Réunion S3 du 8/12/2014

MODELISATION, SIMULATION ET ANALYSE DES SYSTEMES TOLERANTS AUX FAUTES A L'AIDE DES RESEAUX D'ACTIVITES STOCHASTIQUES (SANS)

Samia MAZA
Centre de Recherche en Automatique de Nancy
UMR 7039
samia.maza@univ-lorraine.fr

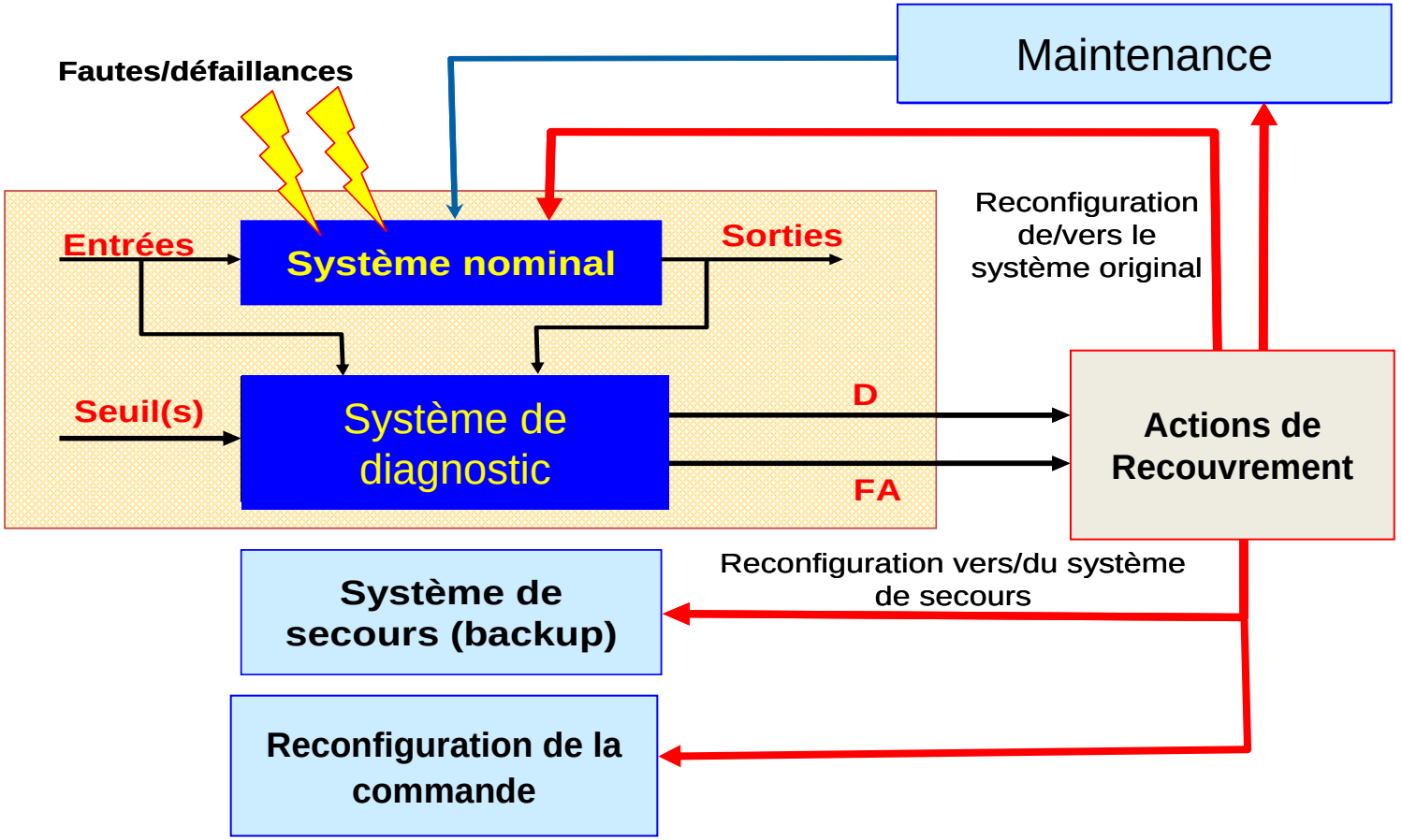
Plan de l'exposé

- Introduction: Les systèmes tolérants aux fautes.
- Les réseaux d'activités stochastiques (SANs).
- ***Partie I :*** Approche de modélisation intégrée systématique par les SANs.

  → Etude en simulation (Monte Carlo).
- ***Partie II :*** Modélisation par les SANs du diagnostic à base d'observateur de Luenberger.

  → Etude en simulation (Monte Carlo).
- Conclusion

Introduction



Ces fonctions ont un impact sur les paramètres FMDS(*) globaux

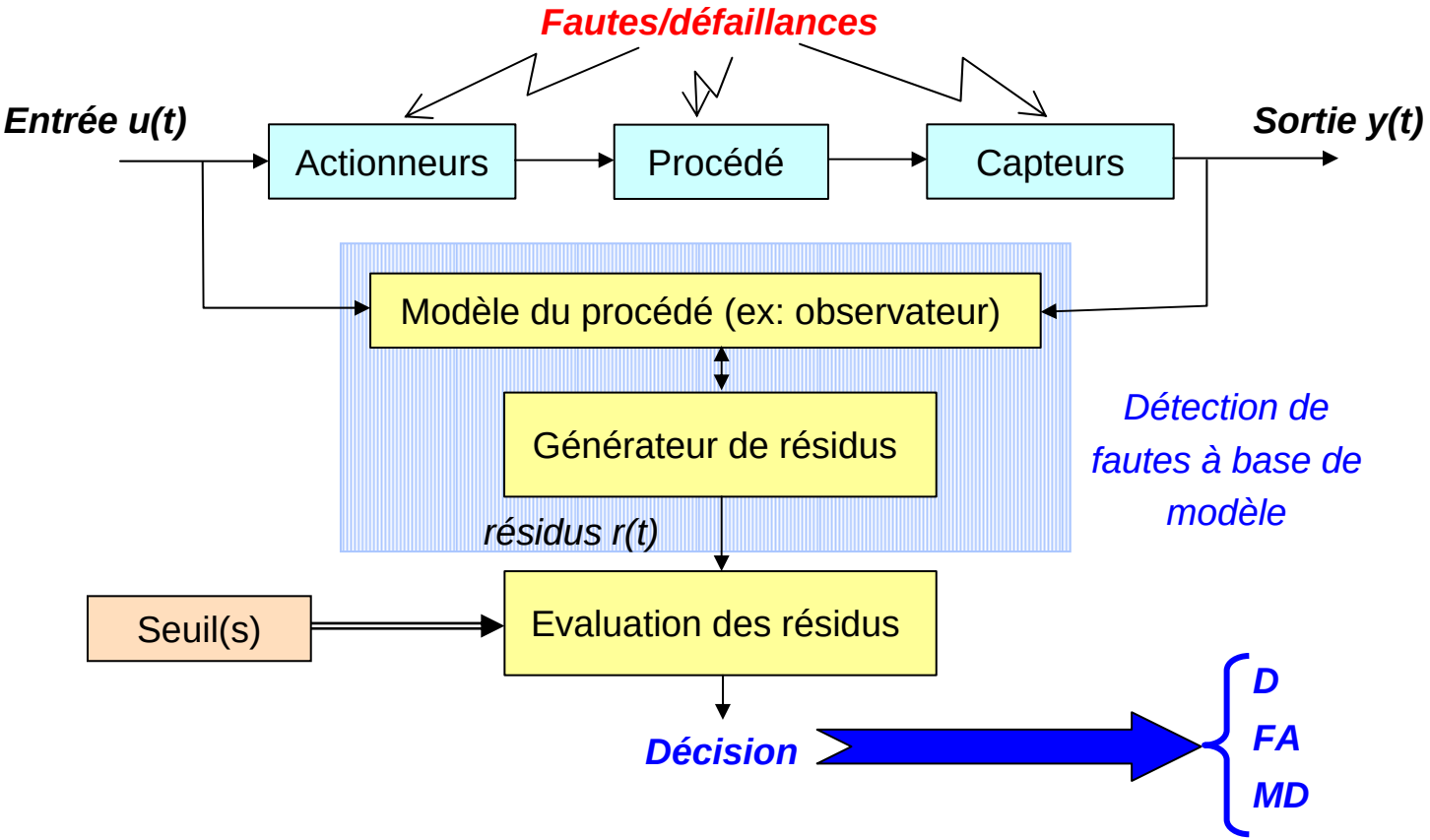
☞ Necessité de les inclure dans le modèle d'évaluation global (ex: Problème de la fiabilité dynamique)

(*) *FMDS* for: Fiabilité, Maintenability, Disponibilité, Sécurité

Introduction

☞ Les fonctions de surveillance: Le diagnostic

Il permet la détection et la localisation de défauts/défaillances du système supervisé.



Introduction

☞ Les fonctions de surveillance: Le diagnostic

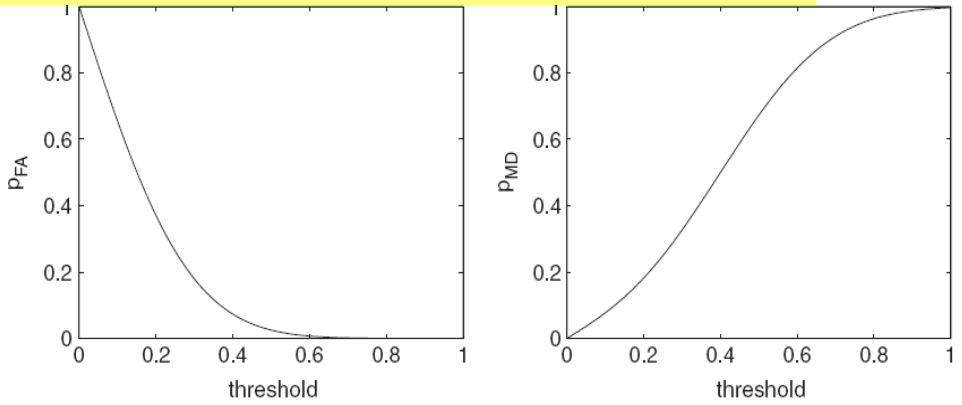
Théoriquement, si $r_i > 0$ une alarme sera produite.

En pratique, les signaux sont corrompues par des bruits ➔ les residus r_i sont alors comparés à un seuil J_i :

Si $r_i \geq J_i$ le test génère une alarme ➔ à tort : *FA*
➔ à raison : *D*

Sinon ➔ *MD*
➔ *RAS*

P(*FA*)=P(*r* ≥ *J* | le système est *Ok*)
P(*MD*)=P(*r* < *J* | le système est *Ko*) } **=>**



Les probabilités de *FA* et de *MD* en fonction du seuil

Introduction

- **Les performances du diagnostic sont souvent ignorées lors de l'évaluation des paramètres de sûreté de fonctionnement des systèmes (FMDS):** ***la détection des défaillances est souvent supposée instantanée et certaine.***

- **Les objectifs en terme de paramètres FMDS ne sont pas pris en compte dans la synthèse d'algorithmes de diagnostic.**

⇒ Il n'y a pas beaucoup d'interaction entre les études de la sûreté de fonctionnement et le diagnostic

⇒ En automatique aussi…

Les réseaux d'activités stochastiques (SANs)

Rappels sur les RdPs stochastiques

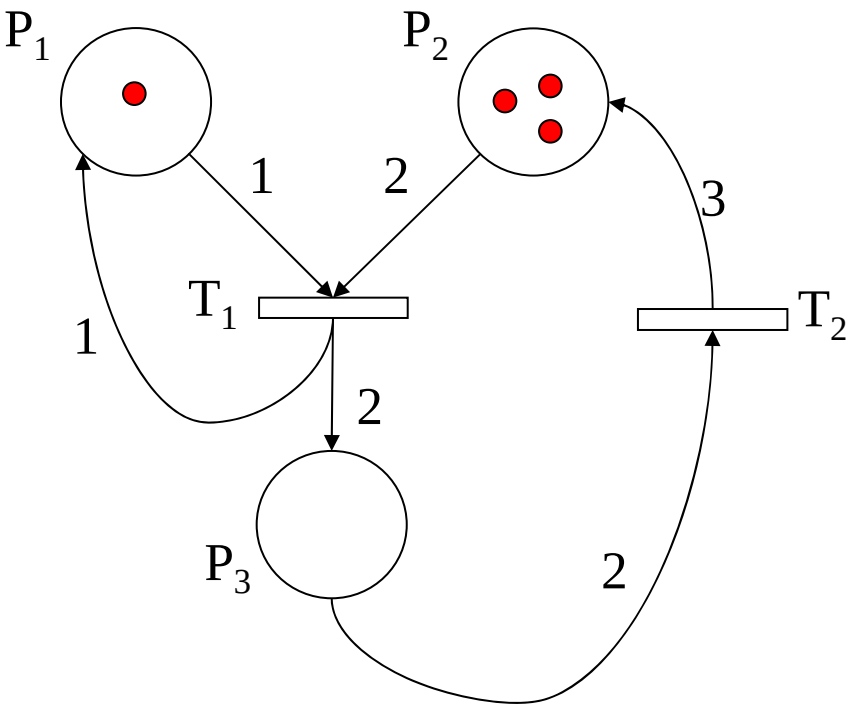
Un RdP stochastique marqué est un graphe orienté biparti défini par le sextuple

$$PN=(P,T,I,O,M_0,\Lambda)$$

- P et T sont deux ensembles distincts de sommets (désignant resp.les ensemble de places et de transitions).
- I et O sont deux applications de l'ensemble des arcs vers l'ensemble des nombres naturels, avec: $I\ (P_i, T_j)$: $PxT \rightarrow \mathcal{N}$ and $O\ (T_i, P_j)$: $TxP \rightarrow \mathcal{N}$.
- M_0 est le vecteur de marquage initial ($M_0=(m_0(P1), m_0(P2),\ldots, m_0(Pn)^T$)
- $\Lambda=(\lambda_1, \lambda_2,\ldots\lambda_m)$ est l'ensemble des taux de tirs associés aux transitions temporisées (ayant des durées qui suivent une loi exponentielle) [Marsan, 1990]
- Les transitions peuvent être immédiates avec des probabilités de tir en cas de conflit structurel.

