BADJI MOKHTAR – ANNABA UNIVERSITY
UNIVERSITE BADJI MOKHTAR – ANNABA

جامعة باجي مختار- عنابة
Année : 2021

**Faculté des Sciences de l'Ingénieur**
**Département d'Electronique**

# Thèse

**Présentée En Vue de L'obtention du Diplôme De Doctorat 3ème Cycle**

**Thème**

# Contribution à l'étude de la sûreté de fonctionnement des systèmes instrumentés intelligents

**Option : Automatique**

Présentée par : **Kharouati Aicha**

**DEVANT LE JURY**

| | | | |
|---|---|---|---|
| DIRECTEUR DE THESE | **: DEBBACHE Nasr Eddine** | **Pr** | **Université Annaba** |
| PRESIDENT | **: ABBASSI Hadj Ahmed** | **Pr** | **Université Annaba** |
| EXAMINATEURS | **: LAKEL Rabah** | **Pr** | **Université Annaba** |
| | **: SOUFI Youcef** | **Pr** | **Université Tebessa** |

# Remerciements

Mes premiers remerciements vont à Allah tout puissant pour le courage, la patience et la volonté qu'il m'a donnée pour accomplir ce travail.

Je tiens à exprimer toute ma reconnaissance et ma gratitude à mon directeur de thèse Monsieur le Professeur **DEBBACHE Nasr Eddine**, pour avoir dirigé ce travail. Je le remercie pour ses précieux conseils et ses commentaires qui m'ont permis de surmonter mes difficultés et de progresser dans mes études. Qu'il soit remercié pour ses qualités humaines et scientifiques, et ses conseils judicieux sur différents points relatifs à mon projet de thèse. J'ai été honoré de travailler avec lui.

Mes remerciements s'adressent à Monsieur **ABBASSI Hadj Ahmed**, Professeur à l'université d'Annaba, d'avoir fait l'honneur de présider mon jury de soutenance.

Je tiens à remercier Monsieur **LAKEL Rabah**, Professeur à l'université d'Annaba d'avoir accepté d'examiner mon travail de thèse et d'être membre de mon jury de soutenance.

Je tiens à remercier aussi, Monsieur **SOUFI Youcef**, Professeur à l'université de Tebessa, de m'avoir fait l'honneur d'examiner mon travail et d'être membre de jury de ma thèse de doctorat.

# ملخص

***ملخص*** *:* تلعب الأدوات الذكية دورًا مهمًا للغاية في تحسين موثوقية الأنظمة الصناعية ، لأنها تتضمن وظائف إضافية ، التعويض ، والتحقق من الصحة ، والتشخيص الذاتي والتكوين الذاتي ، المرتبطة بوسائل الاتصال المناسبة. لهذا السبب ، قمنا بدراسة مساهمة هذه الأدوات الذكية في تطور الأداءين من حيث السلامة التشغيلية لأنظمة السلامة المجهزة . (SIS)المؤشرات التي تؤخذ في الاعتبار كمعيار لتقييم السلامة هي احتمالية الفشل الخطير (PFD) واحتمال الفشل الآمن . (PFS)النهج المستخدم يعتمد على شبكات بيتري العشوائية. تم إجراء دراسة حالة على نظام ميكاترونيك فيما يتعلق بالتحكم في حجم خزانين في التكرار السلبي باستخدام خزان واحد فقط في كل مرة .للقيام بذلك ، تتم مواجهة ثلاث طرق لنمذجة السلوك الوظيفي والاختلال للنظام الذي تمت دراسته في الحالة الكلاسيكية وفي حالة الذكاء ، وهي: شجرة الأعطال ومخطط الموثوقية وشبكة بتري العشوائية. من الضروري تحديد النهج الأنسب لنمذجة حالة الدراسة ومعالجة الجانب الديناميكي. ثم يتم معالجة معلمات السلامة التشغيلية: الموثوقية والتوافر ومؤشري الأمان.

***الكلمات المفتاحية :*** *السلامة التشغيلية ، الأدوات الذكية ، أنظمة السلامة المجهزة ، نظام الميكاترونيك ، شبكة بتري العشوائية.*

# Résumé

***Résumé :*** Les instruments intelligents jouent un rôle primordial dans l'amélioration de la sûreté de fonctionnement des systèmes industriels, car ils intègrent des fonctionnalités supplémentaires, de compensation, de validation, d'autodiagnostic et d'auto-configuration, associées à des moyens de communication appropriés. Pour cette raison, nous avons étudié l'apport de ces instruments intelligents dans l'évolution des deux performances en termes de sûreté de fonctionnement des Systèmes Instrumentés de Sécurité (SIS). Les indicateurs pris en compte comme critère d'évaluation de sécurité sont la Probabilité de Défaillances Dangereuses (PFD) et la Probabilité de Défaillances Sûres (PFS). L'approche utilisée s'appuie sur les réseaux de Petri stochastiques. Une étude de cas a été faite sur un système mécatronique qui concerne la régulation de volume de deux réservoirs en redondance passive avec utilisation d'un seul réservoir à la fois.

Pour ce faire, trois approches de modélisation du comportement fonctionnel et dysfonctionnel du système étudié dans le cas classique et avec intelligence sont confrontées; à savoir : arbre de défaillance, diagramme de fiabilité et Réseau de Petri stochastique. Il convient de déterminer l'approche qui sera la mieux adaptée à la modélisation du cas d'étude et à la prise en charge de l'aspect dynamique. Les paramètres de la sûreté de fonctionnement traités sont alors : la fiabilité, la disponibilité et les deux indicateurs de sécurité.

***Mots-clés :*** *Sûreté de fonctionnement, instruments intelligents, systèmes instrumentés de sécurité, système mécatronique, Réseau de petri stochastique.*

# Abstract

***Abstract :*** Intelligent instruments play a key role in improving the operational safety of the industrial systems, because they include an additional compensation, validation, self-diagnosis and self-configuration functions. For this reason, we have studied the contribution of these intelligent instruments in the evolution of the two performances in terms of safety, Safety Instrumented Systems (SIS). The indicators taken into account as a safety evaluation criterion are the Probability of Dangerous Failures (PFD) and the Probability of Safe Failures (PFS). The approach used is based on stochastic Petri nets. A case study was studied consided on a mechatronic system concerning the volume control of two tanks in passive redundancy with the use of only one tank at a time. To carry out this study, three approaches to modeling the functional and dysfunctional behavior of the studied system in the classical case and with intelligence are confronted, namely: fault tree, reliability diagram and stochastic Petri network. It is necessary to determine the approach that will be best suited to the modeling of the study case and to the handling of the dynamic aspect. The operational safety parameters treated are then: reliability, availability and the two safety indicators.

***Keywords:*** *Dependability, intelligents instruments, safety instrumented systems, mechatronic system, Stochastic petri network.*

# Tables des matières

**Chapitre 2 : La Sûreté de Fonctionnement -analyses et concepts**

**Chapitre 3 : Système instrumenté de sécurité**



**Chapitre 4 : Amélioration de la sûreté de fonctionnement d'un système mécatronique**

# Tables des figures

# Liste des tableaux

# INTRODUCTION GENERALE

# Introduction générale

L'évaluation de la sûreté de fonctionnement d'un système consiste à analyser les défaillances des composants pour estimer leurs conséquences sur le service rendu par le système. Donc on défini la sûreté de fonctionnement est la science de défaillance. N'importe quel dispositif classique ou intelligent peut dysfonctionner d'où la nécessité de l'étude de la sûreté de fonctionnement afin de garantir le bon fonctionnement de l'ensemble du système.

Les instruments intelligents sont des nouveaux systèmes d'instrumentation qui sont apparus avec les progrès de la microélectronique et des réseaux associés aux besoins des utilisateurs. Ces instruments offrent la possibilité d'un traitement local de l'information qui est répartie sur les diverses entités permettant ainsi une distribution de l'exécution des tâches et faisant apparaître une commande distribuée. Le traitement local a été permis par le développement parallèle des réseaux de terrain favorisant le partage des ressources par l'interconnexion des unités de traitement et la réduction des câblages.

L'influence de l'instrumentation intelligente sur l'attribut sécurité de la sûreté de fonctionnement qui consiste à se préserver de situations dangereuses ou catastrophiques est contrastée. Elle contribue à une amélioration dans les applications où la sécurité est critique par la mise en place de moyens d'autodiagnostic et de validation mais elle peut introduire de nouveaux modes de défaillance affectant la sécurité par l'emploi de dispositifs non éprouvés.

Le présent travail a pour objectif d'évaluer les performances en termes de sûreté de fonctionnement des systèmes instrumentés de sécurité (SIS) à disposant d'instruments d'intelligents en conformité avec les normes de sécurité fonctionnelle. La performance d'une fonction de sécurité peut être exprimée comme la probabilité de défaillance dangereuse PFD et la probabilité de défaillances sûres PFS. Les systèmes SIS disposent d'un nombre important de traitements et d'une augmentation de la complexité contrairement aux systèmes classiques qui ne sont pas dotés d'intelligence. Ceci rend la tâche de l'évaluation de la sûreté de fonctionnement plus difficile à appréhender. Les Systèmes Instrumentés de Sécurité (SIS) sont des systèmes utilisés comme moyens de protection pour réaliser des fonctions de sécurité

et mettre le procédé surveillé dans une position de repli de sécurité. L'approche de modélisation utilisée est réseaux de Petri stochastiques.

