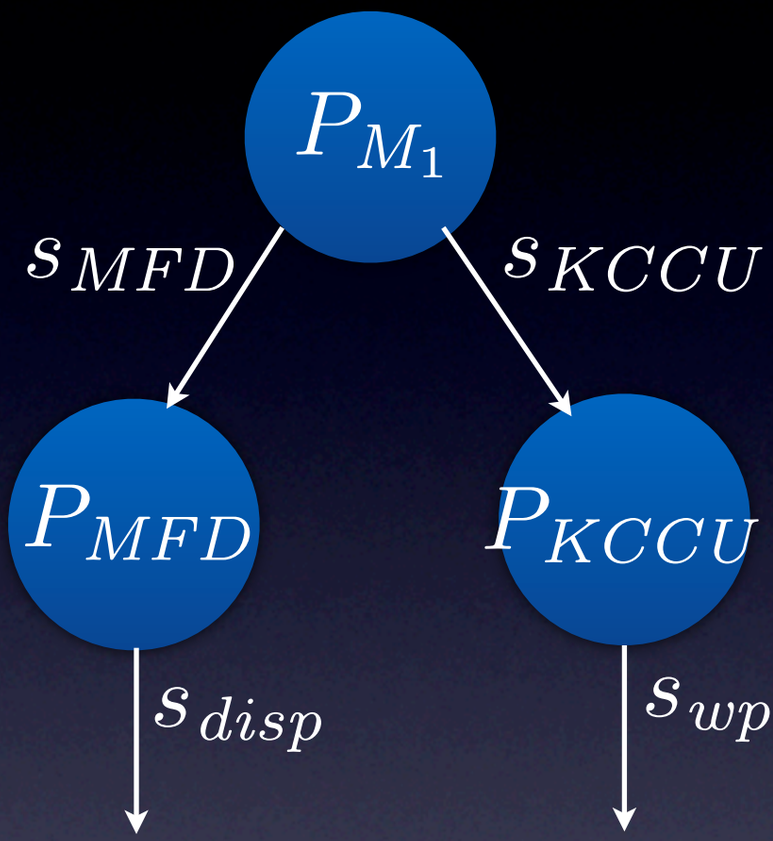
Bornes : approche par trajectoire

Méthode

1. Abstraction du réseau avec des *canaux temporisés* (approche par trajectoire)
2. Formalisation avec le *tagged signal model* [Lee & Sangiovanni-Vincentelli 96]: comportement temporelle + dépendances entre événements
3. Vérification : solution optimale d'un programme linéaire

Tagged signal model

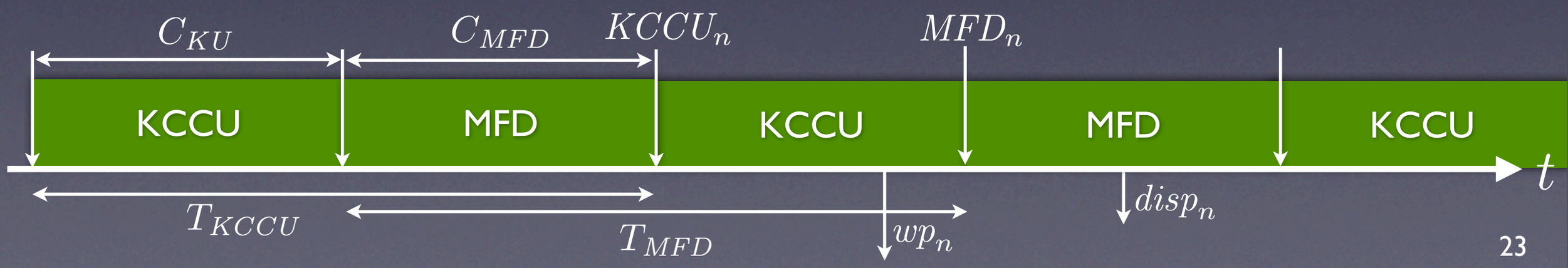
processus : ensemble des comportements possibles



$$P_{M_1} = \{(s_{MFD}, s_{disp}, s_{KU}, s_{wp}) \in S^4 | \forall n \in \mathbb{N}$$
$$t_n^{KCCU} = n \cdot T_{KCCU}$$
$$t_n^{MFD} = C_{KU} + n \cdot T_{MFD}\}$$

$$P_{MFD} = \{(s_{MFD}, s_{disp}, s_{KU}, s_{wp}) \in S^4 | \forall n \in \mathbb{N}$$
$$t_n^{MFD} \leq t_n^{disp} \leq t_n^{MFD} + C_{MFD}\}$$

$$P_{KCCU} = \{(s_{MFD}, s_{disp}, s_{KU}, s_{wp}) \in S^4 | \forall n \in \mathbb{N}$$
$$t_n^{KCCU} \leq t_n^{wp} \leq t_n^{KCCU} + C_{KCCU}\}$$



Formalisation du système

- Comporements du système : intersection des processus

$$P_{M_1} \cap P_{MFD_1} \cap P_{KU_1}$$

- Conjonction de contraintes

Programmation linéaire

Méthode

1. Abstraction du réseau avec des *canaux temporisés* (approche par trajectoire)
2. Formalisation avec le *tagged signal model* [Lee & Sangiovanni-Vincentelli 96]: comportement temporelle + dépendances entre événements
3. Vérification : solution optimale d'un programme linéaire

