



Fiabilité Dynamique de Capteurs–Transmetteurs à Fonctionnalités Numériques

Florent Brissaud

Université de Technologie de Troyes,
Institut National de l'Environnement Industriel et des Risques,
travaux de thèse encadrés par Anne Barros & Christophe Bérenguer

*réunion du GT S3
25 mars 2011
ENSAM Paris XIII^{ème}*

Plan de la Présentation

I. Introduction

*des besoins en maîtrise des risques technologiques...
...au cas des « **systèmes à intelligence distribuée** » (SID)*

II. Modélisation des SID

*modélisation d'un problème de fiabilité dynamique
sur la base de réseaux de Petri*

III. Cas d'Étude et Évaluation d'un SID

*application à un système de contrôle-commande
pour réacteur nucléaire*

IV. Conclusions

...et perspectives



I. Introduction

I.1. Contexte des Risques Technologiques

besoins en maîtrise des risques et objectifs des travaux

I.2. Systèmes à Fonctionnalités Numériques

*cas des « capteurs-transmetteurs intelligents » (CTI)
et des « systèmes à intelligence distribuée » (SID)*

I.1. Contexte des Risques Technologiques

- **Besoin pour la Maîtrise des Risques Technologiques**
 - améliorer la pertinence et l'efficacité de la prise de décision
→ **développement des approches d'évaluations probabilistes**
- **Besoin pour les Évaluations Probabilistes des Risques**
 - disposer d'outils et de méthodes permettant d'évaluer les probabilités de défaillance des systèmes relatifs à la sécurité
→ **développement des méthodes de sûreté de fonctionnement**
- **Besoin pour la Sûreté de Fonctionnement**
 - répondre à la complexité accrue des systèmes
→ **prise en compte des particularités des systèmes à fonctionnalités numériques**

I.1. Contexte des Risques Technologiques

- **Objectifs des Travaux**

- étendre des méthodes de sûreté de fonctionnement, afin de proposer des ***modélisations*** qui prennent en compte ***les diverses interactions et comportements dynamiques des systèmes***, et développer les ***évaluations*** adéquates

- **Sujets des Travaux**

- ***systèmes de contrôle-commande intégrant des capteurs-transmetteurs à fonctionnalités numériques***
 - ces ***capteurs-transmetteurs*** sont communément qualifiés d' « ***intelligents*** »
 - et ces ***systèmes*** de contrôle-commande sont alors dits à « ***intelligence distribuée*** »

I.2. Systèmes à Fonctionnalités Numériques

- **Capteurs-Transmetteurs « Intelligents » (CTI)**

- ***acquérir, traiter, et transmettre*** des informations

- ***fonctionnalités numériques***

- corrections d'erreurs de mesure
- auto-ajustages
- autodiagnostic et validations
- reconfigurations en ligne
- communication numérique et bidirectionnelle

- avantages pratiques, métrologiques, et financiers

- ***problématiques pour la sûreté de fonctionnement***

- fiabilité
- maintenabilité
- sécurité

*capteur-transmetteur
de pression*

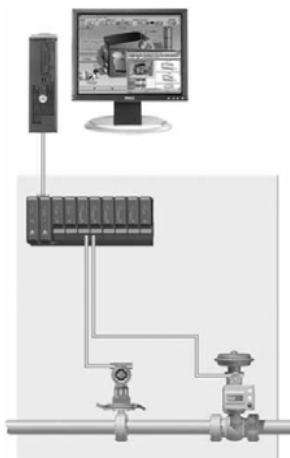


*capteur-transmetteur
de gaz*



I.2. Systèmes à Fonctionnalités Numériques

- **Systèmes à « Intelligence Distribuée » (SID)**
 - *délocalisation de certaines opérations*
 - communication en réseau et *opérations « en collaboration »*
- **Difficultés liées à l'Évaluation des SID**
 - les CTI interagissent entre eux et leur fiabilité est interdépendante
 - les comportements des CTI sont fonction du processus contrôlé, et vice versa



*communication
par bus de terrain*



*communication
sans-fil*





II. Modélisation des SID

II.1. Fiabilité Dynamique

formulation (étendue) d'un problème de fiabilité dynamique

II.2. Formalisme de Modélisation

une approche basée sur des réseaux de Petri pour effectuer des analyses numériques