Nous nous sommes proposé d'étudier aussi l'apport des instruments intelligents dans l'amélioration de la sûreté de fonctionnement(SdF) d'un système mécatronique. Pour ce faire, trois approches de modélisation du comportement fonctionnel et dysfonctionnel du système étudié dans le cas classique et avec intelligence sont confrontées, à savoir : arbre de défaillance, diagramme de fiabilité et Réseau de petri stochastique. Il convient de déterminer l'approche qui sera la mieux adaptée à la modélisation du cas d'étude et à la prise en charge de l'aspect dynamique. Les paramètres de la sûreté de fonctionnement traités dans cette étude sont alors : la fiabilité, la disponibilité et les deux indicateurs de sécurité PFD et PFS. L'outil logiciel de simulation utilisé est GRIF (**Gr**aphiques **I**nteractif pour la **F**iabilité). Les méthodes classiques de la sûreté de fonctionnement (SdF) prennent vite leurs limites face à la complexité des systèmes. Les méthodes combinatoires (arbres de défaillance, Réseau de petri stochastique, diagrammes de fiabilité) permettent exclusivement de retrouver et d'apprécier les combinaisons des événements conduisant à l'occurrence d'une défaillance.

Selon les méthodes de la SdF, notre choix s'est orienté vers la modélisation par Réseau de petri stochastique car cette méthode est très largement utilisée dans ce domaine. Elle permet de modéliser les états de fonctionnement normal et de panne des éléments du système étudier.

Aussi, le travail de cette thèse est structuré en quatre chapitres :

Le premier chapitre aborde en premier lieu un traitement d'état de l'art des instruments intelligents. Les architectures matérielles et fonctionnelles d'un instrument intelligent sont montrées ainsi que quelques modèles génériques. Dans ce chapitre, nous discutons aussi des caractéristiques des systèmes d'automatisation à intelligence distribuée (SAID) qui sont une extension des systèmes automatisés.

Le deuxième chapitre traite l'état de l'art de la sûreté de fonctionnement ainsi que les différentes notions et méthodes, afin de traiter l'aspect de sûreté de fonctionnement des systèmes d'instrumentation. Dans un premier temps, nous avons présenté les différents éléments de la SdF tels que : la fiabilité avec ses différentes formes, la maintenabilité, la disponibilité et la sécurité, ainsi que les indicateurs définissant les différents temps de la SdF. Dans un deuxième temps, nous avons présenté un cadre générique sur les principales méthodes d'analyse de la sûreté de fonctionnement.

Le troisième chapitre nous nous intéressons au concept nouveau de la sécurité intelligente. Ce concept est inhérent à l'utilisation d'instruments intelligents dans les systèmes instrumentés de sécurité. Nous positionnons la problématique de l'utilisation des instruments intelligents dans les applications sécuritaires en situant quelques différences qui existent entre les systèmes classiques et les systèmes intelligents. Ensuite, nous discutons de l'introduction du concept de l'intelligence dans un système instrumenté de sécurité par la distribution des traitements au plus près du processus et suivant les niveaux d'intelligence introduits auparavant c'est-à-dire dans les dispositifs de terrain tels que les capteurs et actionneurs. Enfin, nous proposons une méthodologie d'évaluation des systèmes instrumentés de sécurité(SIS) auxquels il y a eu incorporation d'instruments intelligents pour devenir des Systèmes Instrumentés de Sécurité à Intelligence Distribuée (SISID). On réalise la fonction de sécurité des systèmes instrumentés de sécurité (SIS) à partir de l'étude des deux indicateurs de sécurité. Ces indicateurs sont donnés sous forme de probabilités de défaillance dangereuse (PFD) et de défaillance en sécurité (PFS). L'approche utilisée s'appuie sur les réseaux de Petri stochastiques.

Le quatrième chapitre propose une étude méthodologique comparative d'un système mécatronique dans le cas classique et avec intelligence. Cette étude pour exprimer l'apport des instruments intelligents dans l'amélioration de la sûreté de fonctionnement d'un système mécatronique. Le système étudier est un système mécatronique concerne la régulation de volume de deux réservoirs en redondance passive avec utilisation d'un seul réservoir à la fois. La méthodologie utilisée consiste en la modélisation de l'aspect fonctionnel et dysfonctionnel de ces systèmes en adoptant le formalisme basé sur les réseaux de Petri stochastiques qui assurent la représentation du comportement dynamique de ce type de systèmes. Les paramètres de la sûreté de fonctionnement traités sont alors : la fiabilité, la disponibilité et les deux indicateurs de sécurité PFD et PFS. La fonction de sécurité réalisée alors est la protection du système de passer dans un état de débordement du réservoir, donc réduire les défaillances dangereuses dans le système étudier.

Une conclusion générale montrant les différents résultats proposés par ce travail clôture la rédaction de cette thèse.

# CHAPITRE 1
# INSTRUMENTATION INTELLIGENTE:
# PROBLEMATIQUE ET CONTEXTE

# Chapitre 1

# Instrumentation intelligente: Problématique et contexte

## 1.1 Introduction

L'objet de ce chapitre est de présenter les concepts des instruments intelligents qui sont considérés comme composantes des systèmes d'automatisation à intelligence distribuée (SAID). Ces instruments disposent de techniques numériques intégrées dans les microcontrôleurs et les interfaces de communication et offrent la possibilité d'un traitement local de l'information qui est permis par le développement des réseaux de communication. Les architectures matérielles et fonctionnelles d'un instrument intelligent sont montrées ainsi que quelques modèles génériques. Dans ce chapitre, nous discutons aussi des caractéristiques des systèmes d'automatisation à intelligence distribuée qui sont une extension des systèmes automatisés.

## 1.2 instruments intelligents

Les instruments intelligents sont des nouveaux systèmes d'instrumentation qui sont apparus avec les progrès de la microélectronique et des réseaux associés aux besoins des utilisateurs. Ces instruments offrent la possibilité d'un traitement local de l'information qui est

répartie sur les diverses entités permettant ainsi une distribution de l'exécution des tâches et faisant apparaître une commande distribuée [55].

Le traitement local a été permis par le développement parallèle des réseaux de terrain favorisant le partage des ressources par l'interconnexion des unités de traitement et la réduction des câblages.

L'interconnexion des instruments intelligents en réseau conduit aussi à des problèmes d'informatique répartie comme la synchronisation, le partage des ressources, la communication et des problèmes plus spécifiques à l'automaticien comme le respect des contraintes temporelles, la définition de scénarios de commande, la supervision, la fusion de données, le fonctionnement en mode dégradé ainsi que la planification des actions [12][14].

### 1.2.1 Historique et évolution des instruments intelligents

Le développement et le progrès de la micro-électronique et de la micro-informatique ont connu une croissance rapide durant ces dernières décennies. En effet, les années 70 ont vu l'apparition des calculateurs numériques, en complémentarité des systèmes traditionnels de mesure et de contrôle analogiques et logiques. Les calculateurs traitaient les fonctions de contrôle/commande de façon centralisée.

L'évolution des systèmes automatisés prenant en compte, en plus du contrôle-commande, la maintenance, la sécurité et la gestion technique conduit à un besoin de plus en plus important d'informations, et une augmentation des traitements en nombre et en complexité. Cette évolution mène à une délocalisation des traitements rendue possible par le développement des réseaux de terrain, d'une part, et des équipements intelligents, d'autre part. Les premiers capteurs dits « intelligents » sont apparus dans les années 1980. Dédiés le plus souvent aux systèmes numériques de contrôle-commande, ils sont développés par des grands constructeurs d'automatismes : Honeywell, Fuji, Control Bailey, … En France, des travaux sur les besoins des utilisateurs donnent lieu à un Livre Blanc sur les capteurs intelligents en 1987 et un autre sur les actionneurs en 1988. Les institutions nationales et/ou européennes ont été partie prenante dans la genèse de ces concepts et produits ; en témoignent le soutien apporté aux travaux de la CIAME (Commission Interministérielle pour l'Automatisation et la Mesure) dans les années 1980 et les différents projets qui ont été soutenus [55].

Vers la fin des années 90, les fabricants ont refait la conception des éléments de mesure de beaucoup d'instruments. Des techniques numériques ont été adoptées dans la conception de capteurs et d'actionneurs qui ont fait évoluer ces instruments avec l'emploi de ces nouvelles technologies. Le résultat était significatif dans trois secteurs de performances pour ces instruments:

-Précision,

- Traitement des signaux à bord au plus près du procédé physique avec une délocalisation de certaines tâches de la décision.

-Diagnostic à bord ; une amélioration raisonnable du diagnostic est disponible. Par exemple, un émetteur de différence de pression a maintenant 64 sorties pour le diagnostic de signal disponibles sur le réseau [3].

### 1.2.2 Notion d'intelligence

L'intelligence est une notion particulièrement complexe, et elle est difficile à définir. Plusieurs attributs peuvent entrer dans sa définition. Nous allons commencer tout d'abord par définir le vocable intelligence.

Intelligence vient du latin intellegentia (faculté de comprendre), dérivé du latin intellegere signifiant comprendre, et dont le préfixe inter (entre), et le radical legere (choisir, cueillir) ou ligare (lier) suggèrent essentiellement l'aptitude à relier des éléments qui sans elle resterait séparés [3].

Du point de vue de la psychologie, l'intelligence est l'intégration de la perception, la raison, l'émotion, le comportement de la détection, du savoir, de la planification et de l'action sur le système afin de réussir à atteindre ses objectifs [95]. L'intelligence est généralement définie comme la capacité d'un système à adapter son comportement aux contraintes de son environnement : par exemple la capacité d'adaptation à des situations nouvelles, la capacité d'apprentissage, d'abstraction, de contrôle, de résolution de problèmes, etc.

L'intelligence dans ces instruments intelligents est principalement assurée par des microprocesseurs. Typiquement la mesure du capteur après compensation était convertie en forme numérique et est traitée, par exemple, en linéarisant la sortie dans le cas où elle excède sa plage de fonctionnement, et puis en l'adaptant dans un format approprié à la transmission sur un réseau analogique ou pseudo-numérique [3].