Les réseaux d'activités stochastiques (SANs)

Rappels sur les RdPs



Exemple d'un RdPG

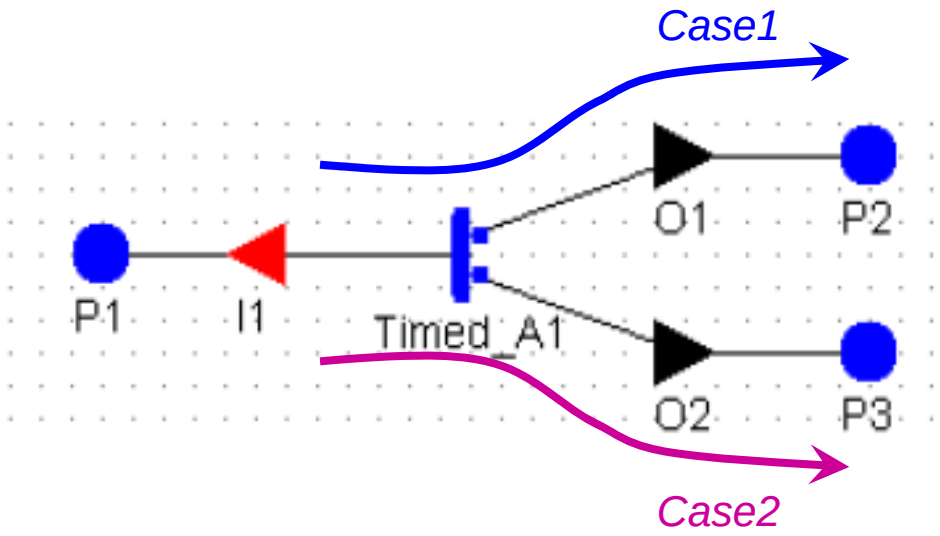
Les réseaux d'activités stochastiques (SANs)

Définition informelle des SANs Extension stochastique aux RdPs classiques avec les primitives suivantes :

- Places: elles sont de deux types: ordinaires (RdPs) ou étendues (~colorées).

- Activités: c'est l'équivalent des transitions. Elles sont de 2 types; immédiates ou temporisées.

Chaque activité a un nombre entier non nul de ***Cas de probabilités***.



Les réseaux d'activités stochastiques (SANs)

Définition informelle des SANs

- Portes d'entrée (*input gates*): chaque porte possède un nombre fini de places en entrée et une seule activité en sortie → une fonction de prédicat et une fonction d'entrée.

- Portes de sortie (*output gates*): chaque porte possède un nombre fini de places de sortie et une seule activité en entrée → une fonction de sortie est associée à chaque porte.

Quelques explications…

☞ Une porte d'entrée: (1) placée juste avant une activité permet de :

- Gérer les conditions d'activation de celle-ci (*prédicat*);
- Gérer les marquages de ses places d'entrée (*fonction d'entrée*).

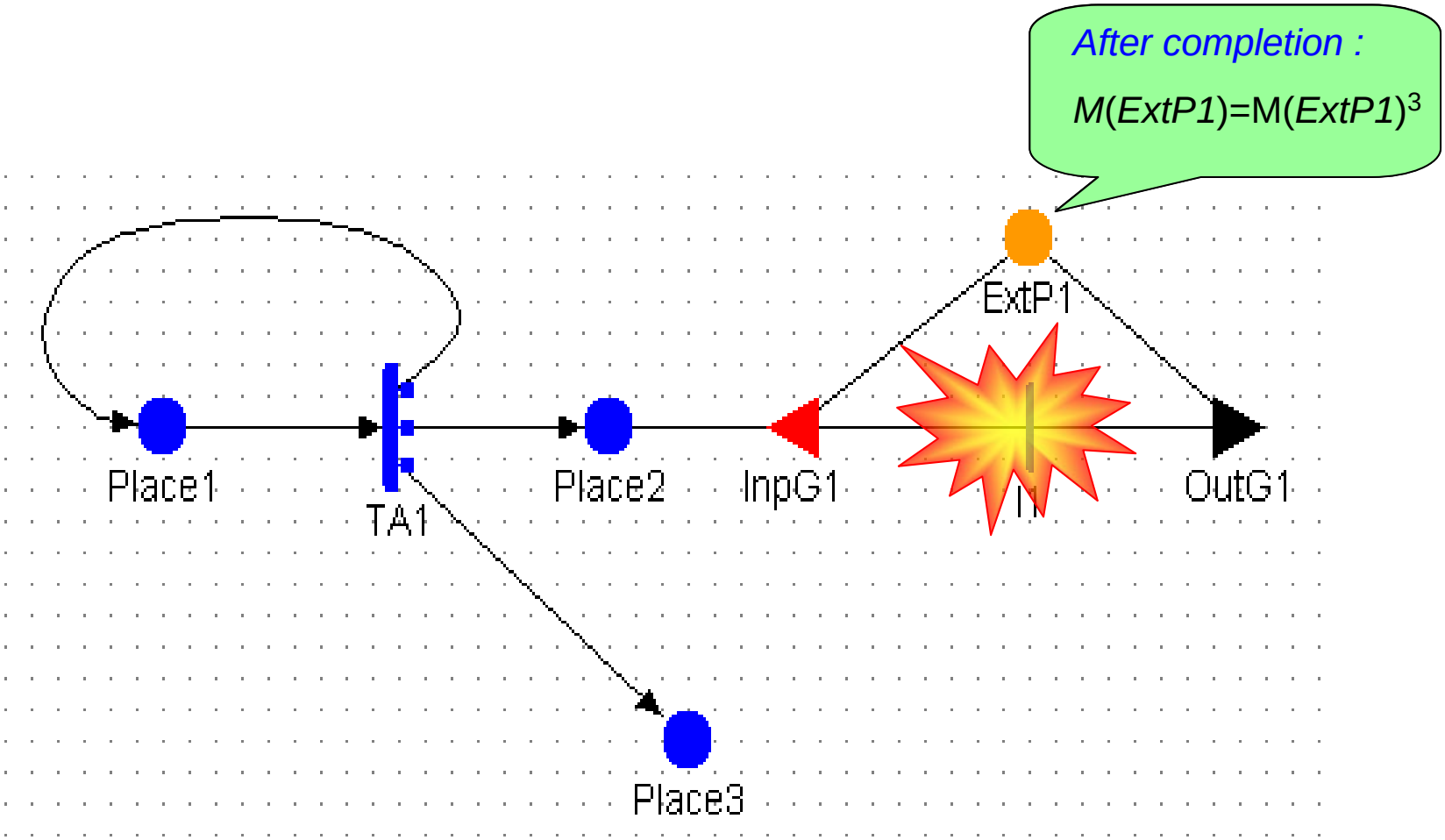
(2) Connectée à une place étendue: elle permet de lire et de modifier son marquage (un réel, un vecteur, une structure mixte de données,…)

☞ Une porte de sortie: (1) placée juste après une activité permet de gérer les marquages de ses places de sortie (*fonction de sortie*).

(2) Connectée à une place étendue: elle permet de modifier son marquage (comme la porte d'entrée)

Les réseaux d'activités stochastiques (SANs)

Définition informelle des SANs



Modélisation des systèmes tolérants aux fautes par les SANs

Partie I

→ Approche de modélisation/analyse intégrée par les SANs incluant les performances du diagnostic (P_D, P_{MD} et P_{FA}) + Quelques procédures de recouvrement.

→ Simulations de *Monte Carlo* pour l'évaluation des performances fiabilistes.

Modélisation des systèmes tolérants aux fautes par les SANs

Résumé de l'approche d'analyse et de modélisation globale [1]

- *Analyse fonctionnelle*: décomposition fonctionnelle par la méthode *SADT* par exemple.
- *Analyse dysfonctionnelle*: établir le lien entre la panne du système global et celle de ses constituants.
- Inclusion des éléments clés comme le diagnostic
- Modélisation systématique par les SANs selon l'approche qui suit
- Simulation *Monte Carlo* et analyse des résultats

[1] S.Maza, *Journal of Risk and Reliability*, vol. 226, pp. 455-463, 2012.

Modélisation des systèmes tolérants aux fautes par les SANs

(1) Modélisation dynamique des composants physiques: chaque composant '*j* ' est représenté par une paire (*Cj_Ok*, *Cj_Ko*), où:

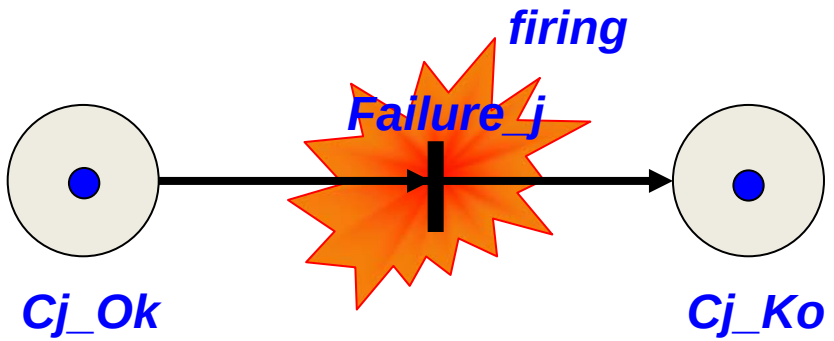
- 1 Jeton en *Cj_Ok* signifie que le composant '*j* ' est *Ok*

- 1 Jeton en *Cj_Ko* signifie que le composant '*j* ' n'est pas *Ok*.

- et une activité temporisée *Failure_j* dont la temporisation suit une loi probabiliste (ex. exponentielle).

$$M(C_j^{Ok}) + M(C_j^{Ko}) \leq 1$$

$$M_0(C_j^{Ok}) = 1 \; et \; M_0(C_j^{Ko}) = 0$$



Modélisation des systèmes tolérants aux fautes par les SANs

(2) Modélisation du composant/système de secours: comme un composant physique par une paire de places $(P^{Ok}_{Secours}, P^{Ko}_{Secours})$ seulement le marquage initial dépendra de politique de redondance employée:

$M_0(P^{Ok}_{Secours}) = 1$ Pour la redondance active

$M_0(P^{Ok}_{Secours}) = 0$ Pour la redondance passive

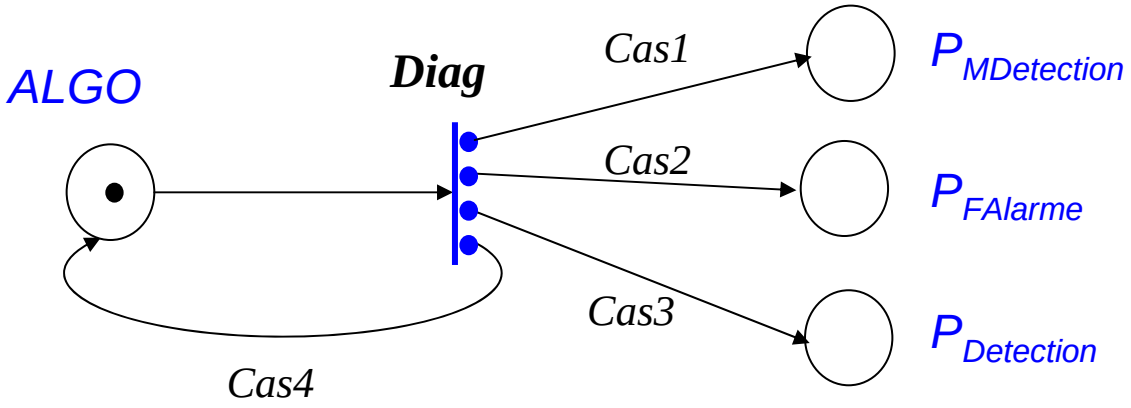
(3) Modélisation du système de diagnostic: Il peut être vu comme générateur de trois évènements mutuellement exclusifs: *D*, *MD*, *FA.*

Il est nécessaire de connaître les performances de diagnostic en termes de probabilités P_D, P_{MD} et P_{FA}.

$$alarm = (FA \wedge \overline{super\_component}) \vee (D \wedge super\_component)$$

Modélisation des systèmes tolérants aux fautes par les SANs

(3) Modélisation du système de diagnostic: trois places modéliseront ces évènements + activité temporisée (*Diag*)



$$P(Cas1) = \begin{cases} P_{MD} & si \quad M(C_k^{Ko}) = 1 \\ 0 & sinon \end{cases}$$