Vérification

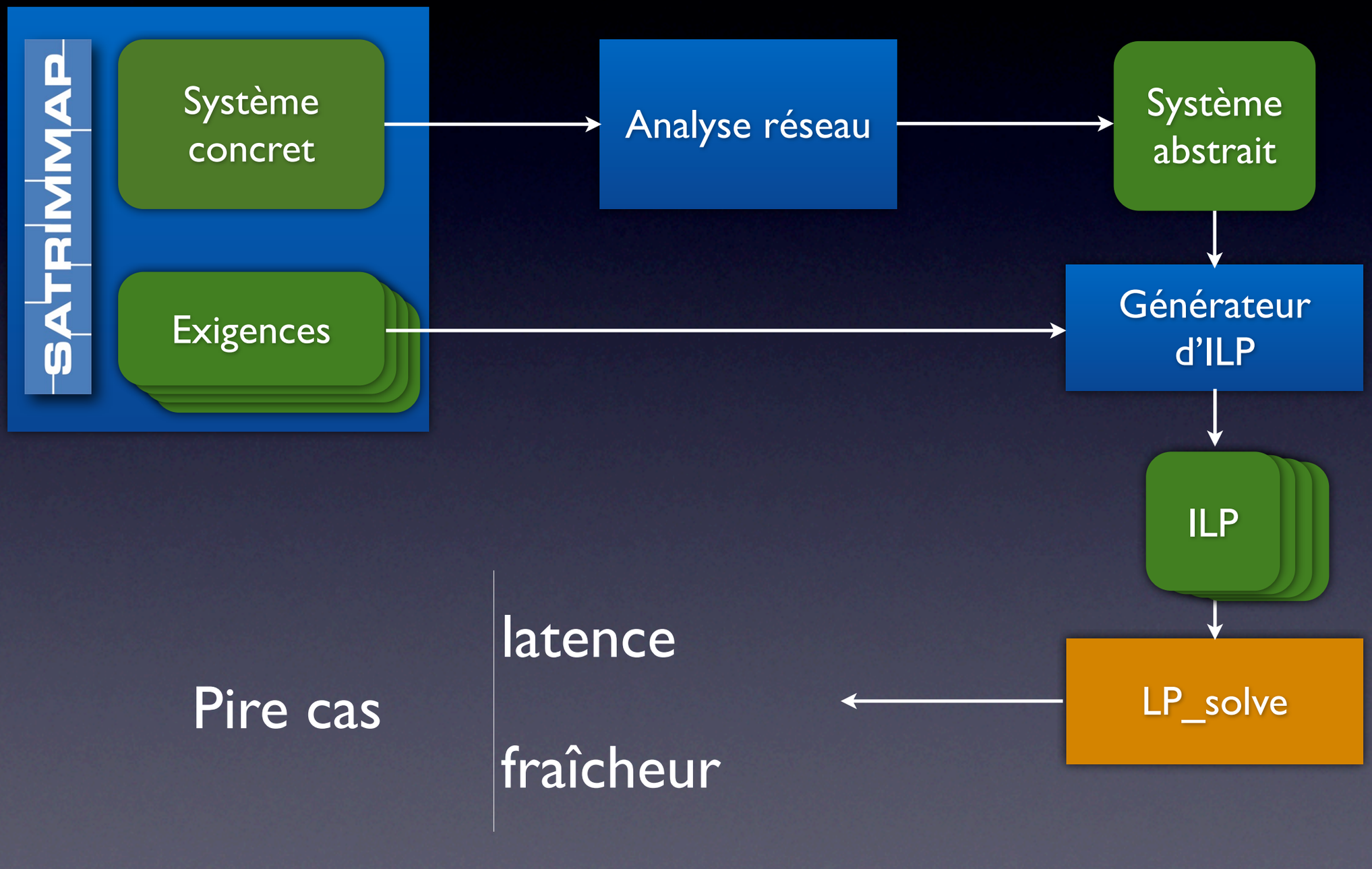
- Comportements du système : ensemble de contraintes
  - => Programmation linéaire (ILP)
  - Propriété : fonction objectif

e.g. pire cas de fraîcheur :

$$ADIRU1 \rightarrow FM1 \rightarrow MFD \rightarrow pilot$$
$$pos_k \rightarrow ETA_j \rightarrow disp_i$$