### 1.2.3 Avantages de l'intelligence d'un capteur

L'intelligence du capteur intelligent réside dans sa capacité de vérification du bon déroulement d'un algorithme de métrologie. Cette intelligence est liée à l'amélioration de performances de capteur (exactitude, temps de réponse,…) par l'accroissement de la crédibilité de la mesure. Un capteur intelligent offre des avantages spécifiques tels que [82] [83] [87] [88] :

- ✓ la possibilité de configurer le capteur à distance ;
- ✓ la crédibilité accrue des mesures ;
- ✓ la coopération via un système de communication dédié en temps réel ;
- ✓ l'aide à la maintenance et à la prise de décision grâce aux informations d'état fournies;
- ✓ la participation à la commande du système en intégrant des fonctions de commande-régulation ;
- ✓ la participation à la sécurité du système en offrant des possibilités d'alarme ;
- ✓ la télésurveillance ;

Les fonctions d'un système aux capteurs intelligents peuvent être décrites en termes de :

- compensation ;
- validation ;
- traitement de l'information ;
- communications ;
- intégration ;

La combinaison de ces éléments respectifs permet aux capteurs intelligents un mode de fonctionnement autonome effectuant une détection active. La compensation est la capacité du système à détecter et à réagir aux changements dans l'environnement réseau à travers les routines d'autodiagnostic, d'auto-calibrage et d'adaptation. Un capteur intelligent doit être en

mesure d'évaluer la validité des données recueillies, les comparer à celles obtenues par d'autres capteurs et de confirmer l'exactitude de toute variation de données suivantes. Ce processus comprend essentiellement l'étape de configuration du capteur. Ce type de capteurs offre des avantages [82] [83] [85] [87] [88] :

- **Métrologiques** : accroissement de la précision (fusion de données, auto-calibrage, coopération,…) ;
- **Fonctionnels** : aide à la maintenance par autotest intégré susceptible de déterminer automatiquement quel est l'élément défaillant, de transmettre des indications d'erreurs, mémorisation des évènements redoutés, configuration à distance, alarme
- **Economiques** : réduction des durées d'étalonnage et de calibration, fiabilité accrue, allègement de la charge du calculateur central,…

### 1.2.4 Concepts et caractéristiques d'un instrument intelligent

On défini un instrument intelligent (qu'il soit capteur ou actionneur) est obtenu par l'association de la technologie issue de l'instrumentation, de l'électronique et de l'informatique. Il est capable d'intégrer des fonctions supplémentaires telles que la validation, l'autodiagnostic, la compensation, la communication, etc. Ces instruments sont capables d'adapter leur fonctionnement suivant des changements produits dans leurs environnements [55].

L'ensemble des fonctionnalités permet à l'instrument intelligent de crédibiliser sa fonction associée à sa coopération dans un système distribué. La capacité à valider la mesure pour le capteur et à rendre compte de la réalisation par l'actionneur reflète cette crédibilisation et la participation dans un système distribué se manifeste par la participation à la commande, à la sécurité (alarmes), à l'exploitation du système… [2][80].

Un instrument intelligent est donc une composante des systèmes d'automatisation à intelligence distribuée. Il est constitué d'un capteur ou d'un actionneur doté de fonctionnalités de communication, de configuration, d'autodiagnostic et de validation, en plus des fonctionnalités de mesure ou d'action [80] [55].

Il est généralement constitué d'un processeur ou d'un microcontrôleur et d'une interface de communication à un réseau de communication (souvent un réseau de terrain). Son logiciel peut implémenter du simple traitement du signal aux méthodes de l'intelligence artificielle.

Les instruments intelligents sont connectés en réseaux à un système central (ordinateur ou automate programmable). Il est aussi possible de créer une application complète, composé uniquement d'instruments connectés entre eux.

Il existe un certain nombre de caractères communs à tous les instruments capteurs lorsqu'ils sont utilisés dans un environnement donné [76].

- ✓ **Précision :** L'écart entre la valeur du paramètre mesuré et l'information délivrée est la précision. Celle-ci, exprimée en pourcentage est l'incertitude absolue obtenue sur la grandeur électrique. Une bonne précision finale dépend d'une bonne corrélation entre une caractéristique d'une grandeur physique pouvant être mesurée et le phénomène à mesurer.
- ✓ **Sensibilité :** Correspond à l'importance de la modification du signal de sortie entraînée par une variation de la grandeur à mesurer. Elle dépend du corps d'épreuve et du transducteur.
- ✓ **Sélectivité :** Correspond à sa capacité à détecter une substance parmi d'autres. Elle dépend de la partie sensible du capteur.
- ✓ **Linéarité :** Un capteur est dit linéaire s'il présente la même sensibilité sur toute l'étendue de sa plage d'emploi.
- ✓ **Réversibilité** : Elle définit la capacité du matériau à revenir à son état initial lorsqu'on supprime l'excitation.
- ✓ **Temps de réponse :** Il exprime le temps nécessaire que met la valeur de sortie du capteur pour se stabiliser lorsque les conditions de mesure varient brutalement d'un état à un autre. Le temps de réponse est pris entre 10% et 90% de la valeur stabilisée.
- ✓ **Fiabilité :** La fiabilité est définie comme la capacité d'un capteur fonctionnant correctement, c'est-à-dire, à fournir des données avec une précision annoncée.
- ✓ **Autonomie :** c'est-à-dire sa durée maximale de fonctionnement continu sans intervention humaine et sa capacité d'autoentretien.

Un capteur doit être rapide, il doit donner une réponse en temps réel, chaque essai doit être reproductible et facile à calibrer, il doit être robuste et résiste aux changements de température, pH, force ionique. De plus son utilisation doit être simple, exigeant un minimum de technicité.

### 1.2.5 Structure d'un capteur intelligent

Les capteurs intelligents intègrent des fonctionnalités supplémentaires leur permettant de relier le monde physique avec le monde numérique en capturant et en révélant des phénomènes physiques du monde réel et la conversion de ceux-ci dans une forme qui peut être traitée et stockée dans le but d'agir et de prendre une décision.

La détection, qui est la fonction primordiale d'un capteur, est une technique utilisée pour recueillir des informations sur un objet physique ou sur un processus, y compris la survenance d'événements (par exemple, les changements d'état tels que la baisse de la température ou de la pression). Un objet exécutant une telle tâche de détection est appelé un capteur. C'est un dispositif de prélèvement d'informations qui convertit une grandeur physique ou un événement en une autre grandeur physique de nature différente (très souvent signal électrique). Cette grandeur représentative de la grandeur prélevée est utilisable à des fins de mesure, de calcul, d'analyse ou de commande. Un autre terme couramment utilisé est le transducteur, qui est souvent utilisé pour décrire un dispositif qui convertit l'énergie d'une forme à une autre. La figure 1.1 illustre le schéma d'un capteur classique [81] [82] [83] [85].

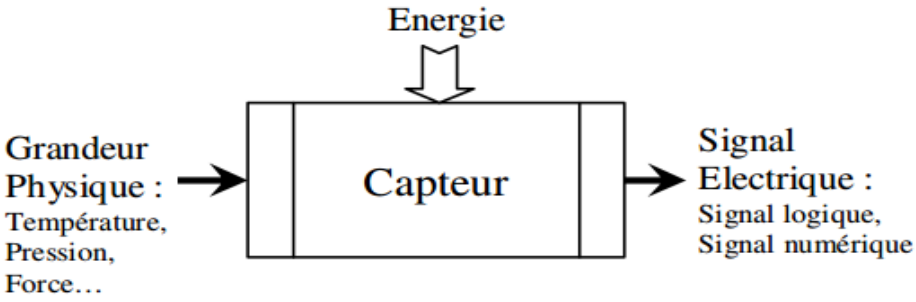



**Figure 1.1** Schéma d'un capteur classique.

Les étapes effectuées dans une tâche de détection (ou d'acquisition de données) sont représentées sur la figure 1.2. Les phénomènes physiques (souvent désignés comme des procédés, systèmes) sont observés par un capteur. Les signaux électriques qui en résultent ne sont souvent pas prêt pour un traitement immédiat. Par conséquent, ils passent par une étape de conditionnement du signal. Une série d'opérations peut être appliquée au signal de capteur afin de le préparer pour une utilisation ultérieure. En effet, les signaux ont souvent besoin d'amplification (ou d'atténuation) pour modifier leur amplitude afin de mieux les correspondre à la gamme du convertisseur analogique-numérique suite à la conversion. En plus, le conditionnement de signaux applique souvent un filtrage ou une compensation pour éliminer les bruits indésirables (grandeurs d'influence) dans certaines gammes de fréquences.

Après le conditionnement, le signal analogique est transformé en un signal numérique en utilisant un convertisseur Analogique/Numérique ADC. Le signal est maintenant disponible sous forme numérique et prêt pour un traitement ultérieur de stockage ou de visualisation [85] [87].

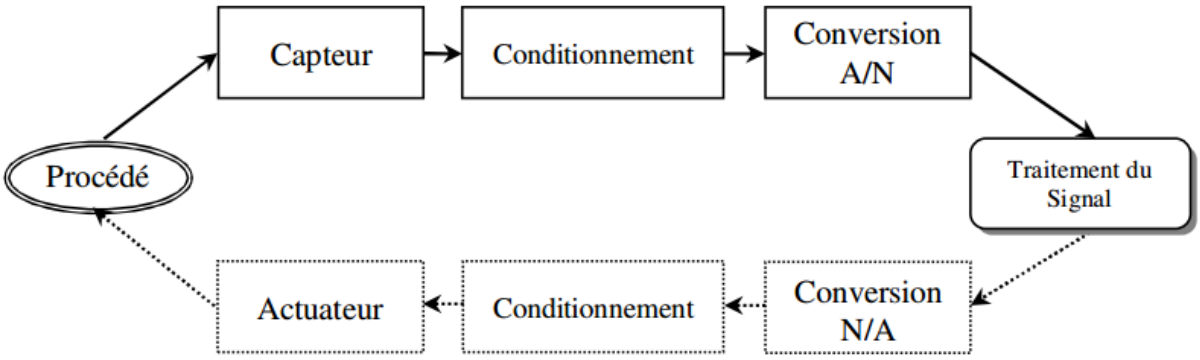



**Figure 1.2** Acquisition des données et actionnement.

Un capteur est à qualifier de *smart* lorsqu'il exploite un traitement numérique piloté par un microprocesseur embarquée quelque soit son apport en termes de services. Tandis qu'un capteur sera *intelligent* lorsqu'il sera capable en plus de participer au système de contrôle, permis par une interface de communication bidirectionnelle. Il est également capable d'envoyer sa mesure à la demande ou de manière systématique à destination du système qui devra l'exploiter. En outre, ce système doit être reconfigurable et capable d'effectuer l'interprétation de données nécessaires, diagnostic avancé, la fusion de données provenant de multiples capteurs et la validation des données locales et recueillies à distance. Le capteur intelligent contient donc une fonctionnalité de traitement embarquée qui fournit des ressources de calcul pour effectuer des tâches de détection et d'actionnement plus complexes avec des applications de haut niveau. Cette différence est illustrée par la figure 1.3 [82] [84] [85] [86].