II.1. Fiabilité Dynamique

- **Problème de Fiabilité Dynamique**

- prendre en compte les **évolutions du système au cours du temps**, notamment **dues à des interactions** avec le processus, l'environnement, et/ou des opérateurs humains
- **Processus (Markovien) Déterministe par Morceaux**
 - variables d'état des composants (discrètes et stochastiques)
 - variables physiques du processus (continues et déterministes)
- ...et les **interactions liées aux fonctionnalités numériques ?**

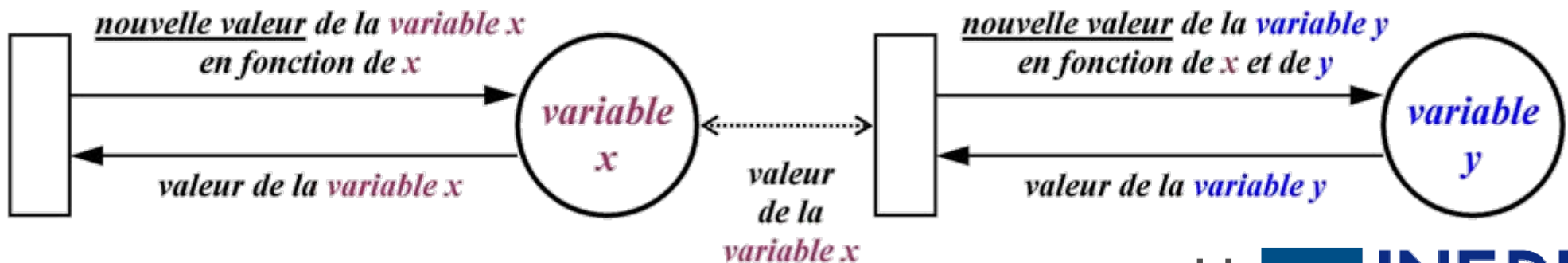


II.1. Fiabilité Dynamique

- **Formulation Étendue du Problème**
 - variables d'**état des composants** (opérant, dégradé, défaillant, ...)
 - configuration du système selon les états de ses composants
 - taux de transition entre états discrets
 - variables du **processus** (niveaux, pressions, températures, ...)
 - variables physiques impliquées dans la dynamique du système
 - équations différentielles
 - variables d'**information** (commandes, mesures, diagnostics, ...)
 - données stockées, traitées, échangées par/entre les composants
 - expressions fonction de valeurs présentes et passées
 - variables de **déviatiion** (dégradations, dérives, ...)
 - déviations/erreurs de nature continue dans les propriétés du système
 - processus stochastiques