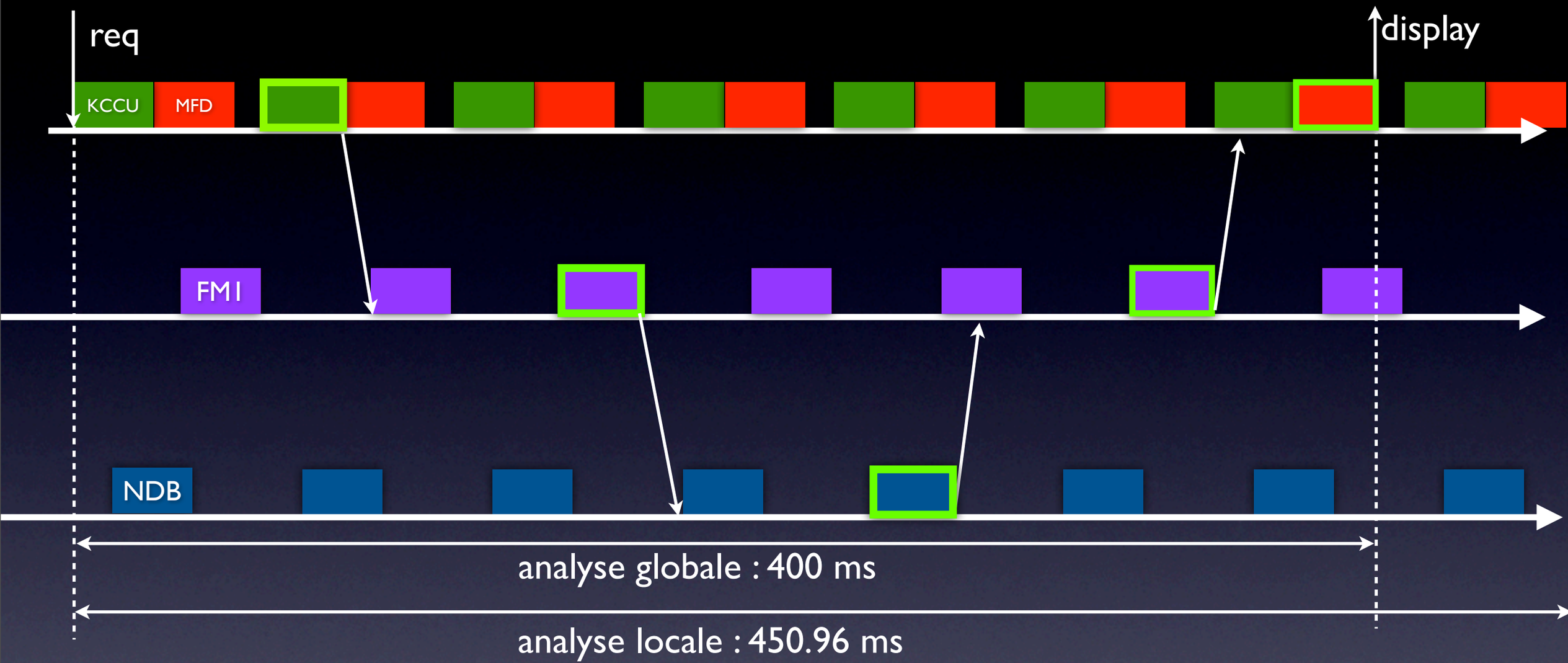
$$max : t_i^{disp} - t_k^{pos}$$

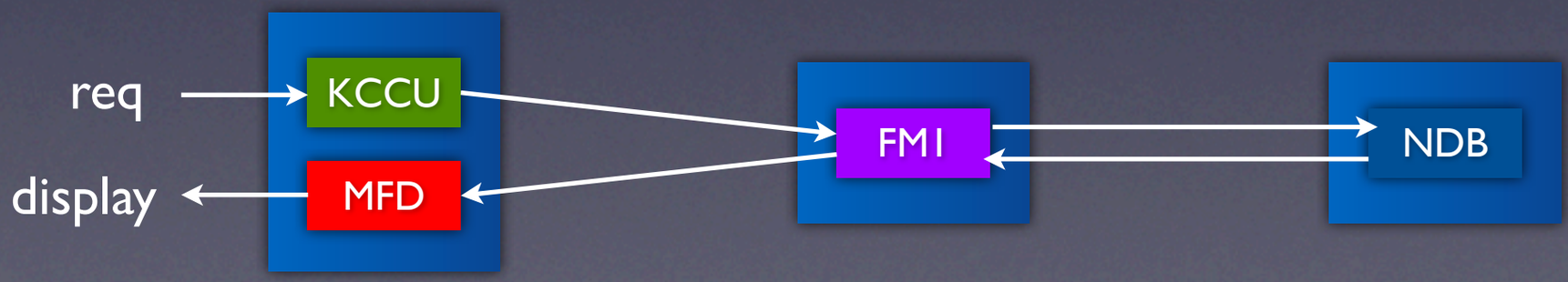
Outillage



Pire cas | latence | fraîcheur

Pire cas de latence





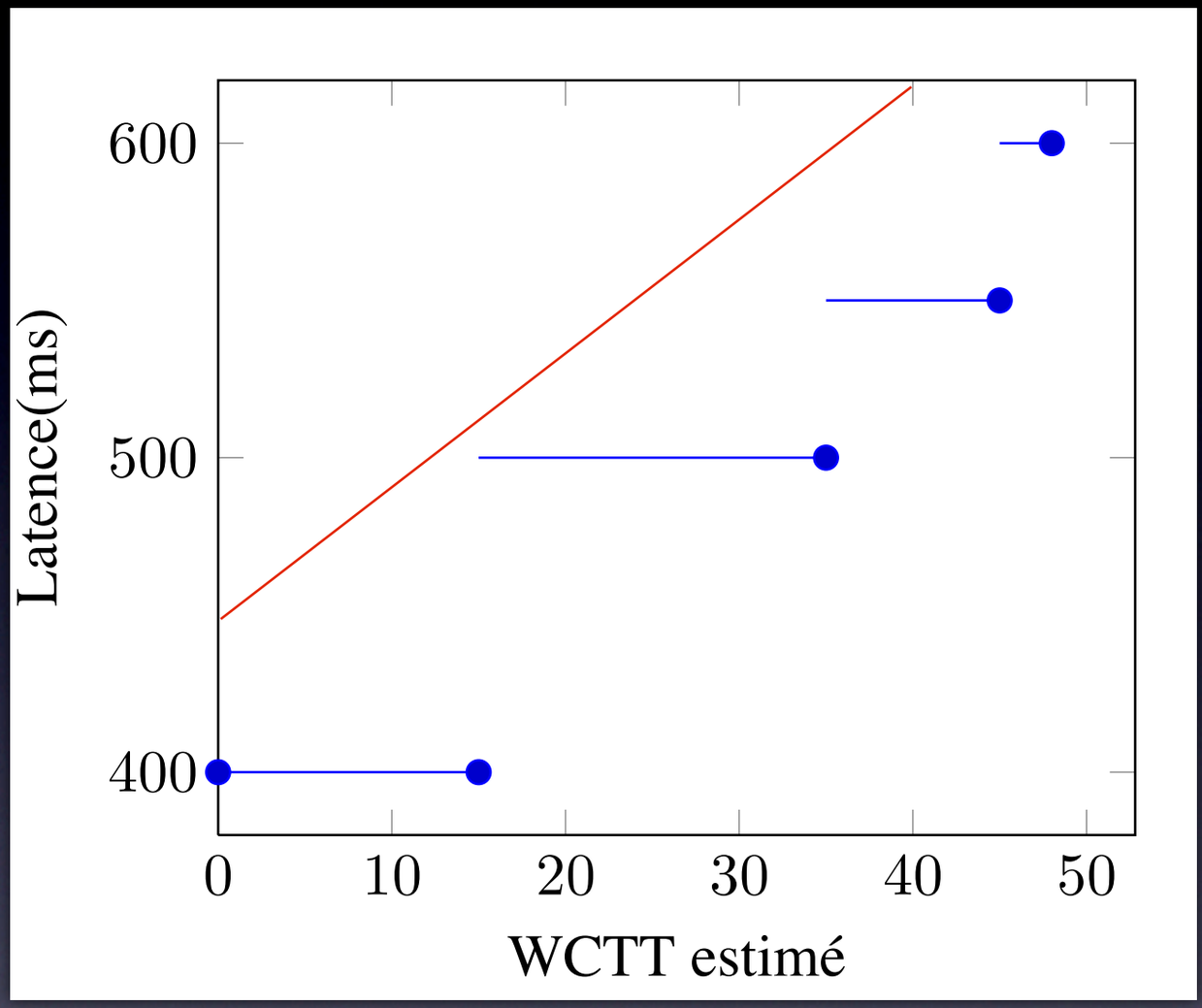