t

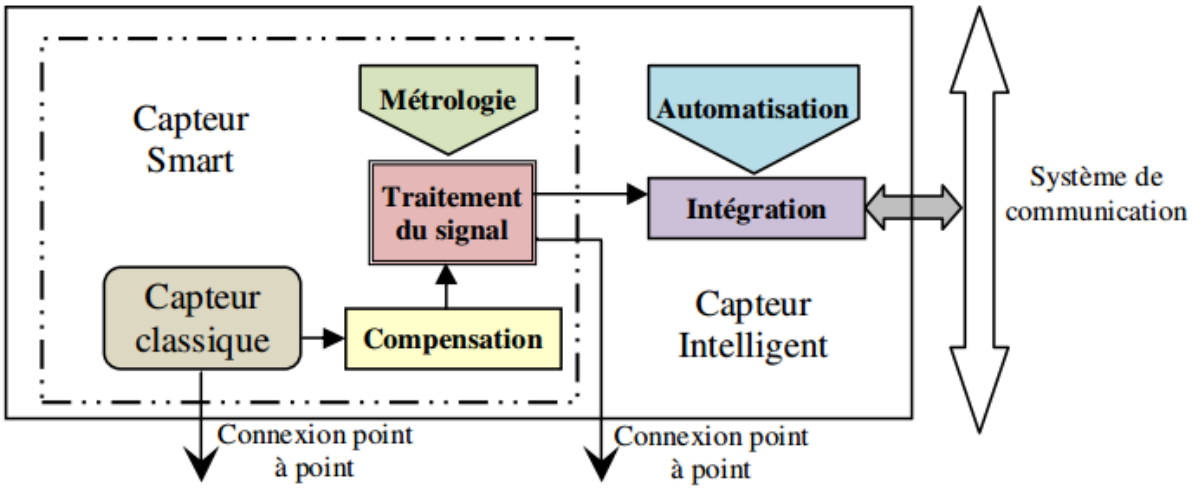



**Figure 1.3** Architecture générale d'un capteur intelligent.

### 1.2.5.1 Architecture matérielle d'un instrument intelligent

Un instrument intelligent doit pouvoir intégrer les fonctionnalités d'un capteur intelligent et celles d'un actionneur intelligent pour tendre vers plus de généricité. La figure 1.4 illustre une proposition de fonctionnalités d'un instrument intelligent générique.

Des fonctions identifiées précédemment, l'architecture matérielle d'un instrument intelligent peut être déduite. Elle comprend :

Une chaîne principale d'interface avec le processus :

- dans le cas du capteur : une chaîne d'acquisition, constituée d'un ou plusieurs corps d'épreuve associés à des conditionneurs ; on retrouve ici les composants de base du capteur, permettant de convertir une grandeur physique en un signal électrique, le plus souvent analogique,
- dans le cas de l'actionneur : une chaîne d'actionnement, constituée par l'élément actif de l'actionneur (l'organe réglant), un moyen de transmission (une chaîne cinématique), un convertisseur (tel qu'un moteur, assurant la transformation d'énergie) ;

Une chaîne de traitement numérique de l'information, incluant :

- une interface vers le processus ; pour la mesure : multiplexeur, amplificateur, CAN, échantillonneur-bloqueur…, ou pour l'actionnement, un préactionneur ayant le rôle de modulateur d'énergie électrique,
- un organe de calcul [microcontrôleur, microprocesseur, DSP Digital Signal Processor), …] et les périphériques associés (mémoires),
- une interface de communication qui assure la communication bidirectionnelle vers le système d'automatisation, via un réseau de terrain,
- une alimentation assurant une stabilisation des tensions nécessaire à l'électronique ; une batterie peut être envisagée pour maintenir certaines activités en l'absence de source d'énergie extérieure (horloge, mémoire…).

À cela et associé aux éléments précédents, il faut adjoindre :

- des dispositifs sensoriels ou moteurs ;
- des capteurs internes ayant un rôle de contrôle de l'état de l'instrument (exemple : couple d'un moteur dans une plage spécifiée), de validation des opérations effectuées (exemple : roue codeuse) ou de compensation (exemple : température interne utilisée pour corriger les dérives des convertisseurs analogiques/ numériques)
- des possibilités d'actions internes utilisées dans le cas de capteur actif (où une modulation de l'énergie apportée permet d'adapter la mesure à une précision voulue), à des fins de test (où une commutation bascule entre le corps d'épreuve et une source de référence permettant un réétalonnage) ou enfin pour maintenir l'instrument dans un état souhaité (tel qu'un ventilateur asservi permettant une régulation de température de l'électronique).

La figure 1.4 présente l'organisation de ces éléments au sein d'un instrument intelligent. On y distingue :

- Trois emplois de corps d'épreuve, chargés de mesurer les phénomènes physiques du processus (grandeur primaire et d'influence), de surveiller le comportement des ensembles moteurs (préactionneur, actionneur, transmission) et d'établir des mesures technologies à des fins de contrôle de l'instrument (alimentation, température électronique…) ;

- La chaîne d'acquisition comprenant des filtres, des conditionneurs, un multiplexeur et un amplificateur et un CAN (convertisseur analogique numérique), dont leur commande permet de sélectionner la source et de s'adapter la mesure au niveau requis. Des sources de référence permettent un contrôle de cette chaîne et, éventuellement, un étalonnage en ligne ;

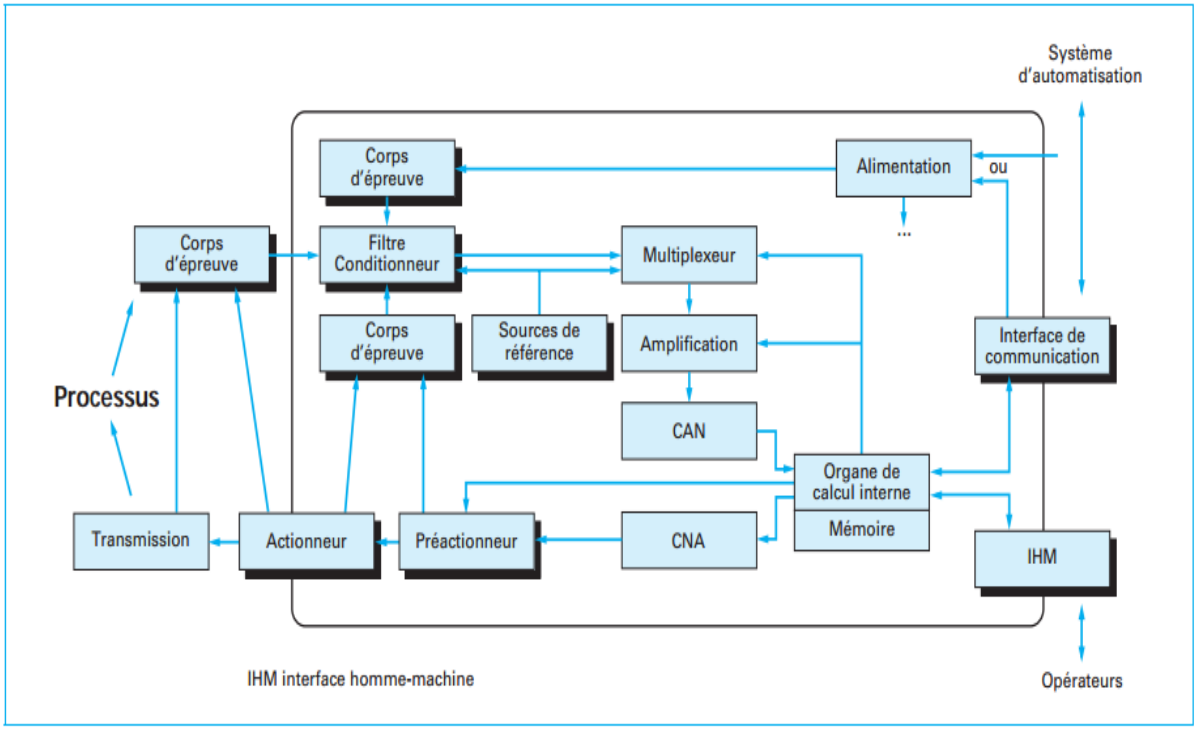



**Figure 1.4**: Architecture matérielle d'un instrument intelligent (capteur et actionneur) [55].

- la chaîne d'actionnement comprenant éventuellement un CNA (convertisseur numérique analogique), un préactionneur, un actionneur, une transmission de l'énergie
- l'organe de calcul associé à une mémoire ;
- l'alimentation avec plusieurs sources d'énergie possible ;
- les interfaces avec les opérateurs ou avec les autres équipements du système.

Selon le cas, tout ou partie des éléments présentés seront implantés. Ainsi dans la configuration minimale, un capteur intelligent comprend : un transducteur, un conditionneur, une interface de communication ; l'alimentation pouvant être fournie par le support de communication.