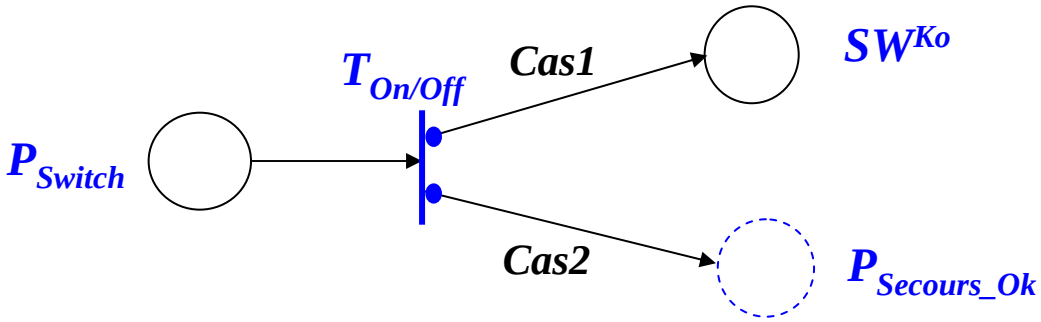
$$P(Cas\ 2) = \begin{cases} P_{FA} & si \quad M(C_k^{Ok}) = 1 \\ 0 & sinon \end{cases}$$

$$P(Cas\ 3) = \begin{cases} P_{D} & si \quad M(C_k^{Ko}) = 1 \\ 0 & sinon \end{cases}$$

$$P(Cas4) = \begin{cases} 1 - P_{MD} - P_D & si \quad M(C_k^{Ko}) = 1 \\ 1 - P_{FA} & sinon \end{cases}$$

Modélisation des systèmes tolérants aux fautes par les SANs

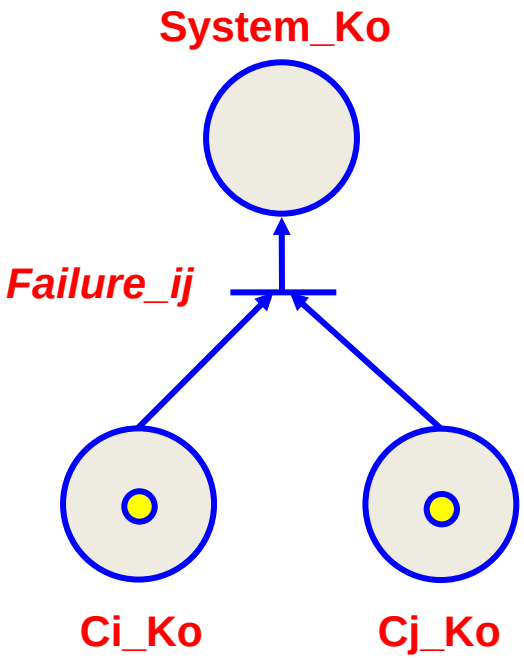
(4) Modélisation du Switch: Il assure la commutation de la partie fautive du système vers la partie opérationnelle redondante à la première.



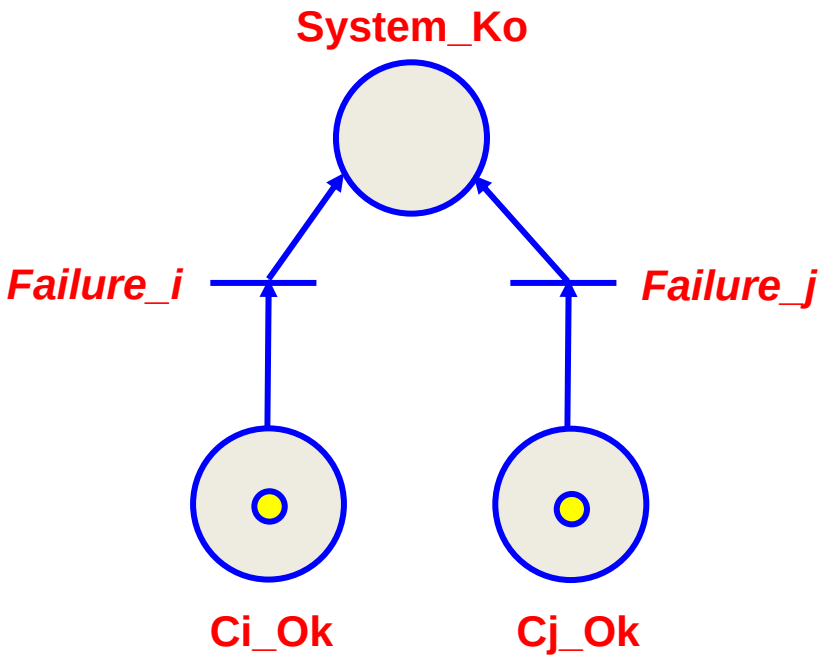
$M_0(P_{Switch}) = 0$ Marquage si le système de diagnostic génère une alarme

Modélisation des systèmes tolérants aux fautes par les SANs

(5) Modélisation globale: les places et activités de ces différents modules seront reliés les uns aux autres selon une certaine logique (type ET / OU)



AND operator

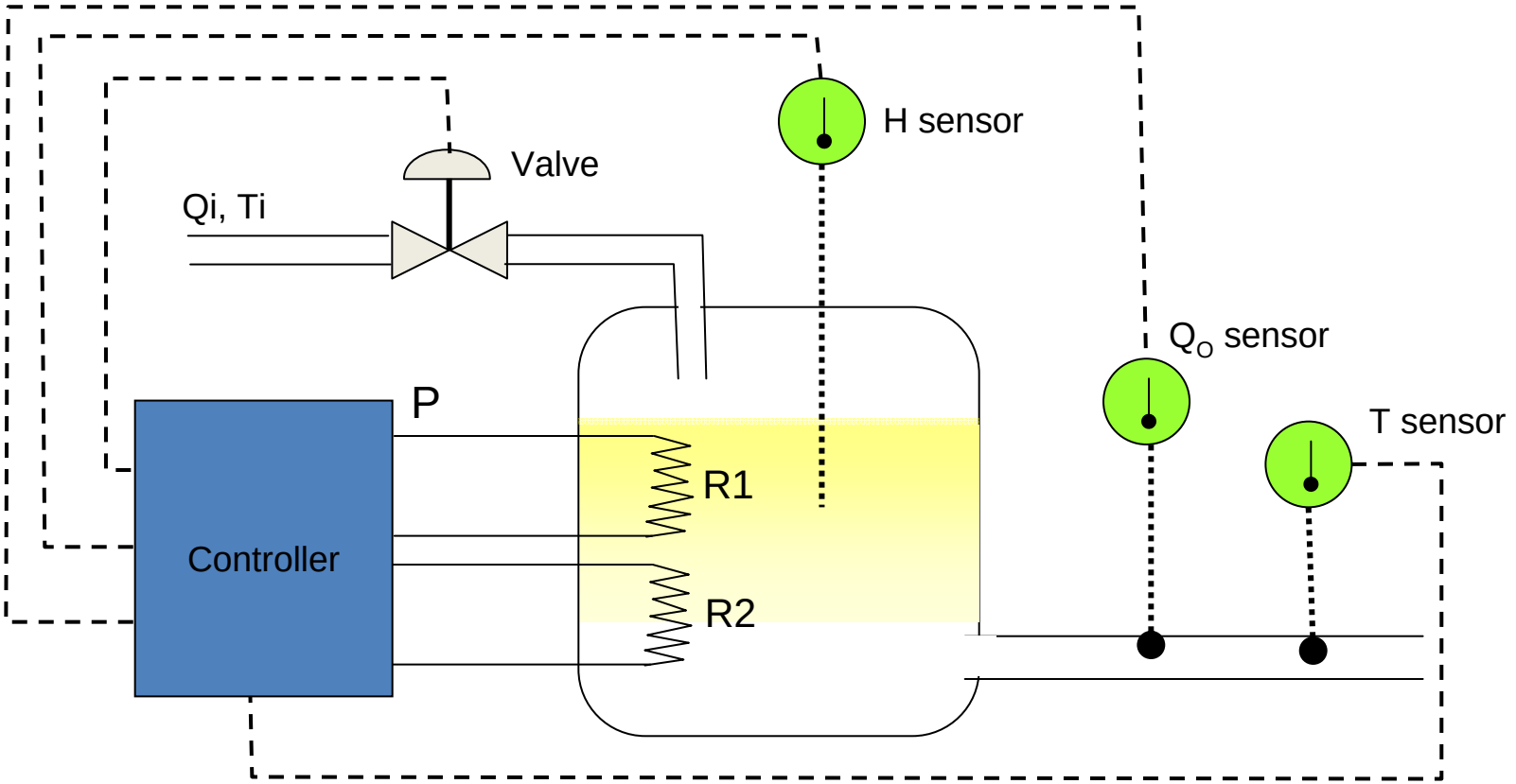


OR operator

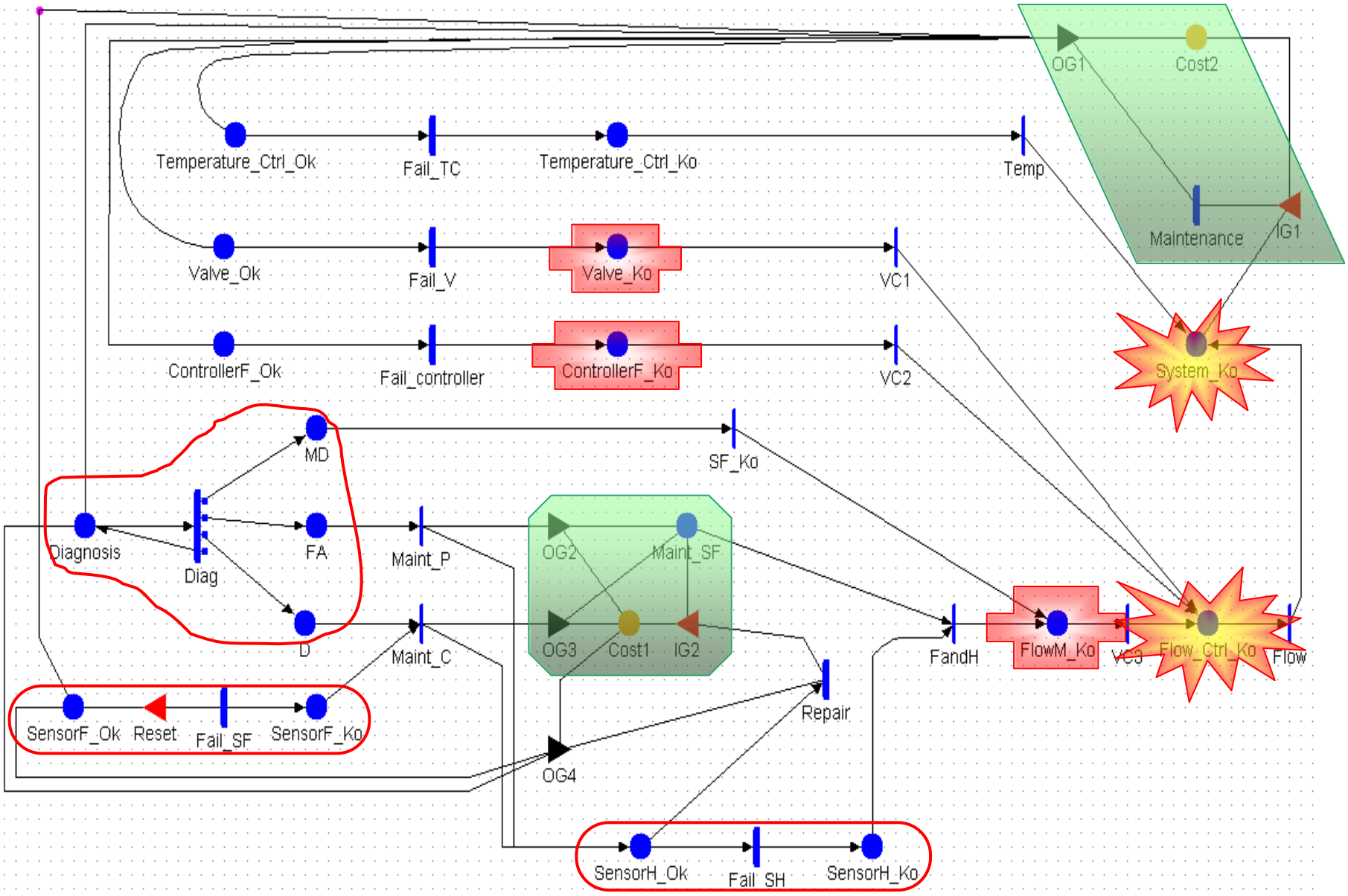
Etude de cas

Le système : Système automatisé de régulation de température et de débit

(le capteur de hauteur est en redondance avec celui du débit)