Latence/fraîcheur sur systèmes IMA

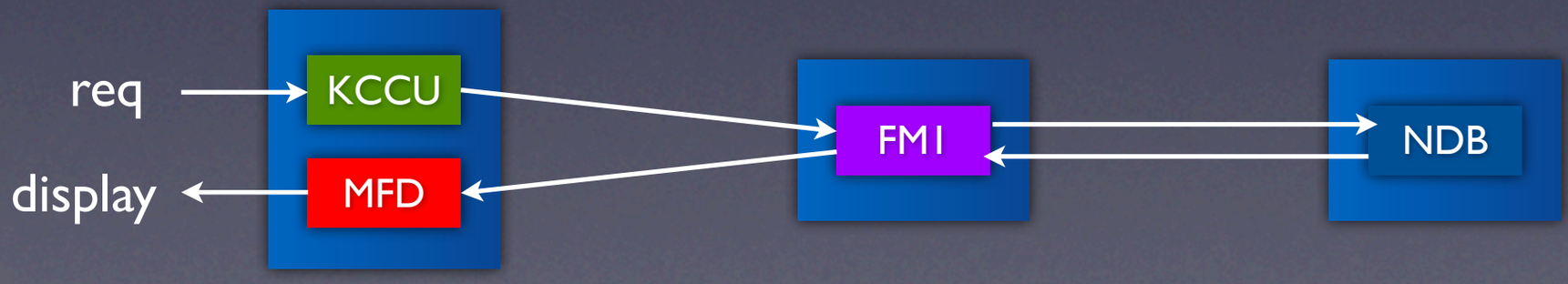
- Introduction
- Vérification des exigences
- Expérimentation
- Conclusion et perspectives

Expérimentations

locale :

globale :