D'un point de vue matériel, un capteur intelligent se compose alors de quatre unités montrées sur la figure 1.5 [81] [82] [85] [87] [88] :

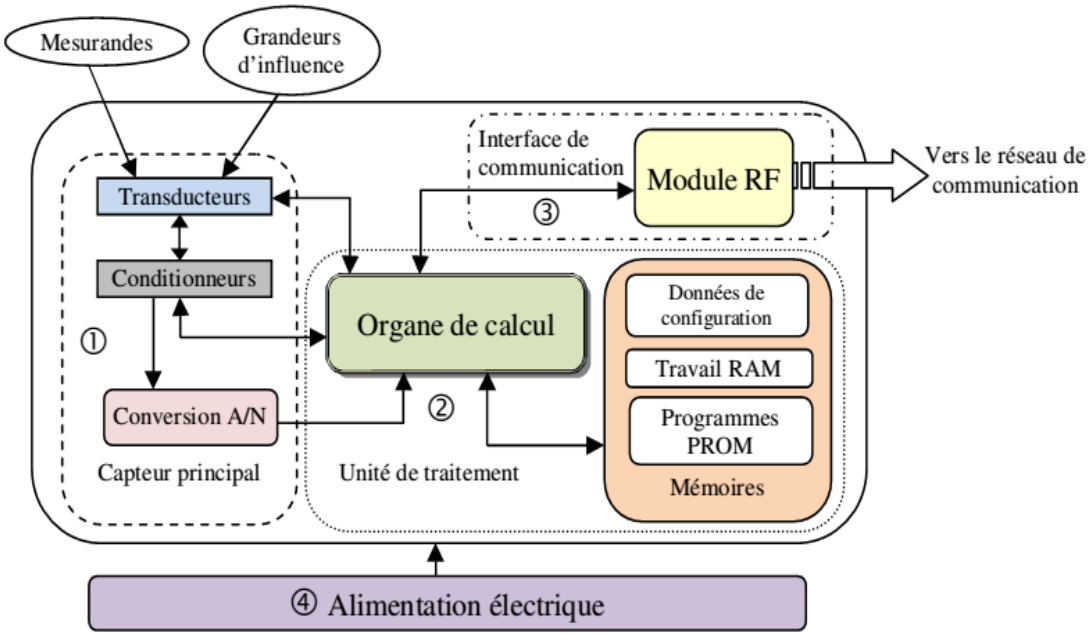



**Figure 1.5** Architecture matérielle d'un capteur intelligent.

- **Un *capteur principal*** spécifique au mesurande avec ses dispositifs d'acquisition et de numérisation du signal de sortie du capteur : transducteur, conditionneur qui adapte le signalélectrique en vue de sa transmission, multiplexeur, amplificateur, échantillonneur bloqueur, convertisseur analogique/numérique ;
- **Un *organe de calcul numérique*** (microcontrôleur, microprocesseur, dsPIC) servant au calcul et à la gestion de l'acquisition, la correction des effets des grandeurs d'influence au moyen de paramètres stockés en mémoire PROM, la linéarisation, le diagnostic des capteurs ;
- **Une *interface de communication*** assurant la liaison du capteur à un calculateur central et permettant un dialogue bidirectionnel de données numériques avec le système d'automatisation.

Cette interface radio ou filaire est caractérisée par :

• plage fréquentielle ;

• technique de modulation ;

• type de multiplexage ;

• type de canal ;

• étalement de spectre ;

- **Une *alimentation*** assurant une stabilisation des tensions est nécessaire à l'électronique de l'instrument. Une batterie peut être envisagée pour maintenir certaines activités en l'absence de source d'énergie extérieure (horloge, mémoire,…).

Le transducteur permet de détecter toute variation de la grandeur physique en entrée du capteur. Sa conception est étroitement liée au domaine d'application pour lequel le capteur sera utilisé. L'interface de communication permet également au capteur intelligent de recevoir les informations du système nécessaires à l'élaboration de sa mesure et à sa validation. Elle peut également être utilisée dans les phases de calibration et de mise en service de l'équipement dans son environnement du travail.

Donc un capteur intelligent peut être considéré comme un véritable système embarqué autonome, qui devra posséder son propre système d'exploitation lui permettant de coopérer au sein d'une organisation.

L'architecture matérielle générique d'un actionneur intelligent est présentée dans la figure 1.6 suivante :

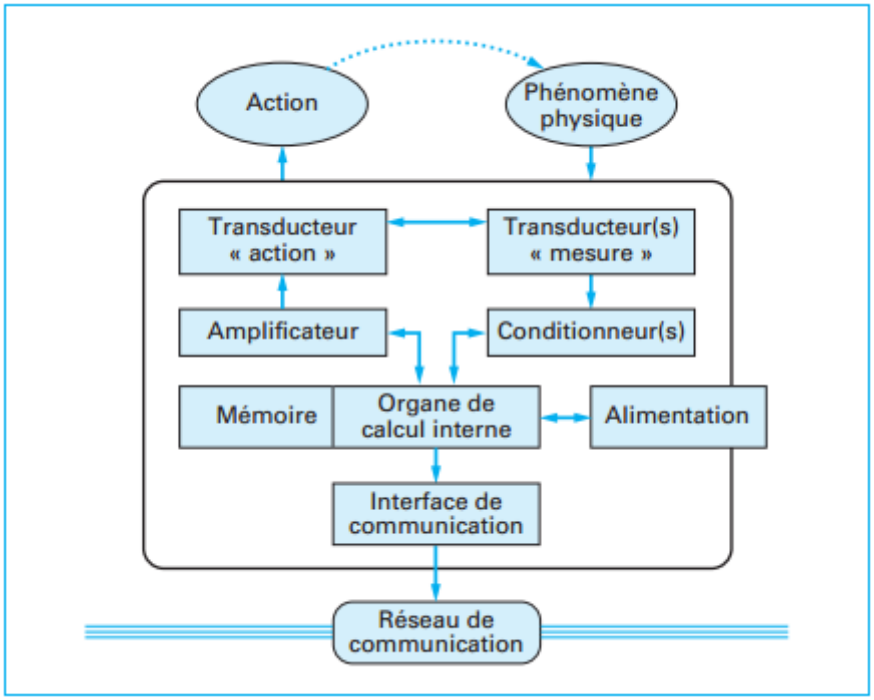



**Figure 1.6** Architecture matérielle générique d'un actionneur intelligent.

D'un point de vue matériel, un instrument intelligent se compose alors de trois sous-ensembles :

- une unité de traitement numérique (c'est-à-dire une unité de calcul associée à de la mémoire) ;
- une interface de communication permettant un dialogue bidirectionnel numérique avec le reste du système ;
- un organe d'actionnement pour l'actionneur.

Pour conclure, un capteur ou un actionneur intelligent peut être considéré comme un véritable « système embarqué », qui devra posséder son propre système d'exploitation lui permettant de coopérer au sein d'une organisation plus complexe [97] [55].

#### 1.2.5.2 Architecture fonctionnelle d'un instrument intelligent

Les capacités internes de calcul et de traitement assurées par un système à microprocesseur ainsi que sa faculté d'échange bidirectionnel d'informations avec le médium externe de communication ont permis à l'instrument intelligent d'intégrer les fonctions du système d'information, ainsi que de nouvelles fonctionnalités susceptibles d'améliorer la qualité de la mesure et de la commande. Diverses fonctionnalités ont été proposées pour un instrument intelligent. Robert [80] a proposé les fonctionnalités de configuration, de communication, de mesure, de calcul et de validation. De même, Meijer [90] inclut trois fonctionnalités; compensation, calcul et communication tandis que Tian [91] suggérait que ce qui s'appelle un capteur intelligent devrait avoir les fonctions de compensation, validation, fusion de données (data-fusion) et communication. Mekid [89] propose les fonctionnalités de compensation, de traitement (processing), de communication, de validation, d'intégration, de fusion de données et de nouvelles fonctionnalités peuvent être ajoutées telles que l'autocalibration.

La figure 1.7 illustre une proposition de fonctionnalités d'un instrument intelligent générique.

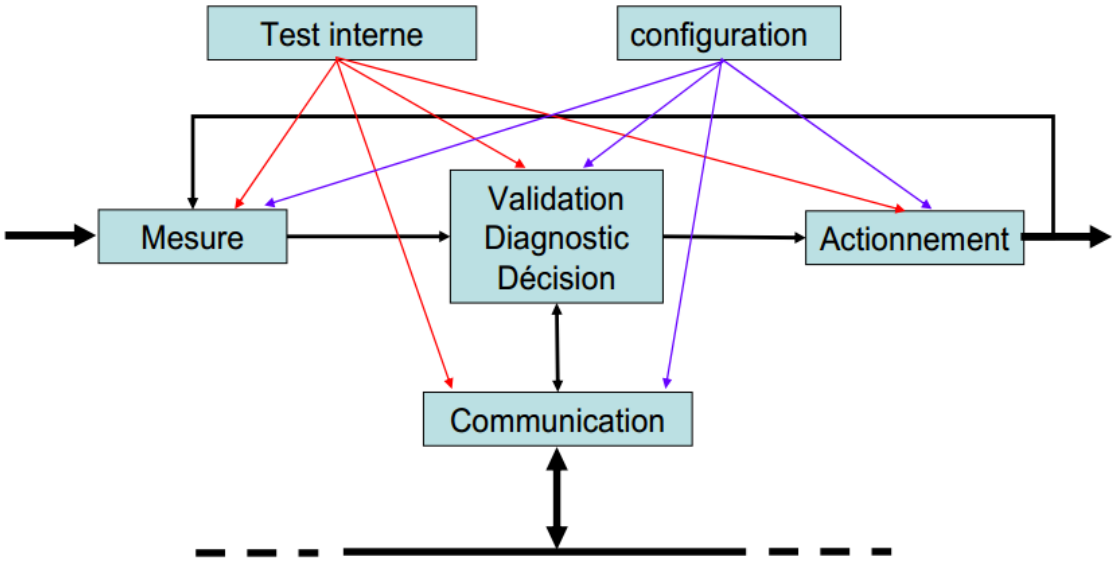



**Figure 1.7** Architecture fonctionnelle d'instruments intelligents [1].

La figure ci-dessus fait apparaître le schéma classique Mesure-Décision-Action dans la description de tout système automatisé. L'instrument intelligent est doté également d'un logiciel qui est implanté dans son nœud pour pouvoir intégrer toutes ces fonctionnalités. L'instrument intelligent par l'implantation de ces fonctionnalités s'octroie des capacités de calcul et des moyens de communication. L'intelligence impliquera plus de renseignements dans le nœud instrument et une distribution accrue d'informations [1].