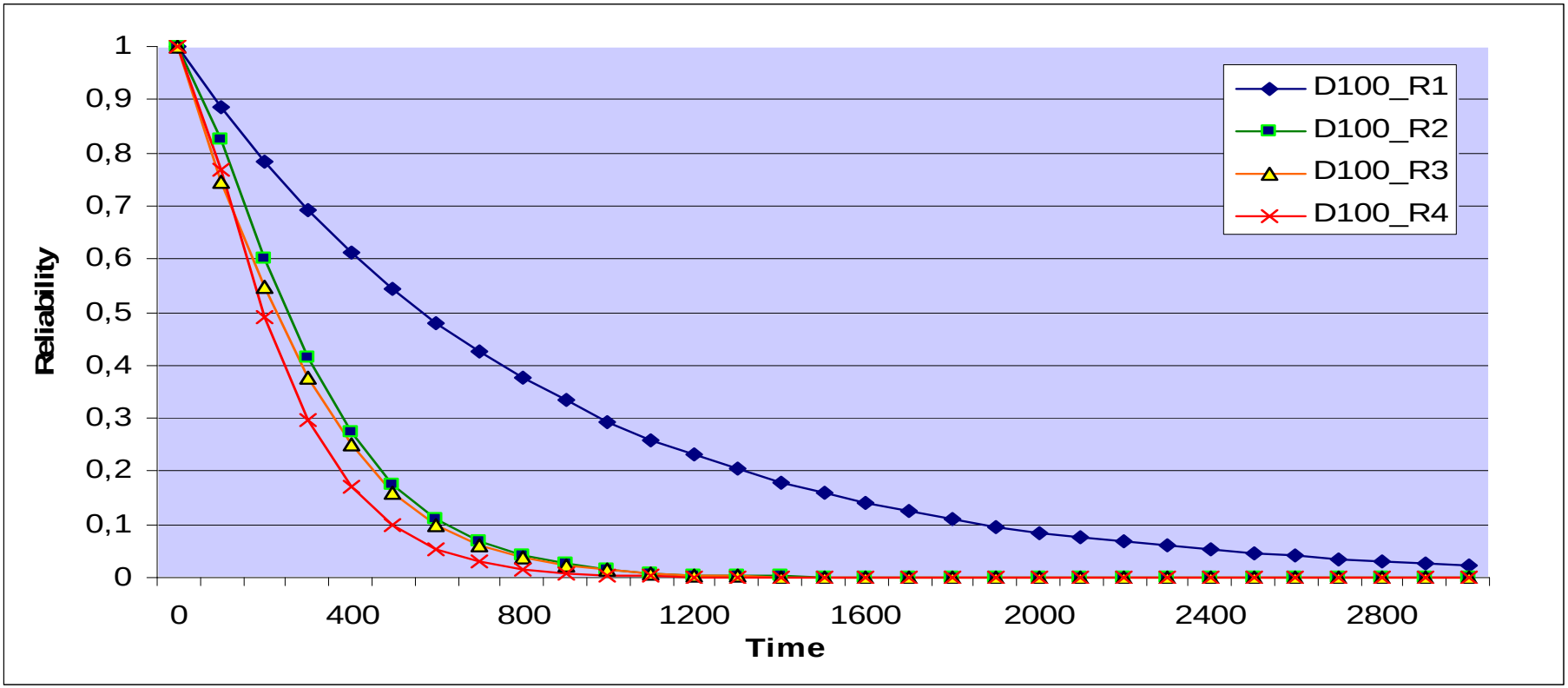
Etude de cas


OG1
Cost2
Temperature_Ctrl_Ok
Fail_TC
Temperature_Ctrl_Ko
Temp
Maintenance
IG1
Valve_Ok
Fail_V
Valve_Ko
VC1
ControllerF_Ok
Fail_controller
ControllerF_Ko
VC2
System_Ko
MD
SF_Ko
Diagnosis
Diag
FA
D
Maint_P
Maint_C
OG2
Maint_SF
OG3
Cost1
IG2
OG4
FandH
FlowM_Ko
VC3
Flow_Ctrl_Ko
Flow
Repair
SensorF_Ok
Reset
Fail_SF
SensorF_Ko
SensorH_Ok
Fail_SH
SensorH_Ko

Etude de cas

Résultats de simulation [3] Evaluation de la fiabilité

R1=Maint&RedPass, *R2*=SansMaint&RedPass, *R3*=Maint&RedAct, *R4*=SansMaint&RedAct



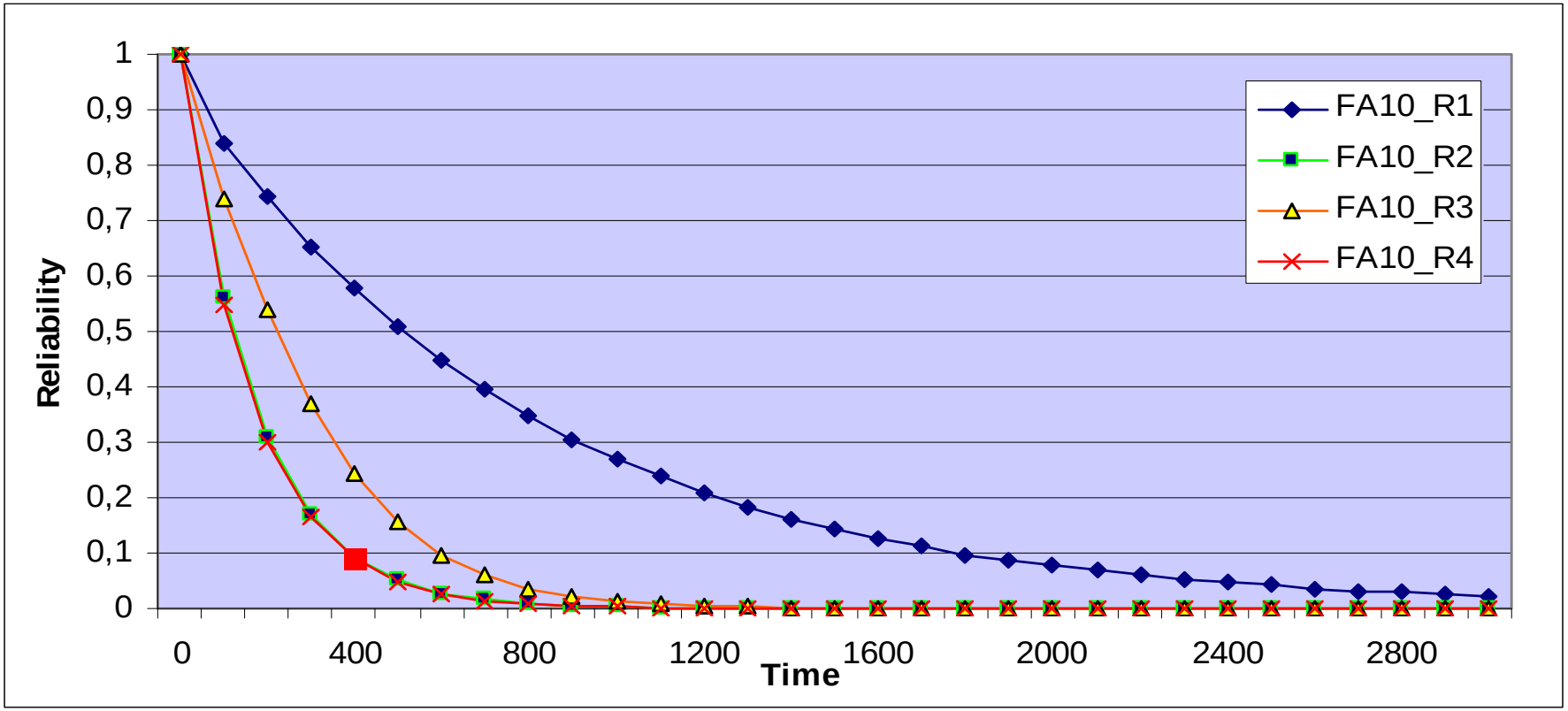
The time evolution of the FT-system reliability when the fault detection is made with certainty (P_D=100%) for the models *Rk*, *k*=1,4.

[3] S.Maza, *Journal of Risk and Reliability*, vol. 228(3), pp. 243-253, 2014.

Etude de cas

Résultats de simulation [3] Evaluation de la fiabilité

R1=Maint&RedPass, *R2*=SansMaint&RedPass, *R3*=Maint&RedAct, *R4*=SansMaint&RedAct

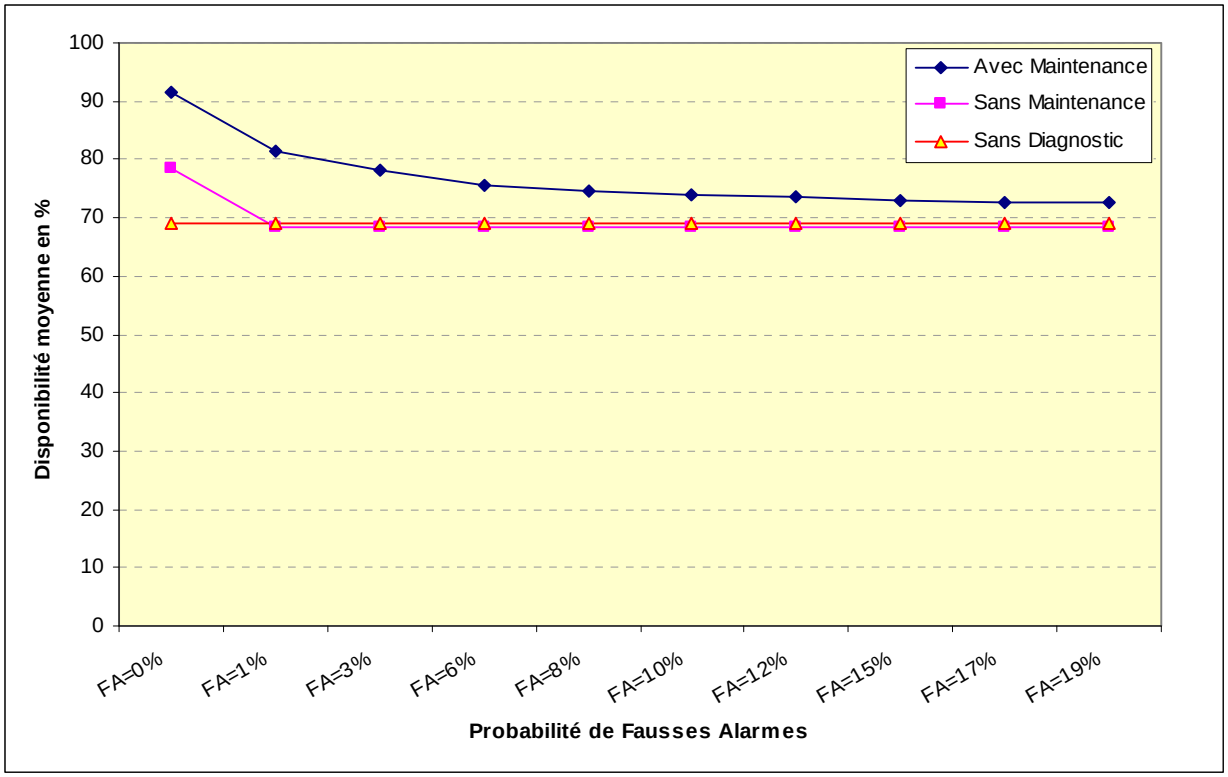


The time evolution of the FT-system reliability when the fault detection is made with certainty (P_D=80% and P_{FA}=10%) for the models *Rk*, *k*=1,4.

Etude de cas

Résultats de simulation [2] Evaluation de la disponibilité

Cas 1 : les capteurs en redondance ont la même fiabilité ($\lambda_{SensorF}=\lambda_{SensorH}=5.10^{-4}$)

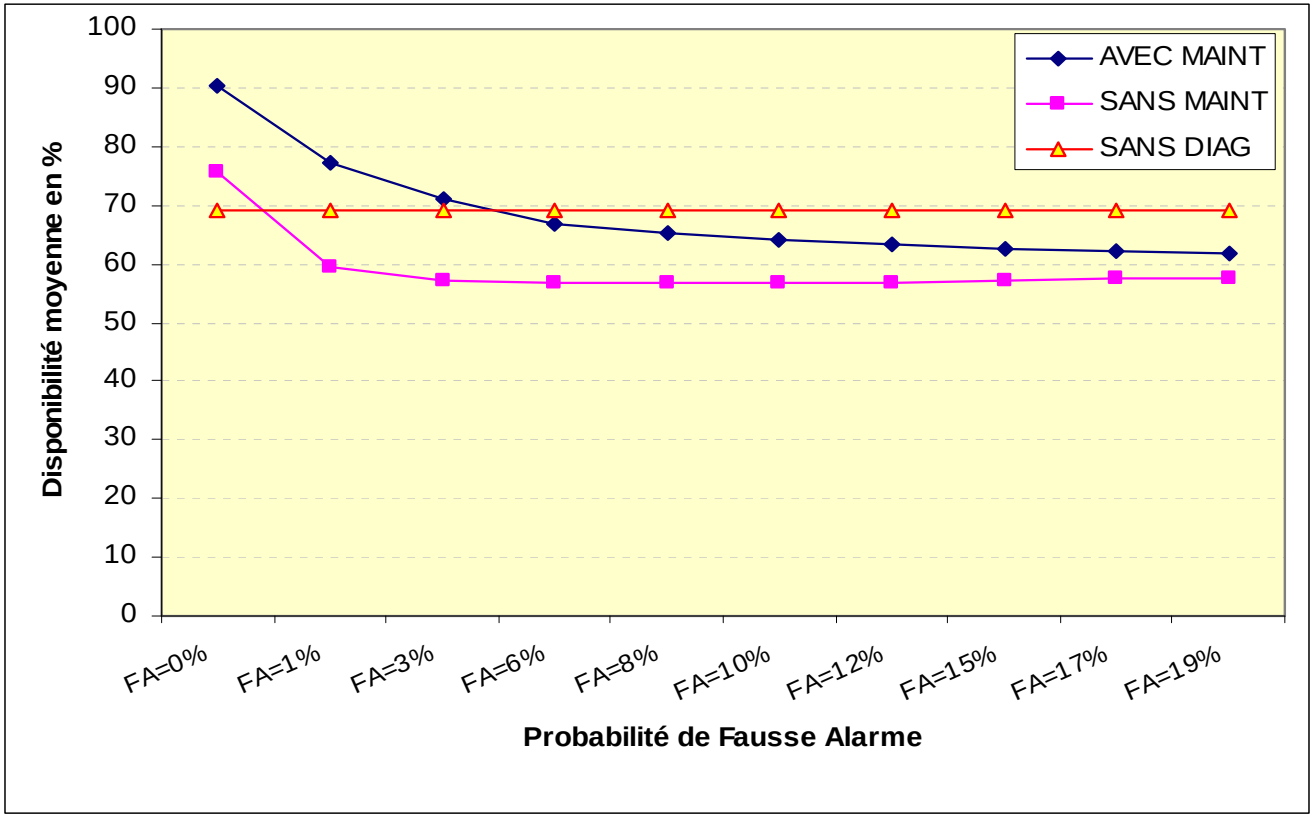


[2] S.Maza, Congrès *Lambda Mu*, Tours, 2013.