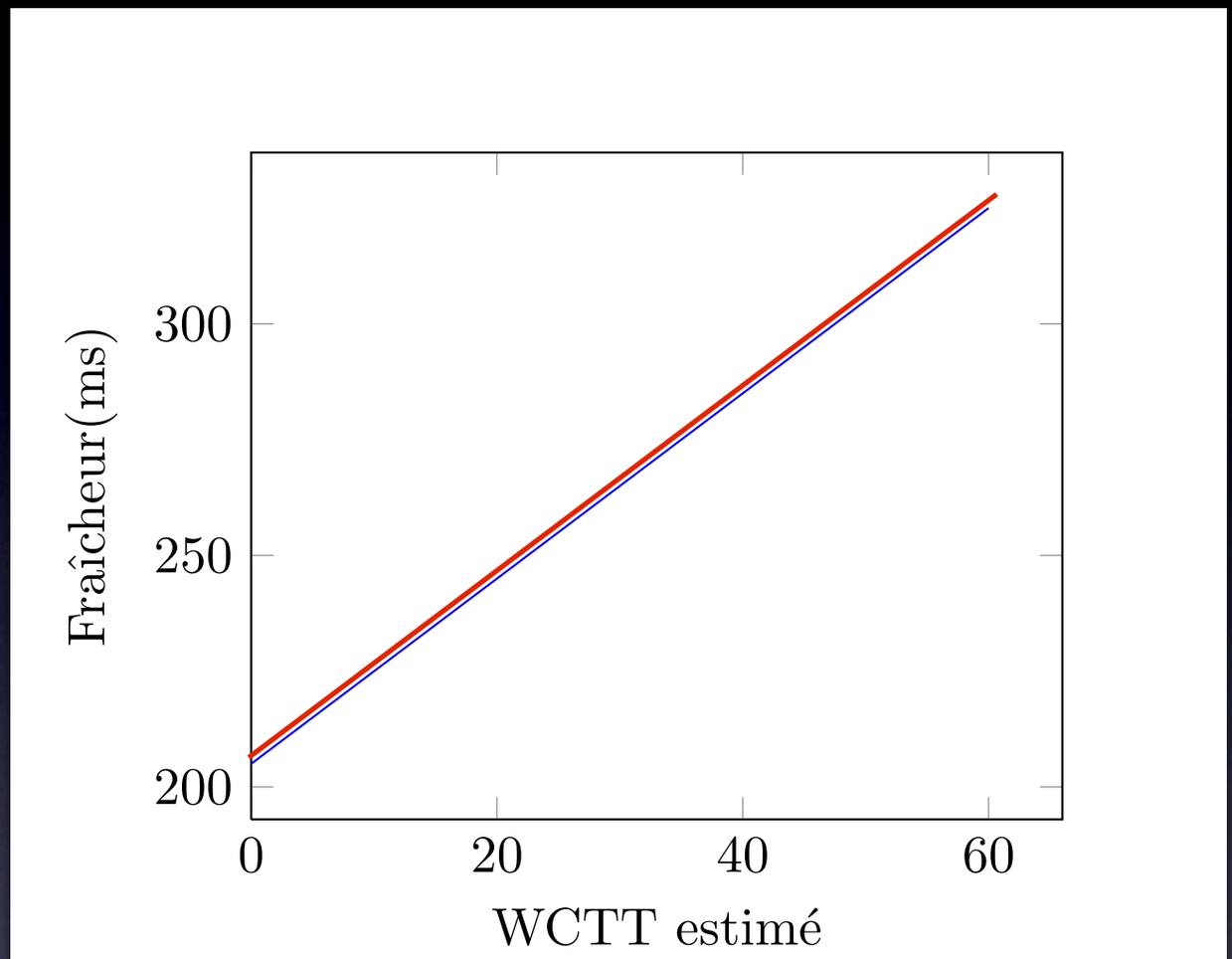




Expérimentations

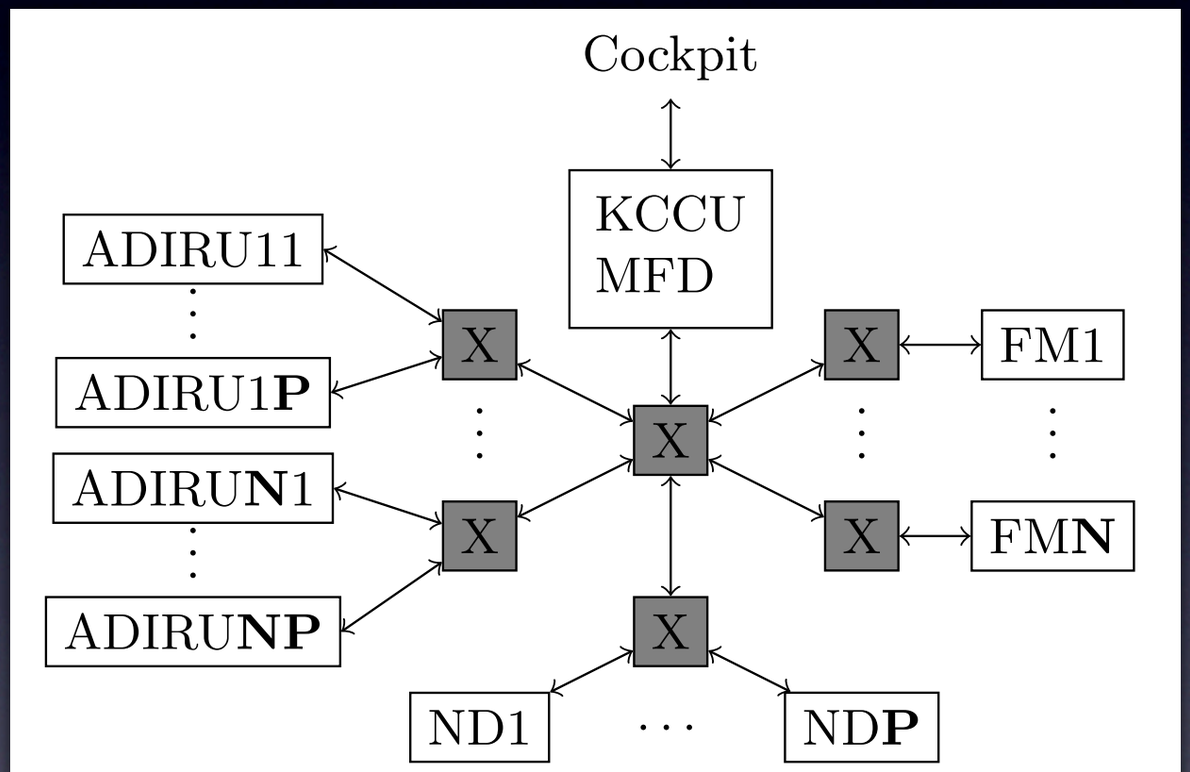
locale :

globale :