La fonctionnalité principale qui caractérise l'intelligence à notre sens est celle représentée par le trio *validation, diagnostic, décision*. Elle est le cœur de l'instrument intelligent et les autres fonctionnalités (autres la mesure et l'actionnement) concourent à son établissement et constituent des moyens au service de cette fonctionnalité. La capacité des capteurs de communiquer avec d'autres parties du système de contrôle permettra d'avoir plus de renseignements au nœud capteur (donc d'intelligence) et une distribution accrue du contrôle. Cette fonctionnalité se rapporte donc à la correction des conditions environnementales et à leur validation, à la réalisation des fonctions de diagnostic et à la prise de décisions. C'est cette fonctionnalité qui sera à la base de l'amélioration de la sûreté de fonctionnement qui liée étroitement à l'amélioration de la crédibilité par la validation, la détection de défauts et la prise de décision adéquate [1].

La fonctionnalité compensation consiste en l'amélioration des mesures pour une meilleure précision en considérant les erreurs dans le système.

La fonctionnalité intégration concerne l'intégration de l'élément de sensation par l'informatique et la communication sur un boîtier simple pour éliminer le raccordement de fils entre les composants, pour réduire la taille globale des capteurs, pour employer de façon optimale l'énergie et pour réduire des coûts [89].

La fonction de la fusion de données est de s'assurer que seulement l'information la plus appropriée est transmise entre les capteurs [91].

### 1.2.6 Les types de capteurs intelligents

Il existe actuellement deux grandes catégories de capteurs définis en fonction du format de l'information qu'ils produisent et manipulent. Ces deux types de capteurs sont les capteurs analogiques et les capteurs numériques. Un système intermédiaire, le concentrateur numérique, permet de concilier certains avantages de ces deux types de capteurs. Ils vont être décrits ci-dessous :

#### 1.2.6.1 Les capteurs analogiques

Les capteurs analogiques, actuellement les plus répandus dans l'industrie, reçoivent, traitent et restituent les informations sous forme analogique, c'est-à-dire sous la forme d'une grandeur pouvant varier continûment. Ils sont généralement constitués d'un transducteur, d'un conditionneur, d'un transmetteur et d'une alimentation dans la figure 1.8.

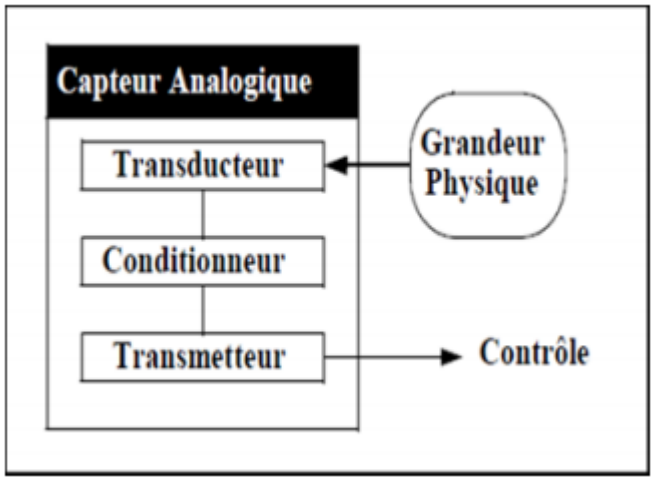



**Figure 1.8** Schéma interne d'un capteur analogique [77].

Le transducteur est en interaction avec le phénomène physique, il produit une grandeur relative à ce phénomène. Cette grandeur peut être une capacité variant en fonction d'une pression, ou dans le cas d'une thermistance, être une résistance variant en fonction de la température à mesurer.

Le conditionneur convertit la grandeur précédente en un signal généralement électrique, parfois optique selon la technologie utilisée. Il l'amplifie avec un gain et dans une gamme déterminée, et effectue des opérations de traitement tels que le filtrage ou la compensation.

A partir du signal produit par le conditionneur, le transmetteur engendre une grandeur dont la nature dépend du médium de communication utilisé. Si le médium est une paire de fils torsadés utilisée en boucle de courant, il produit un courant variant de 4 mA à 20 mA (en cas d'utilisation de la norme 4-20 mA). Le médium peut aussi être un câble coaxial, une fibre optique ou les ondes hertziennes. Il est alors possible de transférer plusieurs informations simultanément en modulant plusieurs porteuses (l'exemple le plus connu est le transfert d'images vidéo qui comportent des informations de luminosité et de chrominance). L'alimentation est interne (batterie), externe ou mixte (alimentation externe plus adaptation interne). Certains capteurs sont associés à un actionneur ayant pour fonction de rendre l'environnement favorable à la mesure. Par exemple, la mesure du coefficient de réflexion d'une surface impose que celle-ci soit éclairée. Certains capteurs chimiques ont des conditions très strictes de fonctionnement en température, et doivent posséder un système de chauffage ou de climatisation. Afin de restreindre notre champ d'investigation, nous ne traiterons pas des actionneurs dans la suite de ce document. Il faut toutefois savoir que pour des raisons de simplicité ou d'efficacité, l'actionneur peut avoir une partie commune avec le transducteur ou le conditionneur [77].

#### 1.2.6.2 Les capteurs numériques

Bénéficiant des progrès technologiques en matière de micro-électronique, ce type de capteur peut engendrer et recevoir des informations numériques. Il possède au minimum un transducteur, un conditionneur, un convertisseur analogique/numérique et un organe de communication. Bien que ces quatre organes puissent constituer une configuration minimale de capteur numérique, l'intérêt de produire ce format d'information réside dans la possibilité d'inclure un processeur dans le capteur. Cette intégration est d'autant plus aisée qu'il existe actuellement des micro-contrôleurs incluant un processeur, de la mémoire, des interfaces

d’entrées-sorties et parfois des convertisseurs analogiques-numériques [77] présenté dans la figure 1.9.

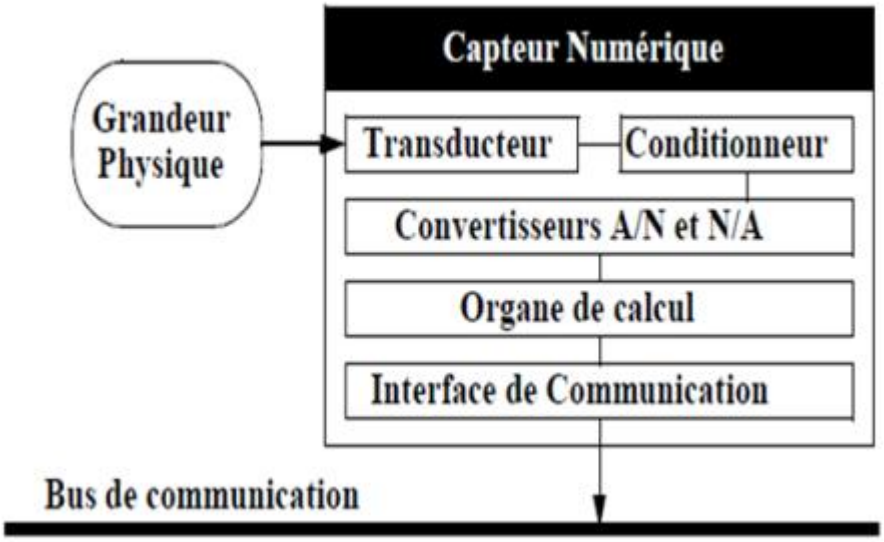



**Figure 1.9** Schéma interne d’un capteur numérique [77].

Le transducteur joue le même rôle que précédemment. IL produit une grandeur relative au phénomène physique observé.

Le conditionneur produit une grandeur, tension ou durée, compatible avec l’entrée du convertisseur, c’est-à-dire dans une gamme imposée par ce dernier. Il dispose d’un filtre anti repliement. Le convertisseur analogique-numérique fournit en sortie des valeurs numériques codées sur 8 à 16 bits. Sa fréquence d’échantillonnage est au moins le double de la fréquence de coupure du filtre antirepliement. Bien qu’il n’en porte jamais le nom, un compteur associé à une horloge peut aussi être considéré comme un convertisseur A/N. Dans ce cas, la grandeur d’entrée est une durée et non une amplitude. Selon ce principe, un interféromètre associé à un compteur fournit une mesure numérique du déplacement.

Le processeur est associé à une mémoire permanente (ROM) contenant la connaissance figée du capteur, et une mémoire vive (RAM) contenant, en général, des informations et connaissances à caractère évolutif. Il permet l’implémentation d’un grand nombre de fonctions telles que le traitement du signal, l’identification, l’auto-adaptation ou la prise de décisions.

L’organe de communication permet la connexion à un réseau informatique adapté aux contraintes du temps réel. Il s’occupe de la gestion du protocole de communication imposé

par le bus. IL permet d'abandonner les connexions fil-à-fil rapidement coûteuses et d'une fiabilité limitée.

On peut remarquer que cette structure est bien plus souple que la précédente. Elle permet l'implantation de nombreuses fonctions et offre de grandes possibilités de configuration [77].

### 1.2.7 Classification des capteurs intelligents

Le choix d'un capteur à intégrer pour une application dépend de la grandeur physique à surveiller. Dans de nombreux domaines (industrie, recherche scientifique, services, loisirs, etc.), on a besoin de contrôler de nombreux paramètres physiques (température, force, position, vitesse, luminosité, etc.). Le capteur est l'élément indispensable à la mesure de ces grandeurs physiques.

La classification des capteurs peut être également basée sur les méthodes qui s'appliquent sur les phénomènes électriques et qui se servent pour convertir les mesurandes physiques en signaux électriques. Les capteurs peuvent être classifiés en deux types : actif et passif [81] [85] [87] [57].