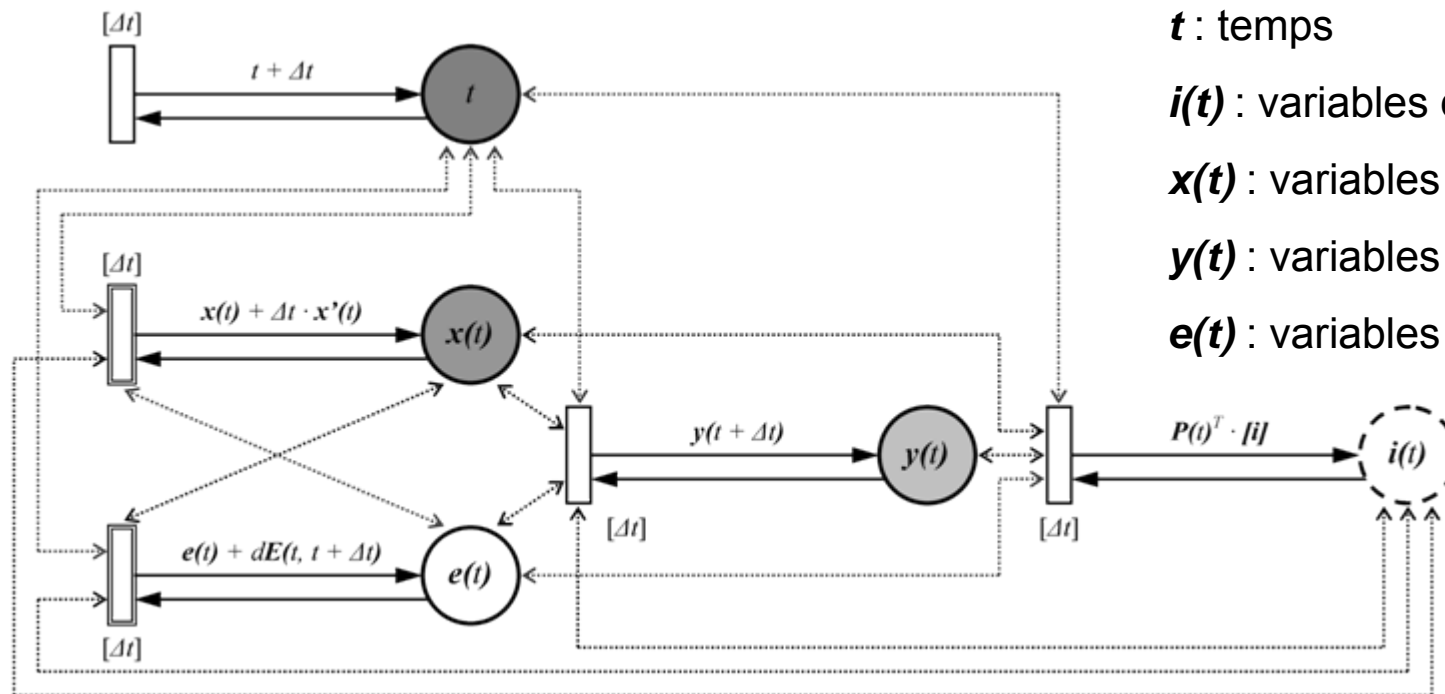
II.2. Formalisme de Modélisation

- **Approche basée sur des Réseaux de Petri**
 - un jeu de variables = {une place, un jeton « coloré », une transition}
 - une « couleur » représente ici un nombre (entier ou réel)
 - les **valeurs des variables** sont données par les **jetons**, au sein des **places** correspondantes, et sont modifiées par les **transitions**
 - les **arcs de sortie** précisent les **nouvelles valeurs à attribuer** aux variables, en fonction des précédentes valeurs de variables, et de variables issues d'autres places



II.2. Formalisme de Modélisation

- **Modélisation Générique pour des Analyses Numériques**
 - dans chaque intervalle de temps $[t ; t + \Delta t[$, les variables au temps $t + \Delta t$ sont calculées en fonction des variables au temps t



t : temps

$i(t)$: variables d'état des composants

$x(t)$: variables du processus

$y(t)$: variables d'information

$e(t)$: variables de déviation



III. Cas d'Étude et Évaluation d'un SID

III.1. Description d'un Cas d'Étude

*systeme de contrôle-commande pour réacteur nucléaire,
intégrant des fonctionnalités numériques*