Expérimentations

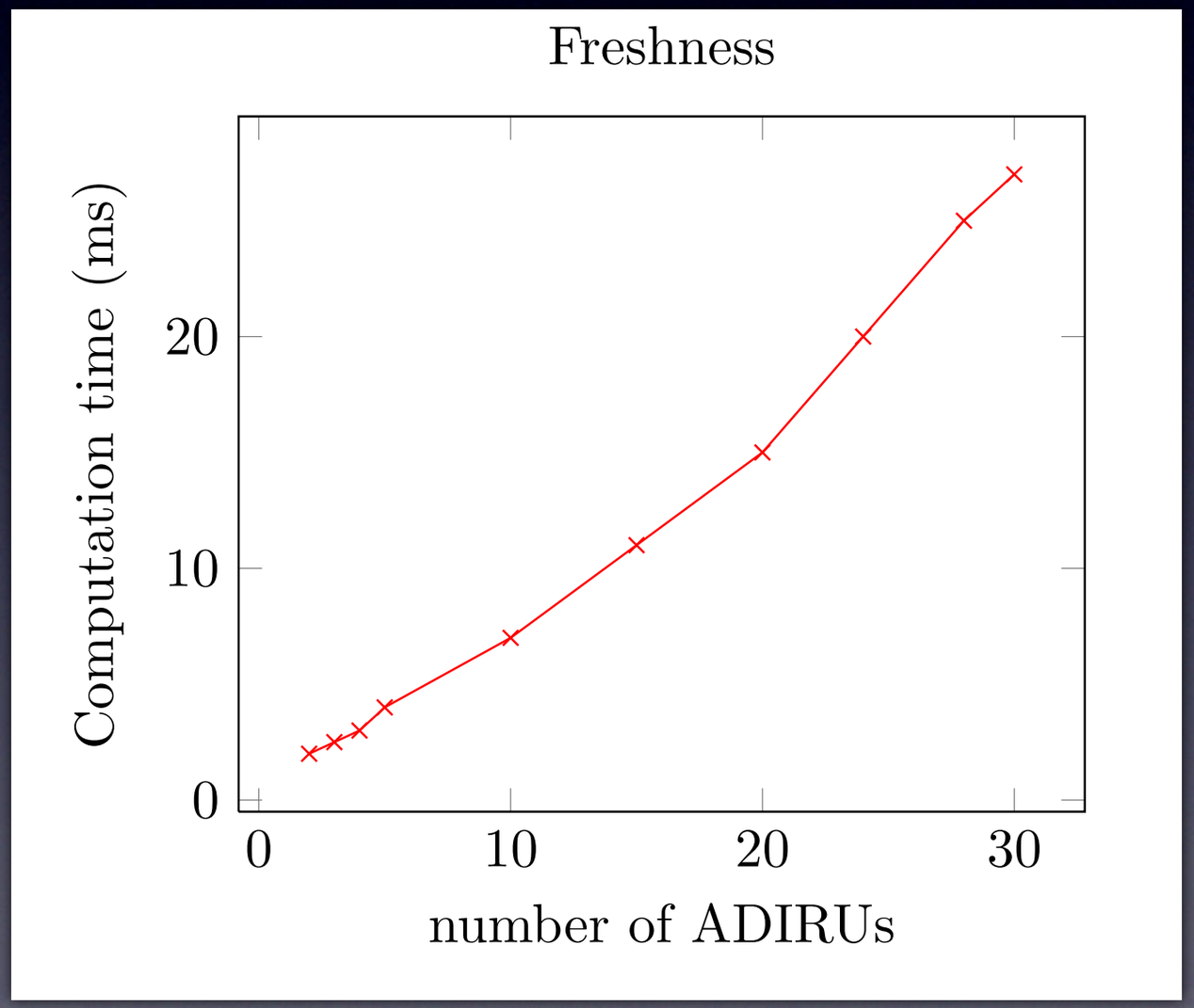
Etude de cas paramétrée



solveur : LP_solve
processeur : 2.53 GHz Intel Core 2 Duo

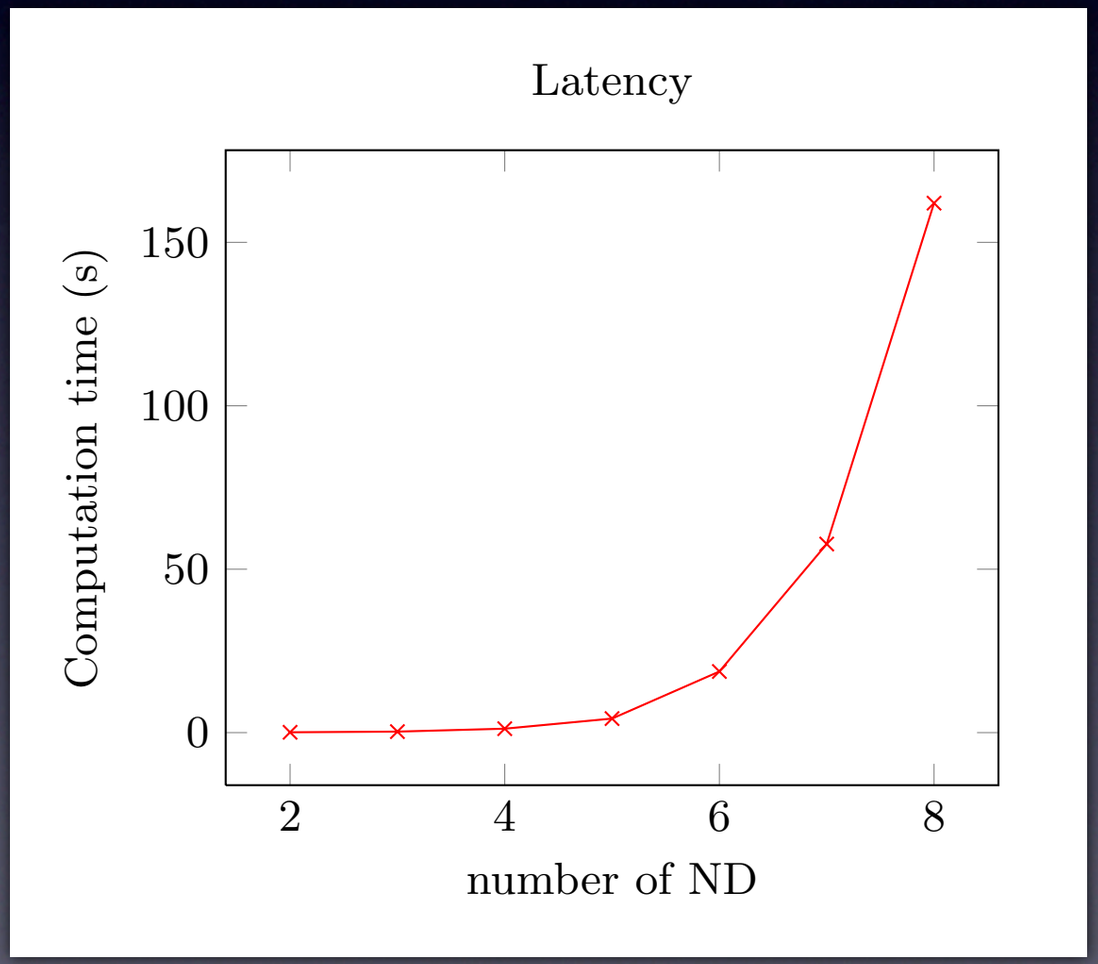
Expérimentations

$$ADIRU1P \rightarrow \ldots \rightarrow ADIRU11 \rightarrow FM1 \rightarrow MFD \rightarrow pilot$$



Expérimentations

$$pilot \rightarrow KCCU \rightarrow FM1 \rightarrow$$
$$ND0 \rightarrow \ldots \rightarrow NDP \rightarrow \ldots \rightarrow ND0 \rightarrow FM1 \rightarrow MFD \rightarrow pilot$$



Conclusion

- Formalisation de systèmes IMA avec le TSM
- Comportement temporel + dépendances entre événements
- Vérification d'exigences temps réel de bout-en-bout (latence, fraîcheur)
- Passage à l'échelle OK (par rapport au contexte industriel)

Perspectives

- Extension à d'autres exigences (meilleur cas, cohérence entre données,...)
- Lien avec les méthodes de conceptions (optimisation de système)
- Généralisation

Merci!

Questions ?