#### 1.2.7.1 Capteurs actifs

Un capteur actif est un système de mesure qui nécessite une source d'énergie embarquée, la plus fréquemment assurée par une batterie. Cela pour la réalisation de la phase de traitement pendant laquelle le signal est filtré, amplifié et converti en un format compatible et exploitable. Pour ce type, le capteur doit non seulement mesurer des propriétés physiques mais doit également effectuer des opérations additionnelles via des circuits de traitement et de communication intégrés. Cet instrument est surtout utilisé pour assurer des mesures continues en temps réel [87] [88] [57].

#### 1.2.7.2 Capteurs passifs

Les capteurs passifs sont des dispositifs qui ne possèdent pas de source d'énergie embraquée et présentent l'avantage d'être facilement intégrables. Ce type de capteur est utilisé dans des applications spécifiques qui nécessitent des unités de mesure miniatures,

passives, de grande précision et fiables. Leur objectif est d'assurer des mesures à distance des grandeurs physiques [87] [88].

### 1.2.8 Modèles génériques d'instruments intelligents

Plusieurs modèles génériques d'instruments intelligents ont été proposés afin de prendre en compte les nouvelles fonctionnalités. Tous ces modèles peuvent être classés en deux catégories selon qu'ils cherchent à spécifier l'instrument intelligent par son modèle interne ou externe.

#### 1.2.8.1 Le modèle interne

Le modèle interne d'un instrument intelligent décrit les fonctions qu'il doit intégrer pour réaliser les services qu'en attendent les utilisateurs. Il définit la structure et la nature des traitements implantés. Dans ce sens, il s'adresse plus particulièrement au concepteur [92].

La méthode SADT (Structured Analysis and Design Technique) ou "Analyse Structurée et Technique de Conception" est une méthode de spécification fonctionnelle analysant un système ou un produit, de manière descendante, modulaire et hiérarchique [94]. La méthode SADT permet la modélisation formelle du concept d'instruments intelligents. Cette méthode descriptive permet la représentation de l'architecture, des différentes activités de l'instrument, des flux de données. Cependant, nombre d'objectifs, besoins et contraintes restent exprimés en langage informel, c'est-à-dire par du texte. Ces descriptions génériques doivent donc être complétées par d'autres modèles de représentation. Des formalismes tels que les réseaux de Petri ou les graphes d'états sont bien adaptés à la représentation des aspects temporels et de la gestion des activités. Une autre approche pour le modèle interne a été la modélisation du capteur intelligent par une approche orientée objet à partir de la méthode OMT (Object Modeling Technique) [93] [96]. Le but de cette méthode semi-formelle est de fournir trois modèles pour décrire les aspects statiques, dynamiques et fonctionnels. La variété des modèles, leur richesse sémantique et leur représentation graphique permet d'exprimer n'importe quel concept en restant très abstrait. Cette capacité d'abstraction peut être vue comme une force mais aussi comme une faiblesse. En effet, elle est source d'incohérences et va à l'encontre de certains principes de la construction du logiciel (validation dès l'analyse, automatisation de la construction).

#### 1.2.8.2 Le modèle externe

Le modèle externe d'un instrument intelligent caractérise, d'un point de vue externe, l'ensemble des services prévus par le concepteur. Ceux-ci sont commandés à l'aide de requêtes et selon un protocole de commande spécifique appartenant au modèle. La structuration de ce modèle est donc indispensable pour assurer l'interopérabilité et l'interchangeabilité d'un ensemble d'instruments constituant une application. Ce modèle s'adresse donc plus particulièrement à l'utilisateur [94] [96].

En ce qui concerne le modèle externe, l'approche USOM (USer Operating Mode) est la plus répandue [94]. Dans ce type d'approche, l'instrument intelligent peut être considéré par un utilisateur comme une entité proposant des services, lesquels manipulent des variables et font appel à un ensemble de ressources. Ainsi, la notion de service est définie en adoptant une représentation de l'architecture matérielle de l'instrument intelligent identique à celle d'une machine informatique classique. Par ailleurs, et afin d'éviter la réalisation par l'utilisateur d'actions incompatibles, les différents services d'un instrument sont regroupés en sous ensembles cohérents dits modes d'utilisations [96].

## 1.3 Systèmes d'automatisation à intelligence distribuée

Les systèmes d'automatisation à intelligence distribuée (SAID) sont une extension des systèmes automatisés. Ils se sont développés au même temps que les nouvelles technologies.

### 1.3.1 Concept des systèmes d'automatisation à intelligence distribuée

Les installations d'automatismes présentent habituellement une architecture centralisée dans la figure 1.10, comprenant un ensemble de capteurs et d'actionneurs raccordés par des liaisons directes via des cartes d'entrées/sorties numériques ou analogiques à une unité de traitement (automate programmable industriel, système numérique de contrôle-commande…). Cette architecture permet l'échange point à point d'une seule information entre les équipements et l'unité centrale :

- ✓ un capteur fournit une mesure ;
- ✓ un actionneur reçoit une consigne.

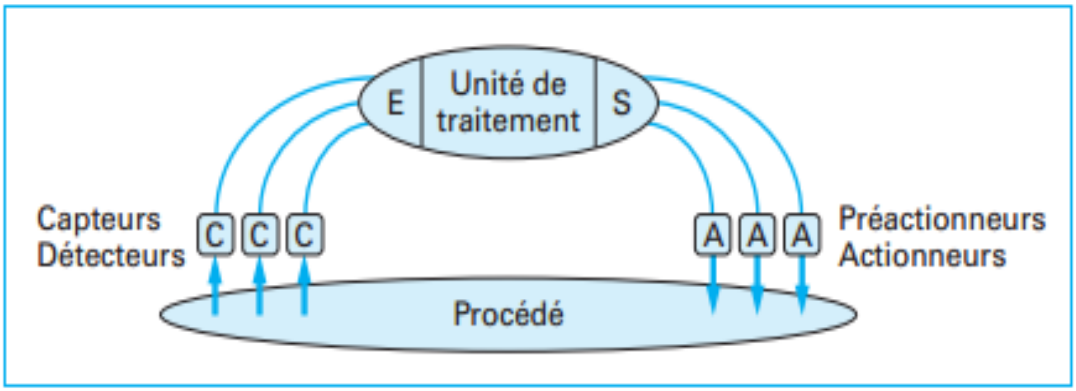



**Figure 1.10** Automatisme centralisé.

L'augmentation croissante du nombre d'informations nécessaires au contrôle des processus industriels a conduit au développement d'unités de traitement de plus en plus performantes, capables de traiter rapidement un grand nombre d'informations. Consécutivement, la conception des systèmes est devenue de plus en plus difficile, les temps et coûts de câblage ont augmenté, la mise au point des installations s'est complexifiée [55] [97].

Une première évolution est apparue avec l'introduction des bus de terrain [55] [97] *Réseaux locaux industriels* : ils ont permis de déporter les entrées/sorties (E/S) digitales et analogiques, et de réduire les coûts et temps de câblage présenté dans la figure1.11. L'ensemble des informations est toujours traité dans l'unité centrale, qui conserve les traitements complexes.

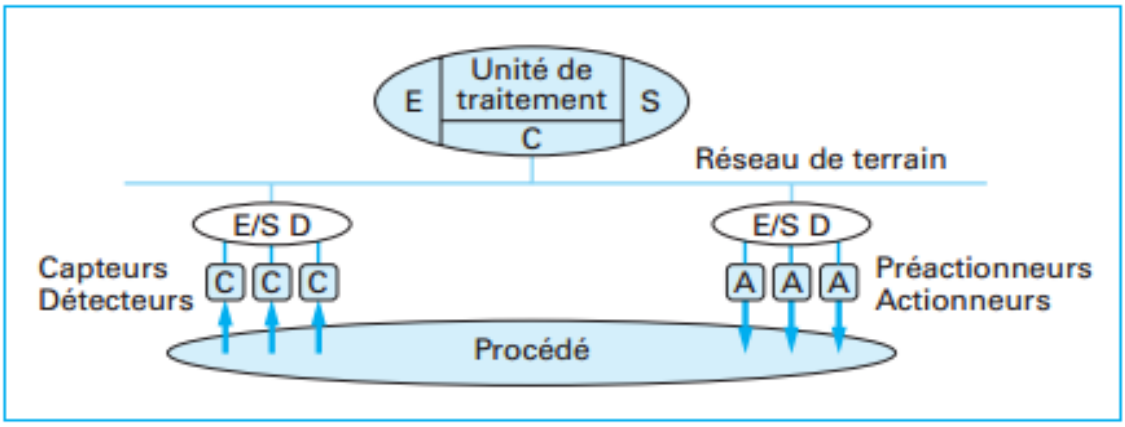



**Figure 1.11** Automatisme centralisé et entrées/sorties déportées (E/SD)

On cumule dans ce cas des inconvénients en termes de temps de réponse, gestion simultanée de nombreuses variables, cohérence temporelle de l'information… L'étape suivante dans l'évolution des automatismes a été de répartir l'unité centrale et de rapprocher

les traitements au plus près des équipements. On parle alors de systèmes automatisés à intelligence distribuée (SAID) schématisé par la figure 1.12. Les traitements locaux peuvent être implantés directement dans les capteurs et actionneurs intelligents ou dans des petites unités de traitements (microautomate par exemple) gérant un sous-ensemble de capteurs et actionneurs.

Ces systèmes sont composés d'instruments intelligents (capteurs et actionneurs intelligents), d'unités de traitement et de réseaux de communication. Les SAID se présentent sous forme d'architecture distribuée contrairement à l'architecture centralisée classique permettant ainsi une délocalisation de quelques tâches de traitements au plus près du processus grâce au réseau de communication [55].

Les principaux composants d'un système d'automatisation sont les capteurs qui déterminent l'état actuel du processus sous contrôle, les régulateurs qui établissent les nouvelles commandes et les actionneurs qui exécutent les nouvelles commandes sur le processus. Les liaisons entre différents constituants des systèmes d'automatisation sont assurées soit par des boucles classiques ou par des réseaux de communication.