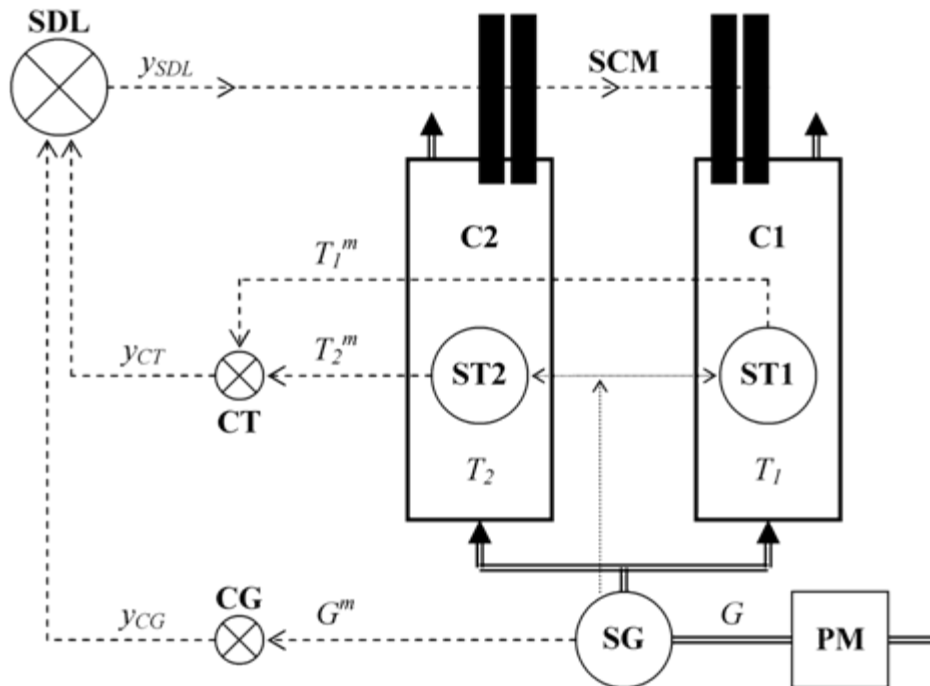
III.2. Évaluation du Cas d'Étude

modélisation, simulations, analyses de fiabilité

III.1. Description d'un Cas d'Étude

• Composants et Variables d'État

- 2 canaux (C1, C2) où du sodium est introduit par une pompe (PM)
- 2 CTI de température (ST1, ST2), 1 CTI de flux (SG)
- 3 contrôleurs (CT, CG, SDL), et 1 arrêt d'urgence (SCM)



exemples de variables d'état des composants

pompe : $SPM = 1$ (opérant), 0 (défaillant), 3 (dégradé)

CTI de température : $SST1 = 1$ (opérant),
 0 (défaillance dangereuse), 2 (défaillance sûre),
 3 (dérives négatives), 4 (dérives positives)

exemple de taux de transition

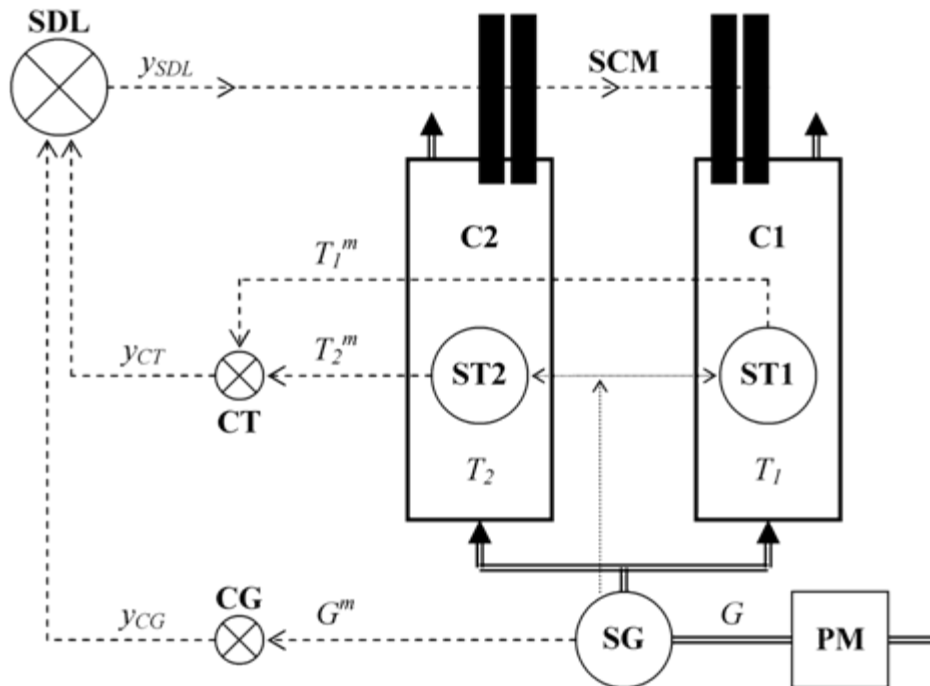
taux de transition de $SST1 = 1$ à $SST1 = 0$:

$$2.5 \cdot 10^{-5} \cdot (1 + [1 \text{ si } SST2 = 0]) \cdot \exp(5.2 \cdot 10^{-3} \cdot T_1)$$