MSR 2011

SATRIMMAP

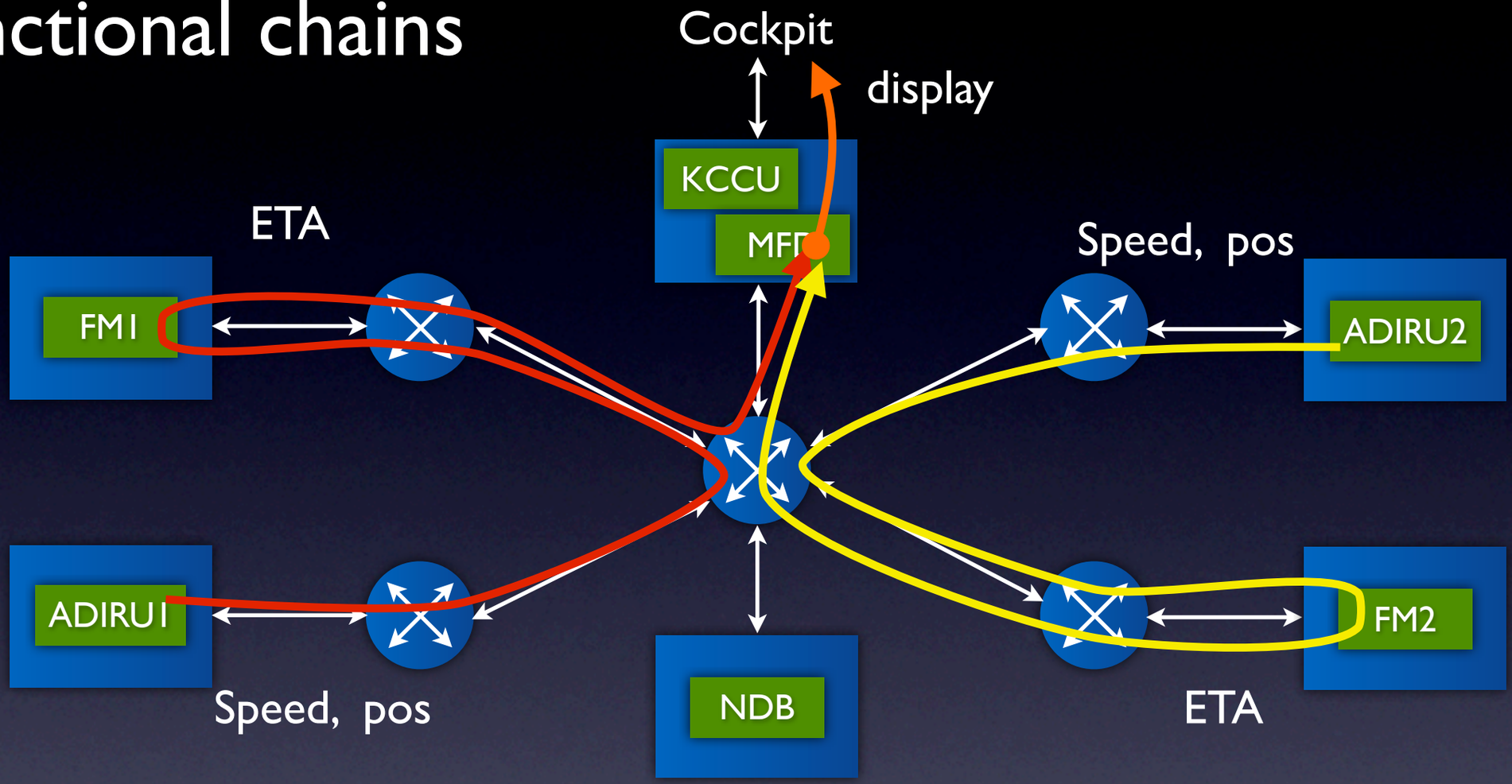
ONERA
THE FRENCH AEROSPACE LAB

IRIT
CNRS - INPT - UPS - UT1 - UTM

Université de Toulouse

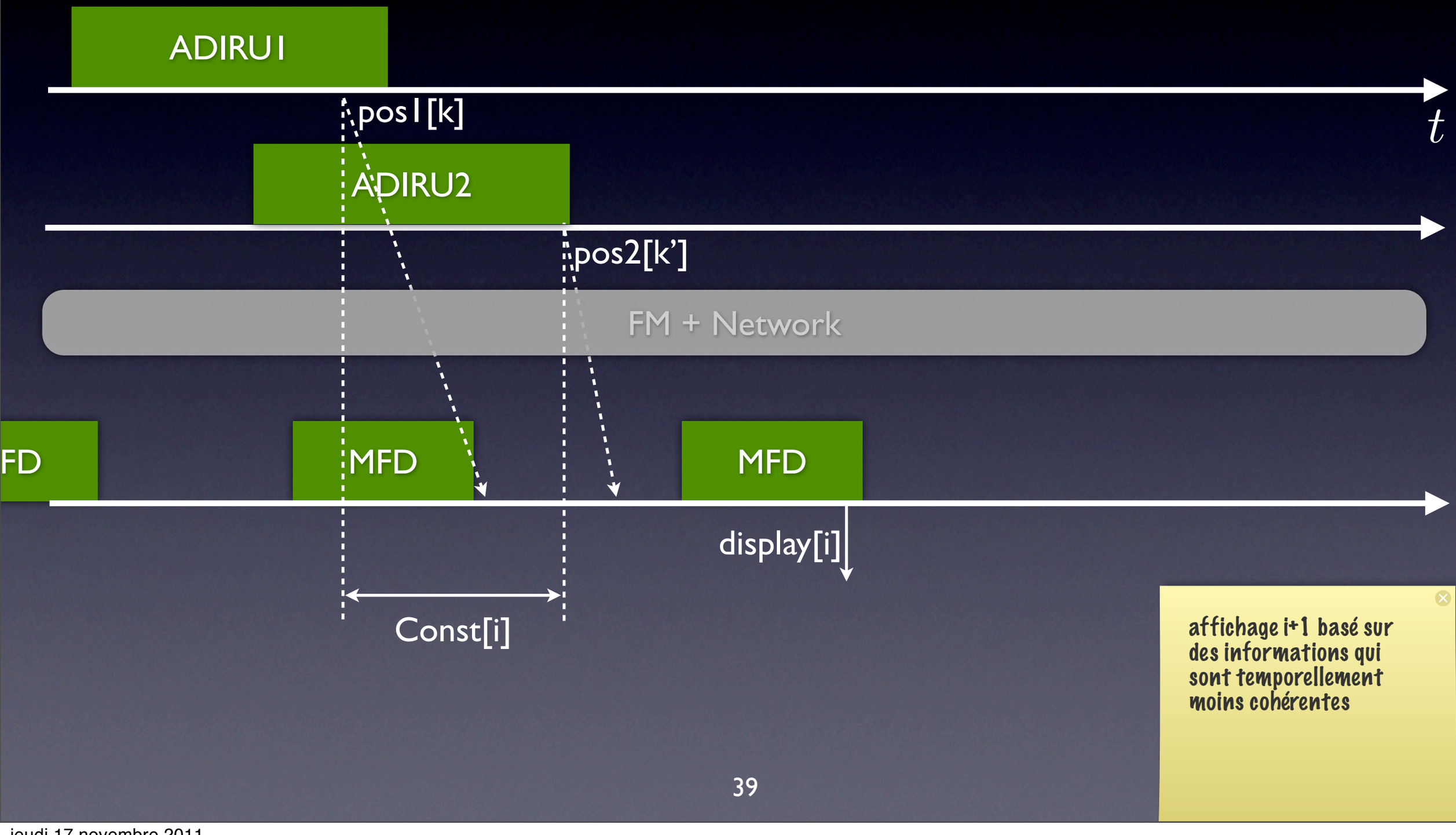
IMA platform

Functional chains



$$consistency \leq 400ms \left\{ \begin{array}{l} ADIRU1 \rightarrow FM1 \\ ADIRU2 \rightarrow FM2 \end{array} \right. \searrow \nearrow MFD \rightarrow pilot$$

Consistency



affichage i+1 basé sur des informations qui sont temporellement moins cohérentes

Consistency