Etude de cas

Résultats de simulation [2] Evaluation de la disponibilité

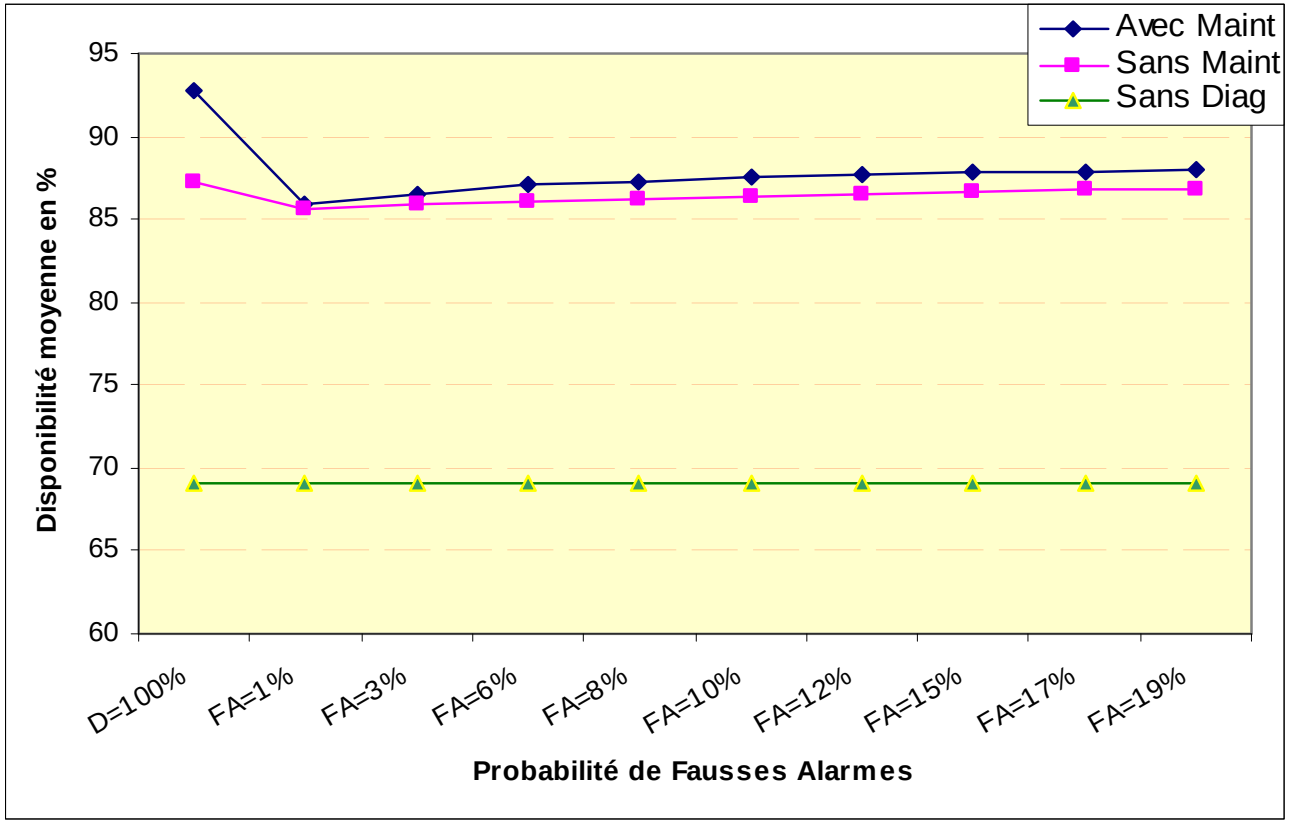
Cas 2 : le capteur principal est plus fiable que son backup ($\lambda_{SensorF}=5.10^{-4}$, $\lambda_{SensorH}=9.10^{-3}$)



Etude de cas

Résultats de simulation [2] Evaluation de la disponibilité

Cas 3 : le capteur principal est moins fiable que son backup ($\lambda_{SensorF}=5.10^{-3}$, $\lambda_{SensorH}=1.10^{-3}$)



Conclusion sur la Partie I

- **Approche de modélisation intégrée, systémique et systématique, incluant explicitement les performances du diagnostic**

- **Complexité algorithmique polynomiale** (nombre de places/activités proportionnel au nombre de composants/fonctions) → *Un gros avantage par rapport aux outils comme les automates par ex*.

- **Résultats de l'étude de l'impact du diagnostic et des politiques de redondances et de maintenance sur les performances globales → Motive l'utilisation d'approches d'analyse et de modélisation intégrée pour l'évaluation des paramètres de sûreté de fonctionnement**

☝ **Connaissance à priori des probabilités de *D*, *FA* et *MD***

Partie II: Modélisation complète de la procédure de diagnostic par observateur de *Luenberger*(*)

Objectifs:

- Modéliser le système de diagnostic, à base d'observateur de *Luemberger*, de façon explicite et détaillée;

- Simulations *Monte Carlo* pour étudier directement l'impact des paramètres de synthèse du superviseur (*Ex*: le seuil de détection) sur les paramètres *FMDS* du système tolérant au fautes.

☞ Être indépendants des valeurs de P_D, P_{FA} et P_{MD} qui sont souvent pas connus.

(*) Publié en ligne dans *International Journal of Quality and Reliability Engineering, juin 2014*

Partie II: Modélisation complète de la procédure de diagnostic par observateur de *Luenberger*(*)

Principe :

(1) Le modèle d'état discrétisé du système nominal :

$$\begin{cases} x_{k+1} = A_d x_k + B_d u_k & (a) \\ y_k = C_d x_k & (b) \end{cases} \Longrightarrow y_k = C_d x_k + F_d \upsilon_k + G_d \xi_k$$

υ_k is a r
noise m
as a ga

ξ_k models the sensor's fault effect (3 types: biais, derivative, oscillatory)

(2) Le modèle discrétisé de son observateur :

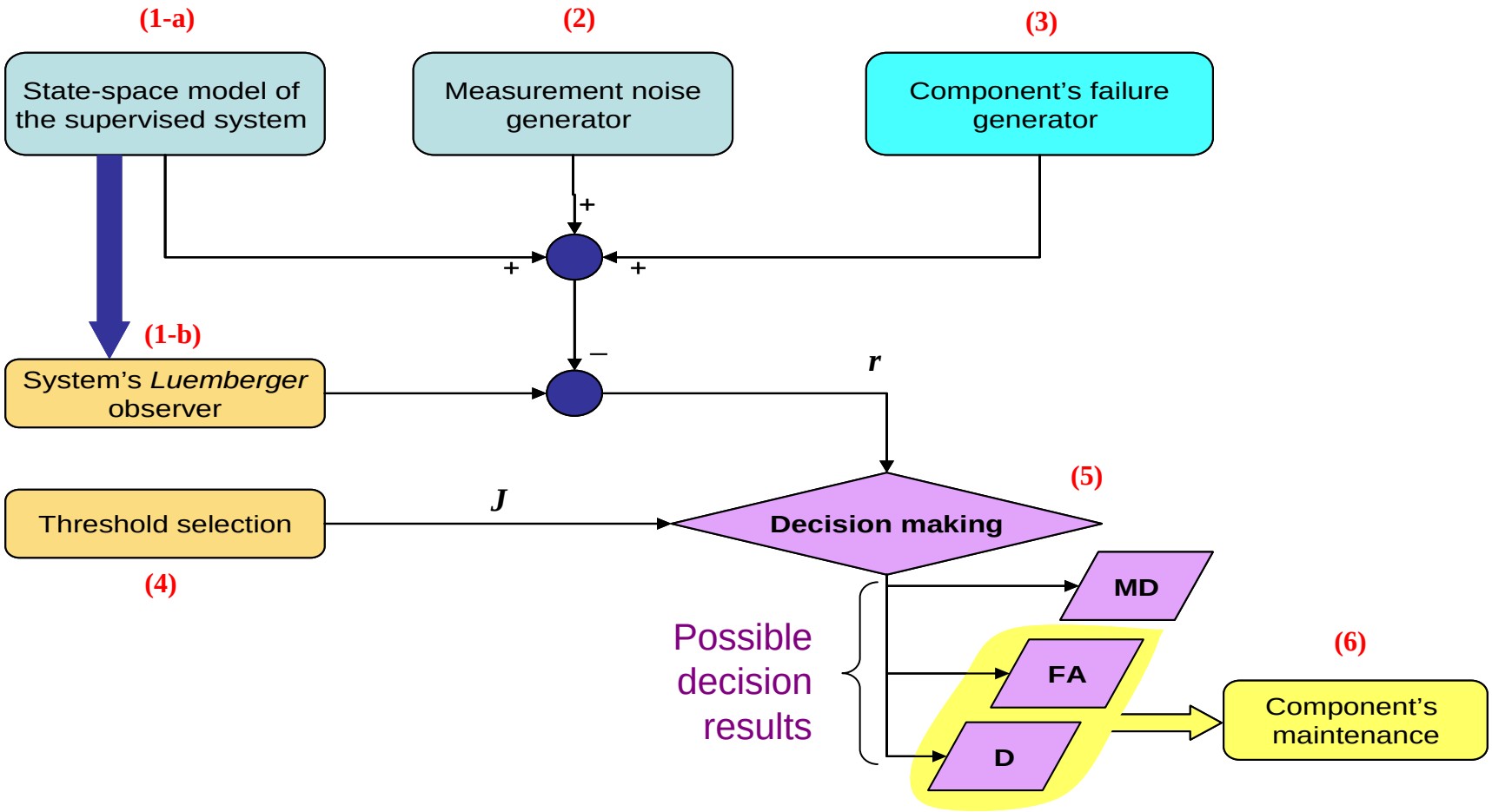
$$\begin{cases} \hat{x}_{k+1} = A_d \hat{x}_k + B_d u_k + L(y_k - \hat{y}_k) & (a) \\ \hat{y}_k = C_d \hat{x}_k & (b) \end{cases}$$