III.1. Description d'un Cas d'Étude

• Variables du Processus et de Déviation

- l'état de la pompe (*SPM*) conditionne sa vitesse angulaire (ω)
- une réduction de la vitesse angulaire diminue le flux de sodium (G), et augmente les températures dans les canaux (T_1, T_2)



exemple de variable de déviation

déviation du couple de la pompe :

$\delta_M(t+dt) - \delta_M(t)$ suit une loi Log-Normale si $SPM = 3$

exemples de variables du processus

$$\frac{d}{dt} \varpi(t) = (C_M - \delta_M(t))/I - K \cdot \varpi(t)/I$$

$$\frac{d}{dt} G(t) = \frac{\nu \cdot G(t)^2}{G(0)} + C_{m2} \cdot (\omega(t)^2 - \omega(0)^2) - \nu \cdot G(0)$$

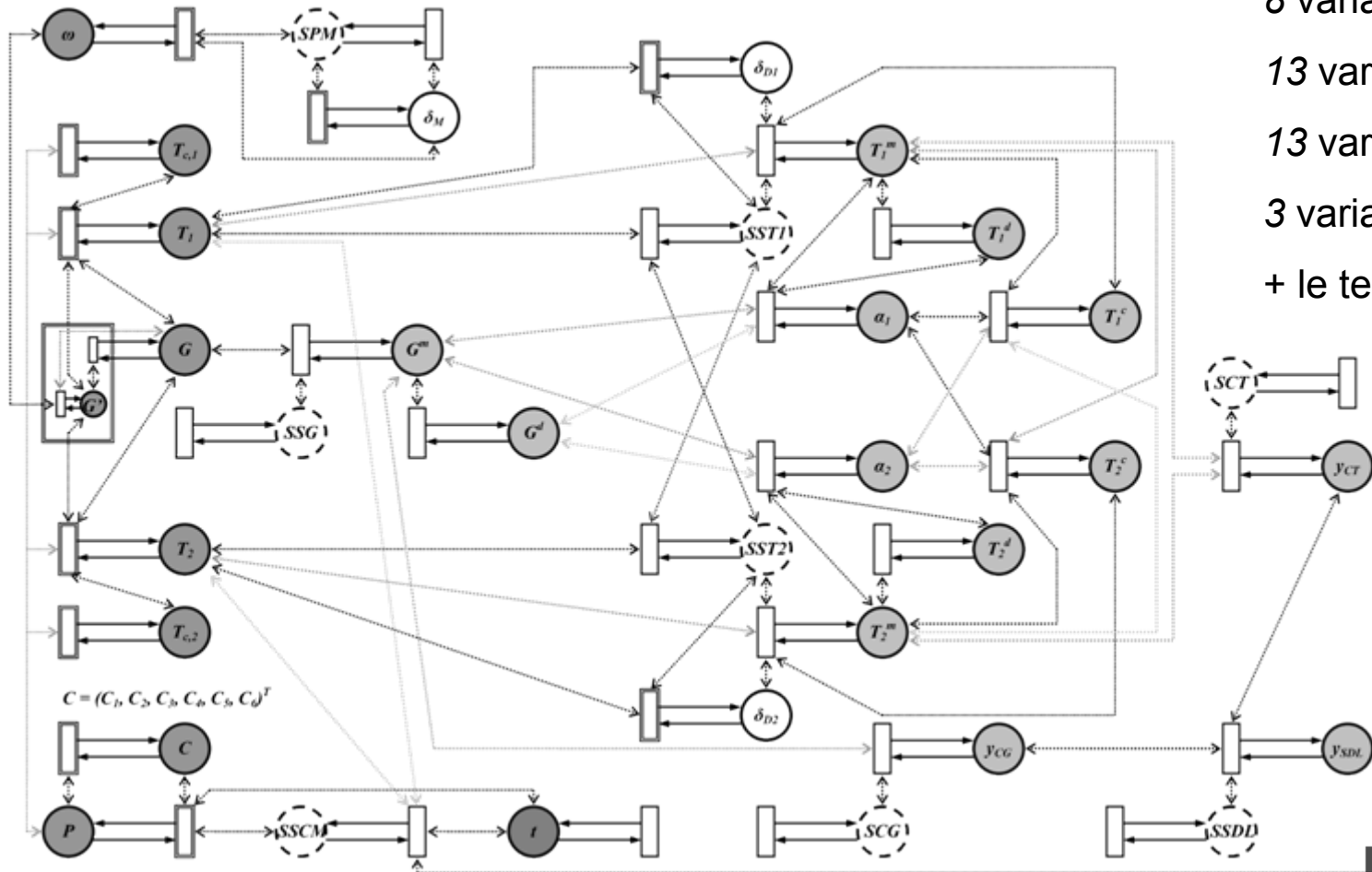
$$\frac{d}{dt} T_i(t) = \frac{w_i \cdot P(t)}{2 \cdot A_i \cdot \tau_i(T_{c,i}(t)) \cdot C_R(T_i(t)) \cdot G(t)} - \dots$$