(3) Les résidus :

$$r_{i,k} = y_{i,k} - \hat{y}_{i,k}$$

Où *i* est la composante du vecteur considéré

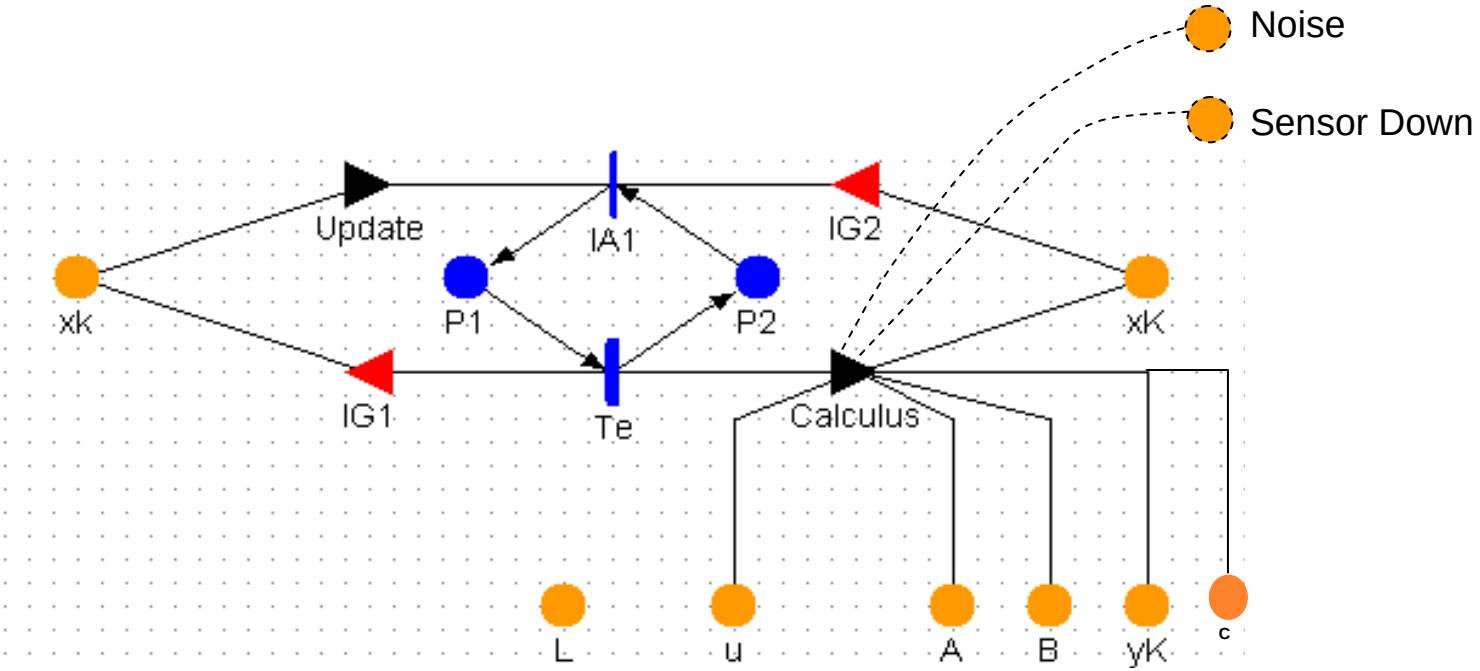
Partie II: Modélisation complète de la procédure de diagnostic par observateur de *Luenberger*(*)



A general scheme for the development of the observer-based diagnosis SAN-model

Partie II: Modélisation complète de la procédure de diagnostic par observateur de *Luenberger*(*)

Modèle SAN du système nominal

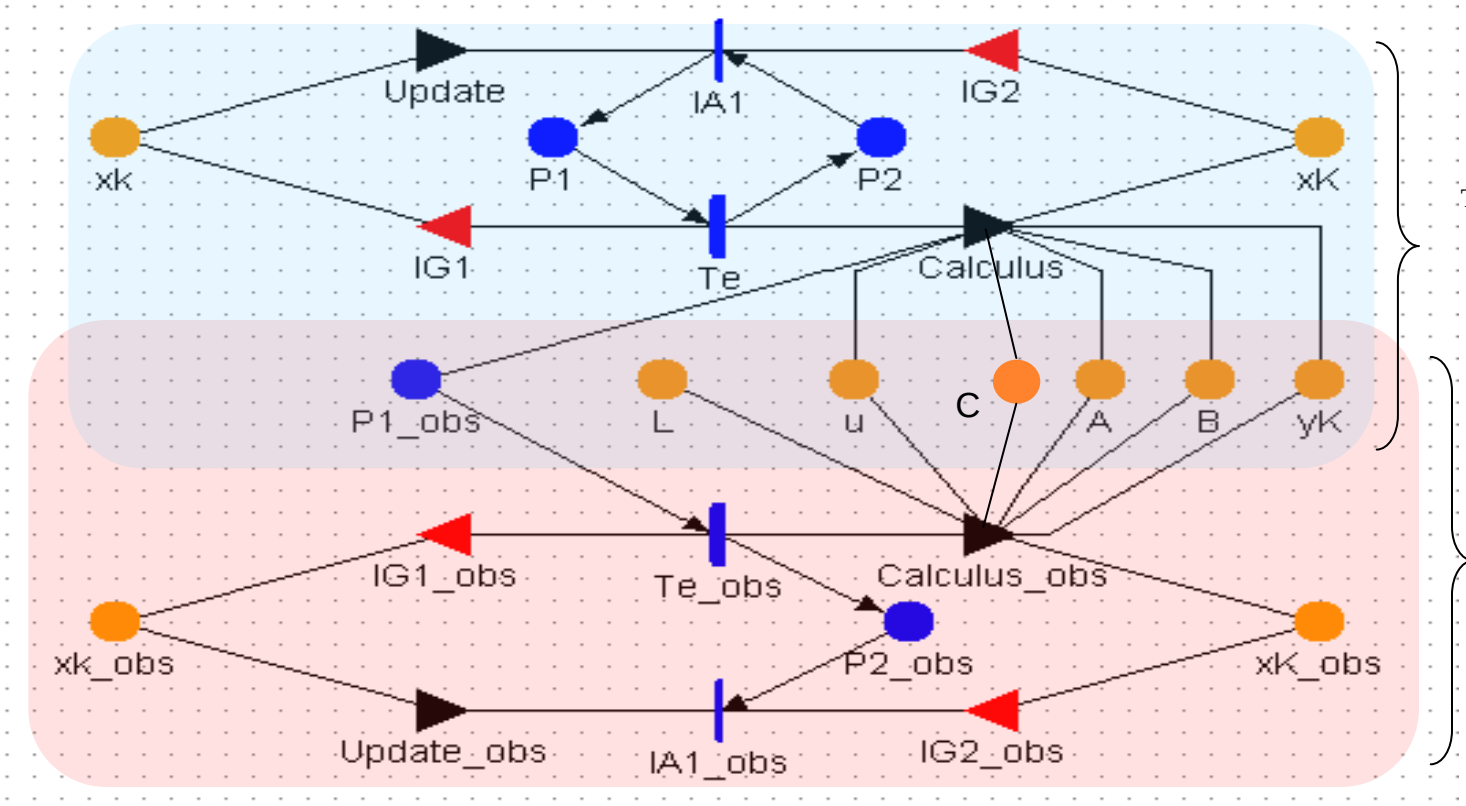


The SAN modelling of the system's state space equations.

Avec : M(*P1*)+M(*P2*)=1

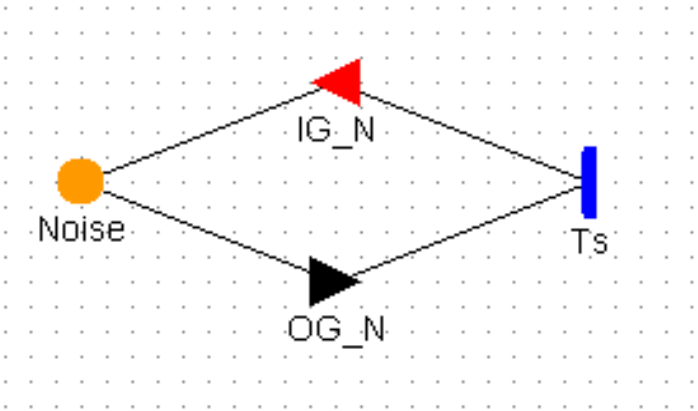
Partie II: Modélisation complète de la procédure de diagnostic par observateur de *Luenberger*(*)

Modèle SAN du système nominal & son observateur

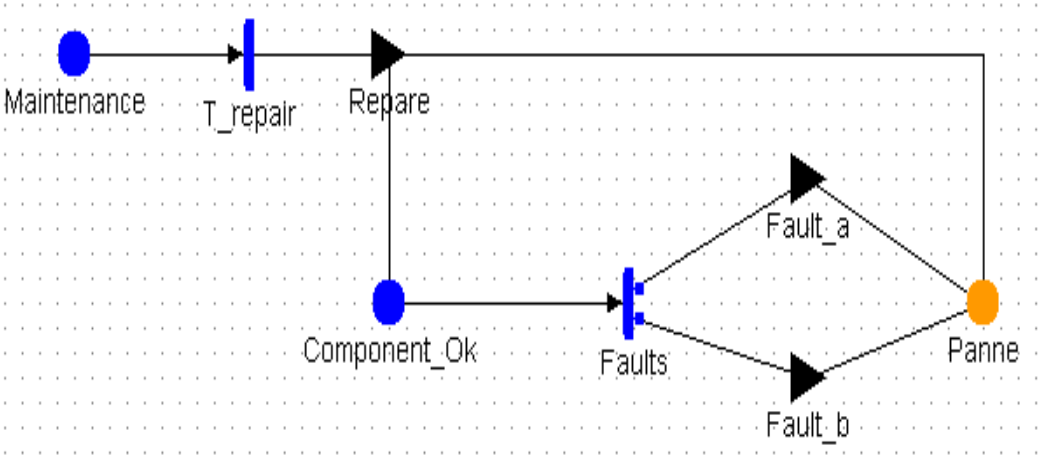


Partie II: Modélisation complète de la procédure de diagnostic par observateur de *Luenberger*(*)

Modèle SAN du bruit et du défaut



(a) The noise model



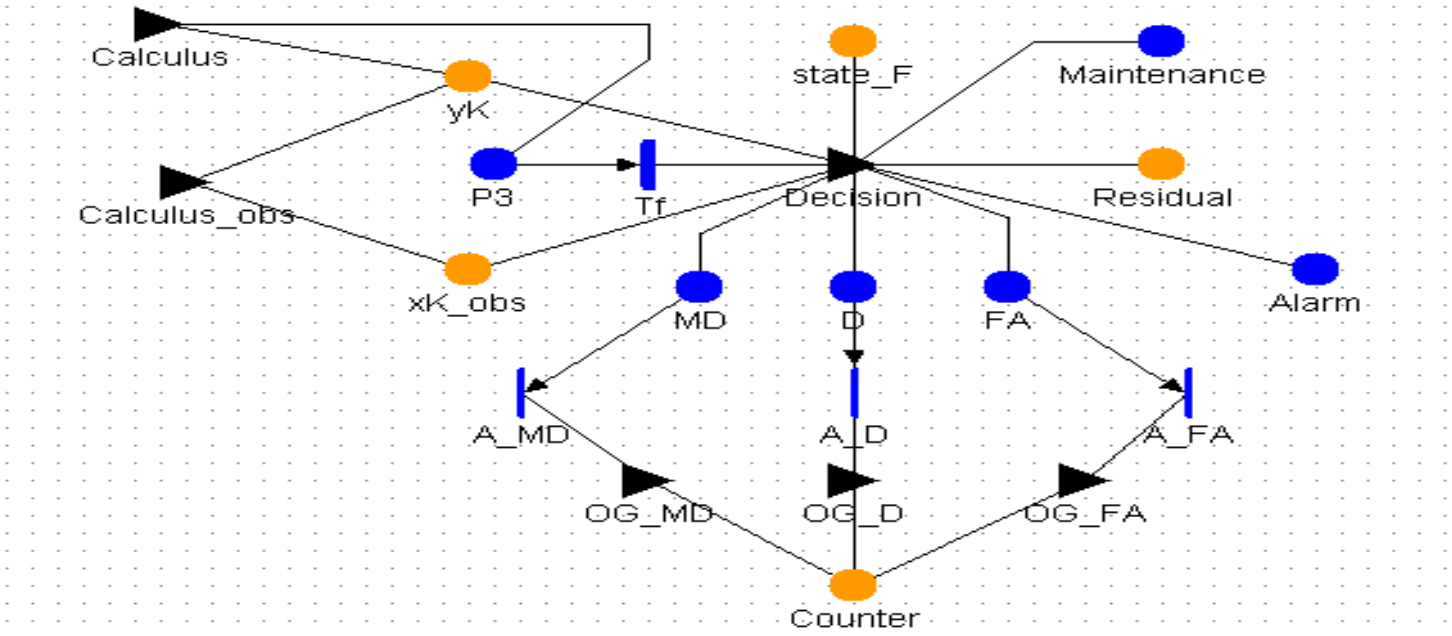
$$\xi = \begin{cases} \alpha, \text{ for } Fault\_a \\ \beta, \text{ for } Fault\_b \end{cases} \quad \text{with} \quad \alpha \gg \beta$$

(b) Component's fault model

The SAN modelling of the sensor's noise and faults

Partie II: Modélisation complète de la procédure de diagnostic par observateur de *Luenberger*(*)

Modèle SAN de la prise de décision :