III.1. Description d'un Cas d'Étude

- « **Fonctionnalités Intelligentes** » et Variables d'Information
 - les résultats de mesure des CTI de température
 - dépendent des états des CTI de température
 - dépendent des températures mesurées
 - peuvent être sujets à des dérives
 - sont compensés par des paramètres de correction
 - « fonctionnalités intelligentes » des CTI
 - i. les CTI de température et de flux **mémorisent leurs résultats de mesure présents et passés**, et se **les communiquent entre eux**
 - ii. les CTI de température **évaluent la cohérence de leurs résultats**, sur la base des relations théoriques (fonction des dérivées)
 - iii. les CTI de température **détectent de potentielles dérives**, et **calculent des paramètres de correction des dérives**

III.2. Évaluation du Cas d'Étude

• Modélisation



8 variables d'état des composants

13 variables du processus

13 variables d'information

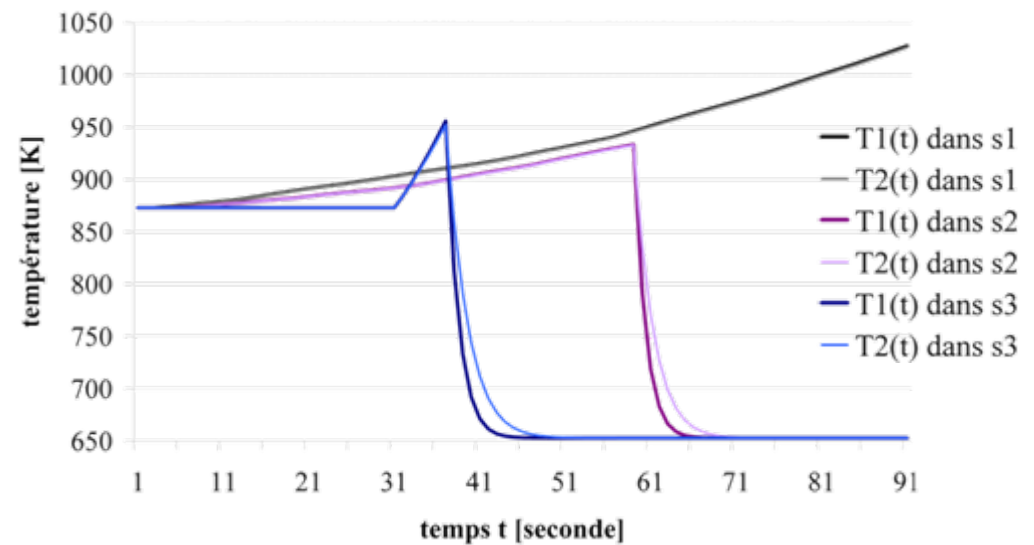
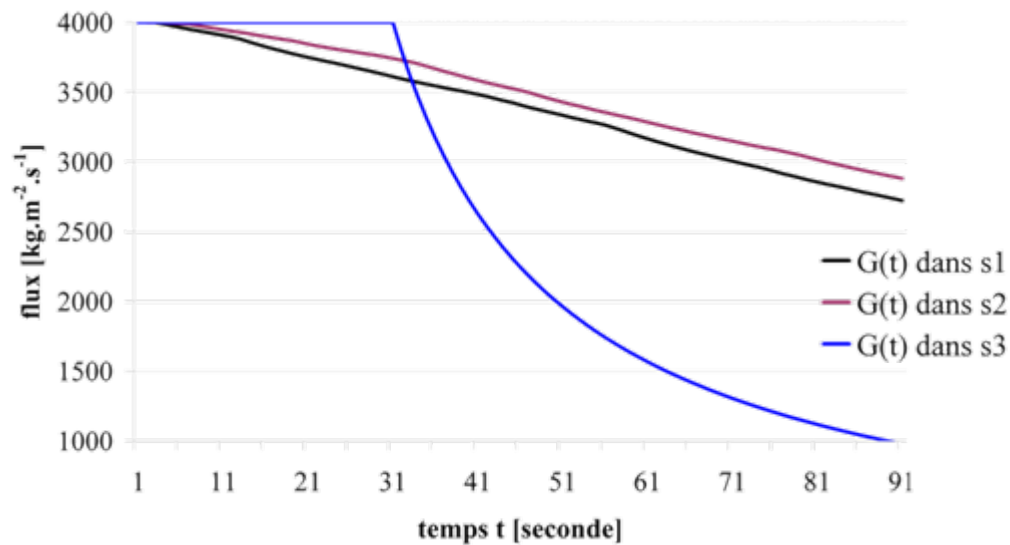
3 variables de déviation

+ le temps t

III.2. Évaluation du Cas d'Étude

• Simulations

- s1 : état dégradé de la pompe, et arrêt d'urgence jamais activé
- s2 : état dégradé de la pompe, puis arrêt d'urgence activé à $t = 57$ s
- s3 : état opérant de la pompe puis état défaillant à $t = 30$ s, puis arrêt d'urgence activé à $t = 35$ s



III.2. Évaluation du Cas d'Étude

- **Analyses de Fiabilité**

- événement initiateur : ***état dégradé de la pompe***
- activation de l'arrêt d'urgence : ***température haute*** ou ***flux bas***
- répartition des scénarios obtenus après simulations :

scénario	sans « fonctionnalités intelligentes »	avec « fonctionnalités intelligentes »
<i>déclenchement intempestif</i>	49.3 %	39.3 %
<i>évènement dangereux</i>	1.6 %	2.3 %
<i>sous-contrôle</i>	49.1 %	58.4 %

- les « fonctionnalités intelligentes » ***impliquent des compromis entre la disponibilité et la sécurité***



IV. Conclusions

IV.1. Conclusions Générales

apports, développements envisageables

IV.2. Perspectives (Quelques Réflexions)

travaux futurs sur la maîtrise des risques...

IV.1. Conclusions Générales

- **Apports des Travaux**

- ***extensions de modèles de fiabilité*** afin de prendre en compte les ***particularités de systèmes à fonctionnalités numériques*** :
 - interactions externes (autres éléments dont CTI, processus contrôlé)
 - comportements dynamiques
- ***évaluations plus fines***, adaptées à la complexité de ces systèmes
→ ***vers de meilleures prises de décision en maîtrise des risques***

- **Développements Envisageables**

- enrichissement des analyses (simulations, approches formelles, ...)
- intégration de travaux connexes (fiabilité logicielle, communication numérique, fiabilité humaine, facteurs organisationnels, ...)

IV.2. Perspectives (Quelques Réflexions)

- **Applications en Maîtrise des Risques**
 - établir des procédures formelles d'*intégration de ces travaux* dans les méthodes d'*évaluations probabilistes des risques*
 - développer des *outils logiciels appropriés*
 - *multiplier les cas d'études*, valider la mise en application
- **Poursuivre les Améliorations en Maîtrise des Risques**
 - intégrer convenablement les *notions de probabilité* dans les politiques et les méthodes de maîtrise des risques
 - développer la pratique des *évaluations probabilistes des risques*
 - engager des *études et recherches en sûreté de fonctionnement* et en évaluations probabilistes, au sein des établissements publics
 - *légiférer sur les approches probabilistes*, en France et en Europe



Merci !

florent.brissaud.2007@utt.fr