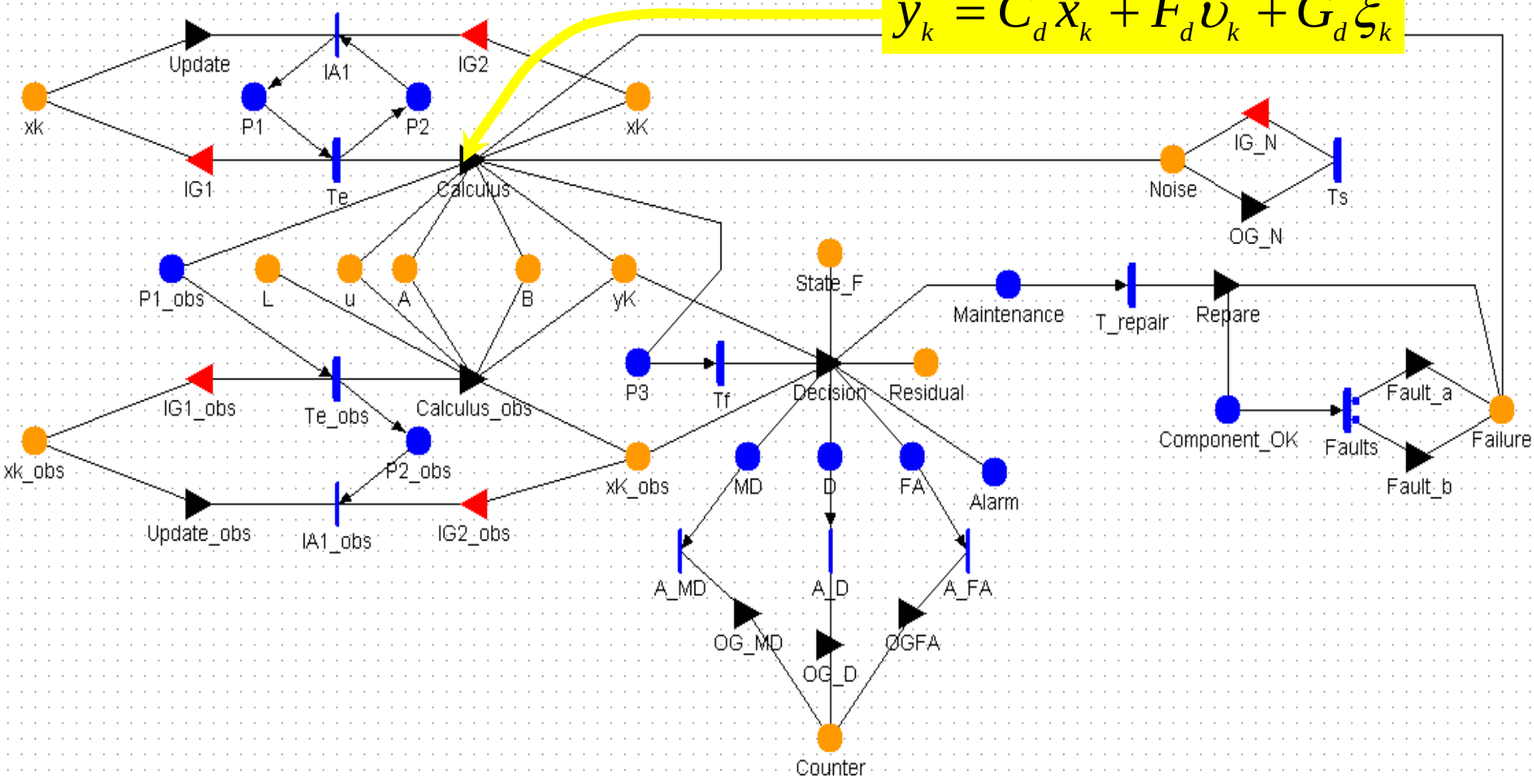


The SAN modelling of the diagnosis decision making

Partie II: Modélisation complète de la procédure de diagnostic par observateur de *Luenberger*(*)

Modèle SAN du système supervisé avec son superviseur :

$$y_k = C_d x_k + F_d \upsilon_k + G_d \xi_k$$



Partie II: Modélisation complète de la procédure de diagnostic par observateur de *Luenberger*(*)

The system's equations

$$\begin{cases} \dfrac{dh(t)}{dt} = \dfrac{1}{S}\left(Q_i(t) - s\sqrt{2gh}\right) \\ \dfrac{dT(t)}{dt} = \dfrac{1}{S.h(t)}\left(\dfrac{P(t)}{\rho C} - (T(t) - T_i) \times Q_i(t)\right) \end{cases}$$

avec

$$\begin{cases} x(t) = \begin{pmatrix} T(t) \\ h(t) \end{pmatrix} \\ y(t) = x(t) \\ u(t) = \begin{bmatrix} Q_i \\ P \end{bmatrix} \end{cases}$$

➔

$$\begin{cases} \begin{pmatrix} x_{1,k+1} \\ x_{2,k+1} \end{pmatrix} = A_d x_k + B_d u_k = \begin{pmatrix} 0.98 & 0 \\ 0 & 0.98 \end{pmatrix}\begin{pmatrix} x_{1,k} \\ x_{2,k} \end{pmatrix} + \begin{pmatrix} -50 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} u_{1,k} \\ u_{2,k} \end{pmatrix} \\ y_k = x_k + \xi_k + \upsilon_k \end{cases}$$

The supervised sensor's dependability and physical parameters

- Failure of sensor1 → a constant failure rate, λ=0.09, and follows an *exponential distribution* with parameter λ.
- Two possible fault effects with two different magnitudes: α=5 and β=0.6
- Fault1 is more likely to be detected and has a bigger probability to happen: P_α=0.8 and P_β=0.2
- Sensor noise → uniform distribution with parameters (γ1,γ2)= $(-|\Delta_{noise}|, |\Delta_{noise}|)$ avec $\Delta_{noise} = \pm 3\%.y_{ss} = 0.8$

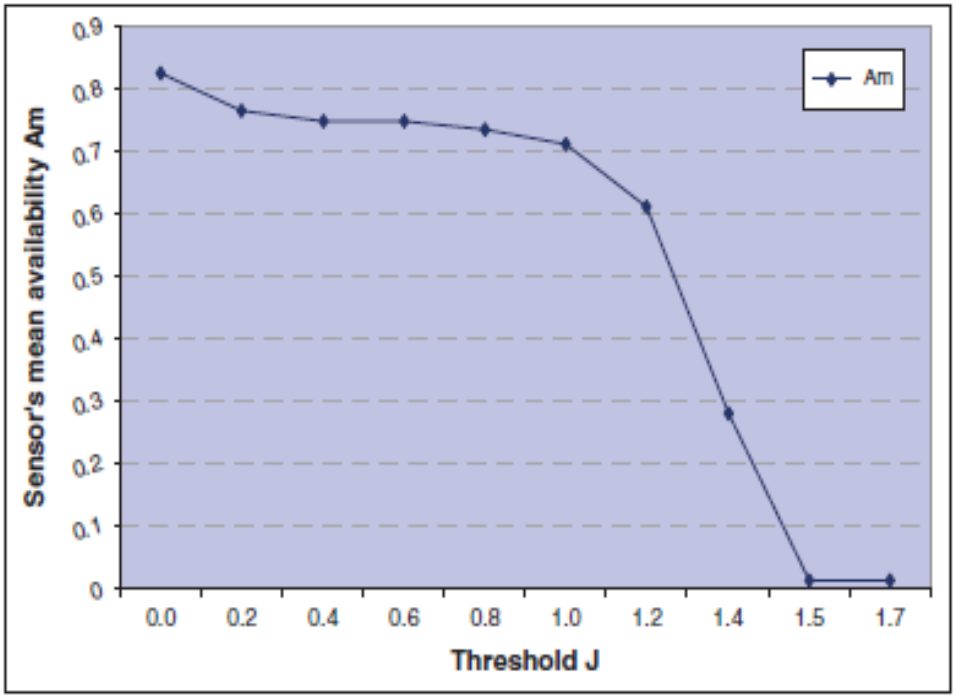
The MC simulations parameters

The number of simulated histories N_h is chosen $10^3 \leq N_h \leq 10^4$. Each history has a duration of $T_h=10^5$ *t.u.*

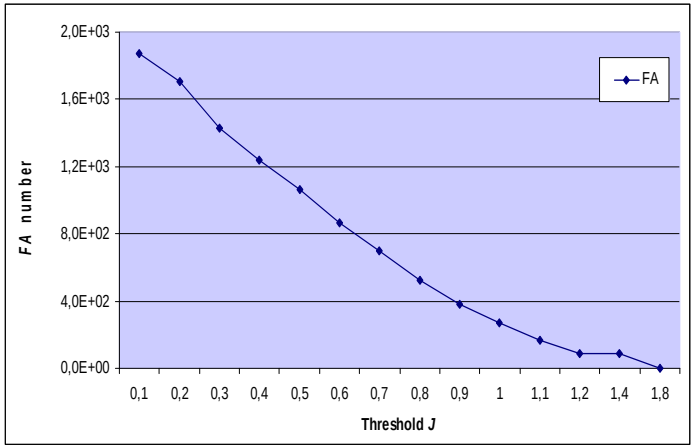
Confidence level=95% & confidence interval=10%

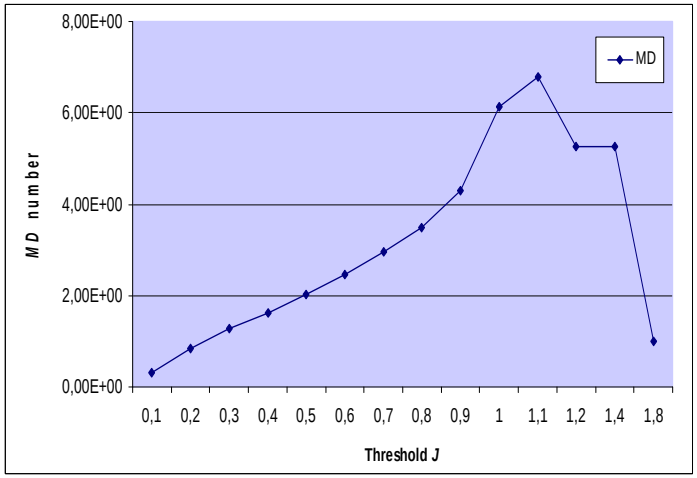
Partie II: Modélisation complète de la procédure de diagnostic par observateur de *Luenberger*(*)

Simulation results



(b) The sensor's mean availability A_m





The impact of the threshold *J* value on the diagnosis performance indicators: *FA* and *MD*.

La suite…

→ Etudier l'impact du seuil sur les paramètres FMDS du système tolérant aux fautes global (incluant donc des actions de maintenance et de reconfiguration).

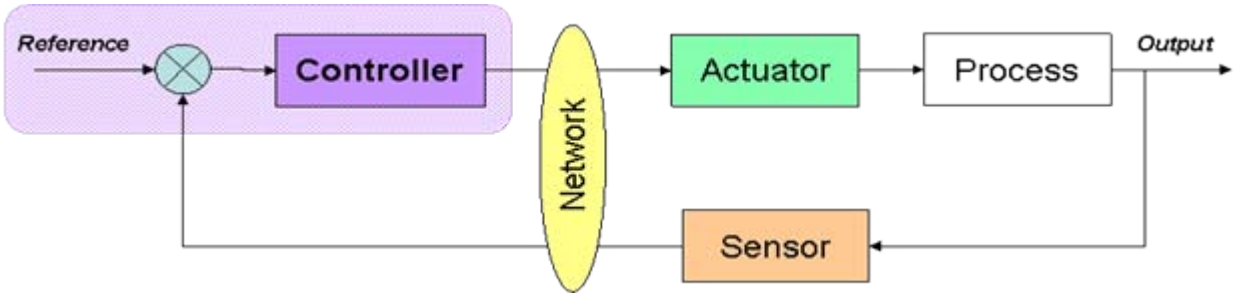
→ D'autres paramètres du diagnostic : Des suggestions ??

→ Diagnostic plus réaliste par banc d'observateurs (les fautes sont identifiables par la signature de plusieurs résidus)

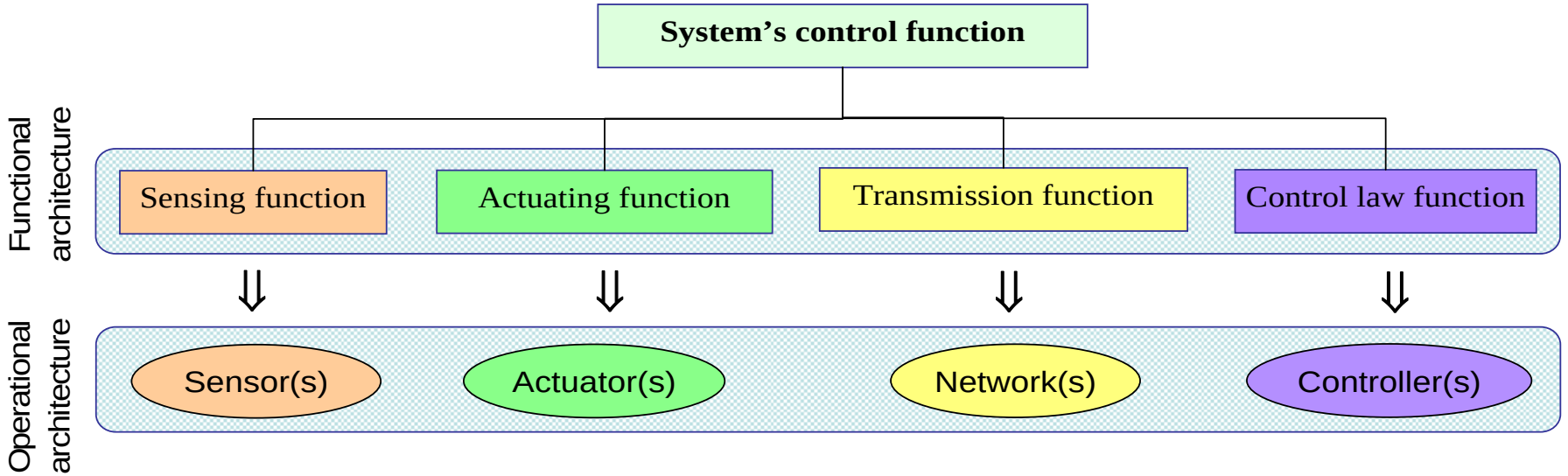
→ Prise en compte de la commande dans la modélisation/analyse

→ Stratégies de reconfiguration plus complexes

Etude de cas

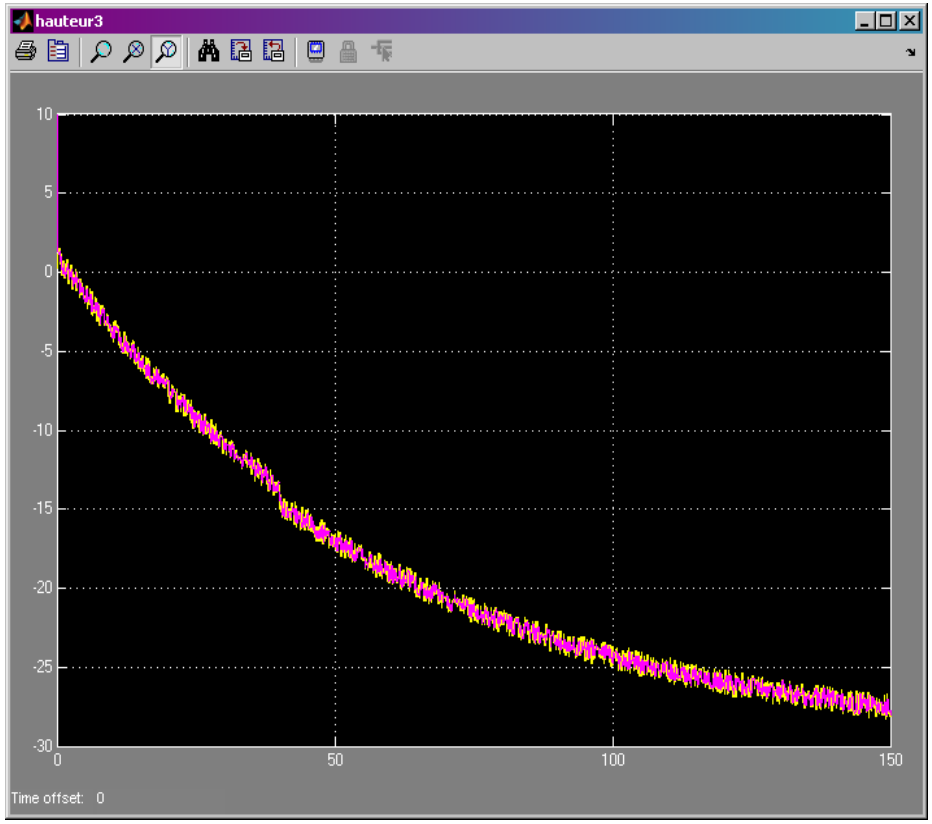


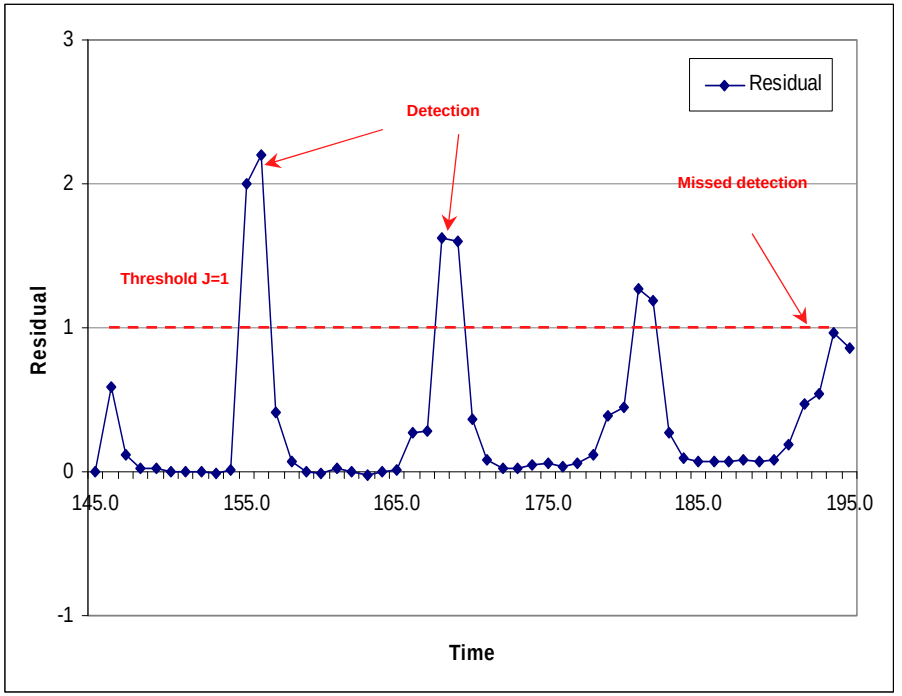
The closed loop functional scheme of an automated system



The functional decomposition applied to a general automated system

Partie II: Modélisation complète de la procédure de diagnostic par observateur de *Luemberger*





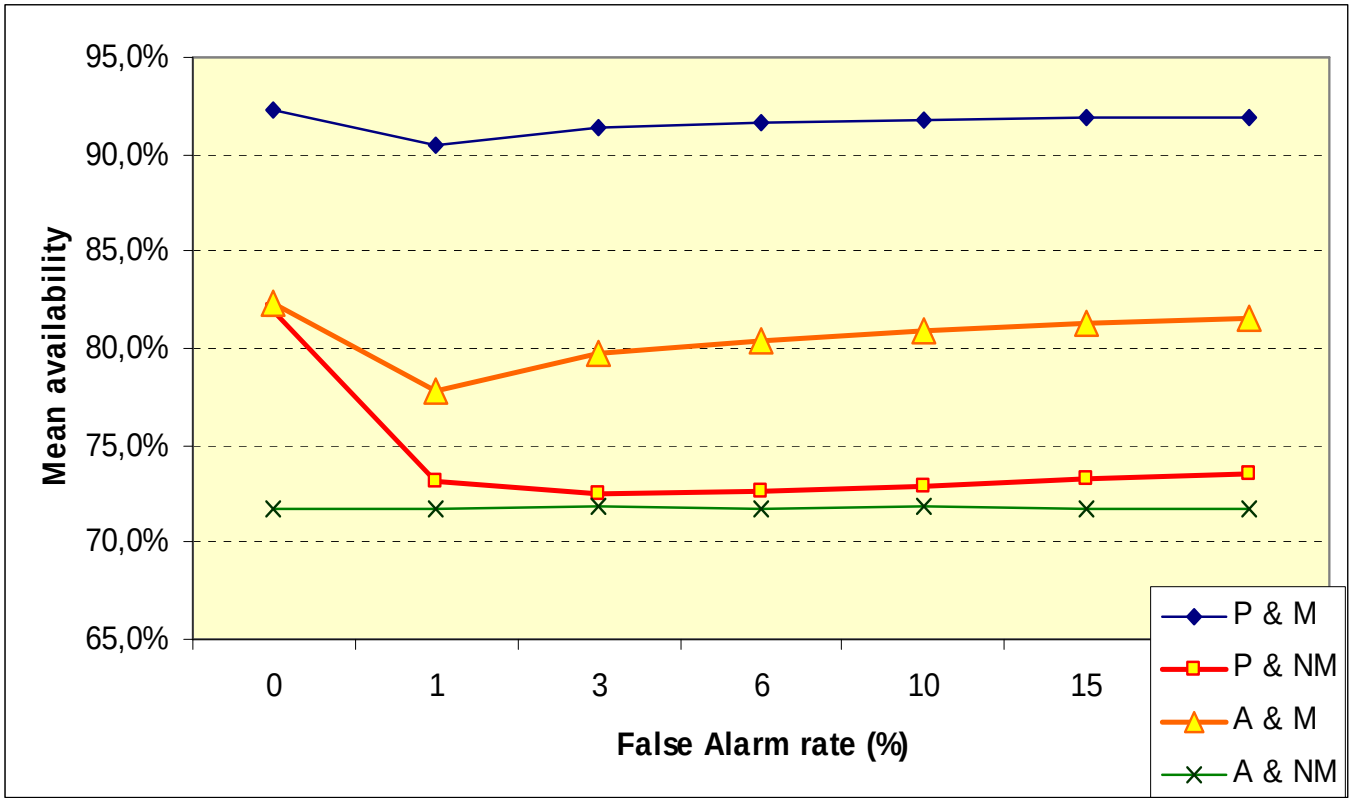
(b) Time evolution of the residual signal

Time evolution of the system and observer's outputs and the residual signal.

Etude de cas

Résultats de simulation [1]

Cas 1 : La disponibilité moyenne du système global



P&M=Redondance passive avec maintenance

P&NM=Redondance passive sans maintenance

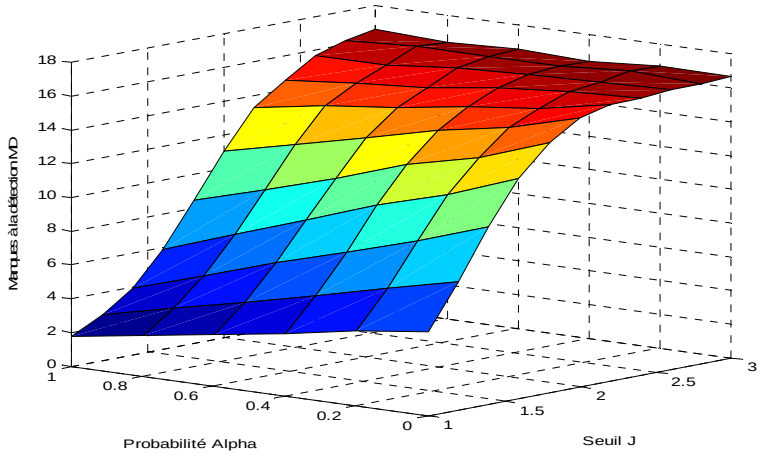
A&M=Redondance active avec maintenance

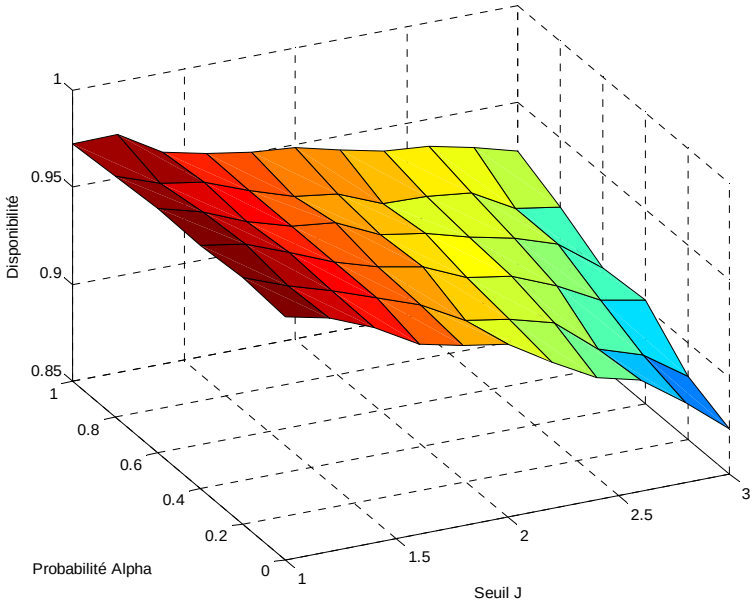
A&NM=Redondance active sans maintenance

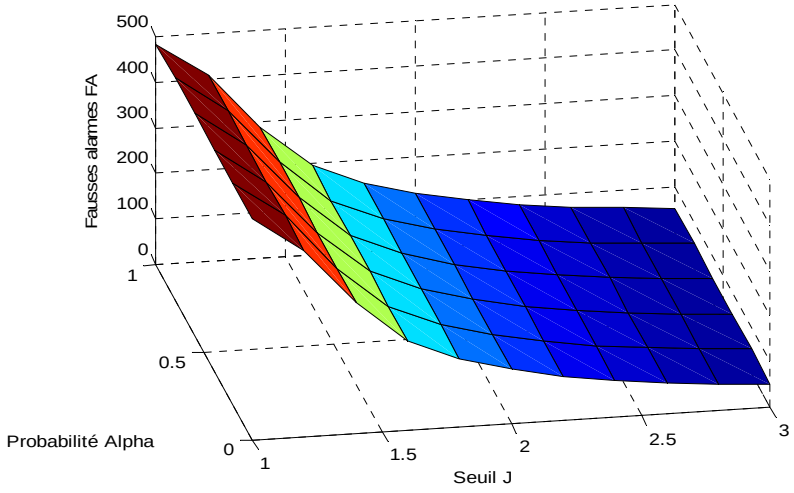
[1] S.Maza, *Journal of Risk and Reliability*, vol. 226, pp. 455-463, 2012.

Etude de cas

Résultats de simulation







Introduction

Un peu de littérature…

Il y a cependant de plus en plus de travaux qui traitent de la modélisation, l'analyse et l'évaluation des systèmes tolérants aux fautes:

(1) Les travaux liés à l'évaluation de la fiabilité dynamique (ex. Travaux de Castaneda et al., Y.Dutuit, …)

(2) (Weber et al., Schön et al.) Sur la prise en compte des informations sur la fiabilité des composants pour la reconfiguration de la commande tolérante aux fautes

(3) (Aslünd et al.,) Sur la prise en compte des performances du diagnostic pour l'analyse de la sécurité par les arbres de causes.