Les systèmes d'automatisation à intelligence distribuée sont constitués d'instruments intelligents qui sont des capteurs et des actionneurs intelligents. Ils constituent avec les systèmes de communication les constituants de base des SAID, ils sont dotes d'une intelligence manifestée par une capacité de traitement local offrant des fonctions autres que les fonctions primitives (mesurer pour un capteur et agir pour un actionneur). Un système d'automatisation à intelligence distribuée illustrant la répartition de l'unité centrale et le rapprochement des traitements au plus près des équipements. Ces traitements sont implantés directement dans les capteurs et actionneurs intelligents ou dans des petites unités de traitements gérant un sous-ensemble de capteurs et actionneurs.

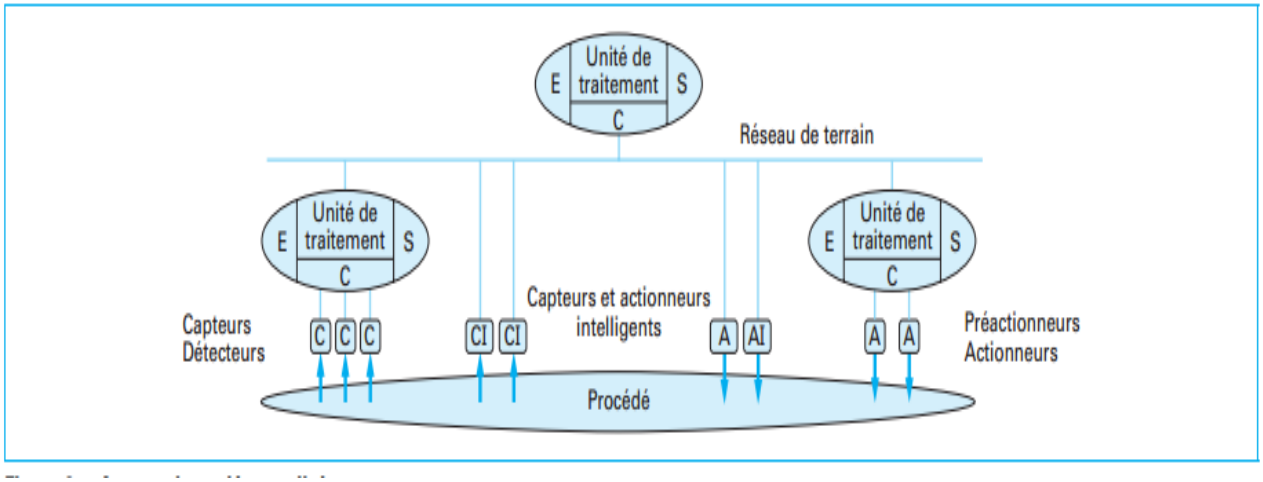



**Figure 1.12** système d'automatisation à intelligence distribuée.

Les architectures distribuées sont la base de beaucoup de systèmes industriels. Ces architectures distribuées offrent non seulement un câblage réduit et une simplification de la maintenance mais elles offrent aussi une occasion d'implémentation de lois de commande sophistiquées. L'automatisme décentralisé permet une réelle distribution des fonctions au plus près des capteurs/actionneurs. L'intelligence peut être intégrée directement dans les C/A.

### 1.3.2 Caractéristiques des SAID

Les SAID sont caractérisés par un ensemble de propriétés telles que la structuration hybride qui est reflétée par la coexistence de systèmes continus et de systèmes échantillonnés et d'autres à événements discrets, les reconfigurations offertes par le caractère dynamique de ces systèmes, l'intégration de fonctionnalités relatives à la présence d'un réseau de communication dans un système de commande.

D'après [3], un système automatisé est un système hybride avec des sous-systèmes continus, échantillonnés et des sous-systèmes à événements discrets. Cette propriété est retrouvée au sein même d'un constituant du système qui est par exemple le capteur qui envoie périodiquement sa mesure et peut envoyer une information de dépassement d'un seuil par exemple.

Les reconfigurations offrent un caractère dynamique des SAID durant le cycle de vie [3]. Les changements par rapport à l'état initial peuvent être très rapides, tels que l'arrêt de fonctionnement d'un composant ou encore lents tels que la diminution de vitesse d'action d'un actionneur subissant une usure [97].

Outre le caractère hybride et la propriété de dynamisme caractérisant les systèmes d'automatisation à intelligence distribuée, ces systèmes utilisent un réseau de communication. Celui-ci rend complexe leur analyse conception. Quelques facteurs influent sur le fonctionnement de ce type de systèmes tels que le délai de transmission de données qui peut dans certains cas déstabiliser le système, les éventuelles pertes de trames de communication et leur impact sur le système et le réseau peut être considéré comme défaillant, l'ordre d'arrivée des trames de communication peut aussi différer de l'ordre de l'émission et les informations peuvent aussi être tronquées en plusieurs trames [97].

Néanmoins, ces systèmes associant des réseaux de communication offrent des ameliorations par rapport aux systèmes classiques telles que la réduction du câblage, l'augmentation de la flexibilité, le potentiel de communication des informations sur la supervision ou le diagnostic, la coopération des composants au sein d'une architecture distribuée [3].

### 1.3.3 Le SAID et la sûreté de fonctionnement

L'incorporation des instruments intelligents dans les boucles de sécurité nous mène vers une sécurité intelligente et les systèmes deviennent des systèmes instrumentés de sécurité à intelligence distribuée (SISID). La justification de l'usage de ces instruments dans les applications de sécurité n'est pas complètement avérée. Ces instruments disposent d'atouts importants utiles à ce type d'applications [1]. Ces systèmes disposent d'un nombre important de traitements et d'une augmentation de la complexité contrairement aux systèmes classiques qui ne sont pas dotés d'intelligence. Ceci rend la tâche de l'évaluation de la sûreté de fonctionnement plus difficile à appréhender.

L'influence de l'instrumentation intelligente sur l'attribut sécurité de la sûreté de fonctionnement qui consiste à se préserver de situations dangereuses ou catastrophiques, est contrastée. Elle contribue à une amélioration dans les applications où la sécurité est critique par la mise en place de moyens d'autodiagnostic et de validation mais elle peut introduire de nouveaux modes de défaillance affectant la sécurité par l'emploi de dispositifs non éprouvés plus complexes et disposant d'éléments logiciels.

Ainsi, les nouvelles fonctionnalités incorporées offrent des possibilités d'autodiagnostic et une mise en place d'arc réflexe permettant l'amélioration de la sécurité. De par leur complexité, ces systèmes peuvent également être sources de défaillance.

D’une façon générale, la sûreté de fonctionnement des systèmes automatisés reste difficile à évaluer. Cette difficulté réside essentiellement dans la complexité à modéliser l’évolution comportementale du système. Cette complexité peut revêtir différents aspects [1] dont:

- ✓ la taille
- ✓ l’aspect technologique
- ✓ le nombre d’états
- ✓ la complexité stochastique
- ✓ le nombre de composants
- ✓ les effets de l’intégration
- ✓ le modèle fonctionnel
- ✓ le modèle structurel

## 1.4 Conclusion

Le présent travail aborde une étude bibliographique sur les instruments intelligents, et les systèmes d’automatisation à intelligence distribuée, leurs différences aux systèmes classiques, leurs atouts ainsi que leurs complexités.

Quant à l’évaluation de la sûreté de fonctionnement de ce type de systèmes, elle n’est pas triviale. La difficulté de l’évaluation de la sûreté de fonctionnement de ce type de systèmes trouve son origine dans l’existence de difficultés liées à la modélisation. Les incidents ou accidents qui perturbent le système durant son cycle de vie sont les résultats de défaillances liées aux entités qui constituent le système et son environnement. Nous nous tournons vers une étude de l'état de l'art de la sûreté de fonctionnement, leurs paramètres, et leurs principes méthodes d'analyse dans le chapitre suivant.

# CHAPITRE 2
# LA SURETE DE FONCTIONNEMENT : ANALYSES ET CONCEPTS

# Chapitre 2

# La Sûreté de Fonctionnement : analyses et concepts

## 2.1 Introduction

La Sûreté de Fonctionnement s'est développée principalement à cause de l'évolution des systèmes critiques industriels et se caractérise par l'analyse des défaillances et de leurs conséquences. Cela passe par une analyse exhaustive du fonctionnement du système ainsi que des exigences que le système doit vérifier.

Au cours de ce chapitre, il est fait état de l'art de la sûreté de fonctionnement ainsi que les différentes notions et méthodes en vue de traiter l'aspect de sûreté de fonctionnement des systèmes instrumentés intelligents. Dans un premier temps, différents éléments de la SdF sont présentés tels que la fiabilité avec ses différentes formes, la maintenabilité, la disponibilité et la sécurité ainsi que indicateurs définissant les différents temps de la SdF. Dans un deuxième temps, un cadre générique sur les principales méthodes d'analyse de la sûreté de fonctionnement est présenté.

## 2.2 Historique de la sûreté de fonctionnement

Les problèmes de Sûreté de Fonctionnement existent depuis très longtemps, dès qu'un système a pu défaillir ou tomber en panne [23] [27], [3]. A partir des années 1930, l'analyse intuitive, la durée de vie et les taux de défaillance sont exploités dans plusieurs domaines tels que les systèmes mécaniques, l'électricité, le transport aérien et les grandes catastrophes [26] [1]. Dans les années 1940-1950, la théorie de la fiabilité est née [30].L'ingénieur s'appuiera sur l'amélioration de la qualité dans le domaine de l'aéronautique et l'électronique militaires,

où les techniques de fiabilité commencèrent à se développer à travers la fiabilité prévisionnelle [23].

Dans les années 1960, le concept de maintenance fait son apparition [31]. H. A. Watson des laboratoires Bell [32] met au point la méthode dite des arbres de défauts qui permet de décrire les aléas du fonctionnement de systèmes complexes [39].

En 1962, l'Académie des Sciences accueille le mot "fiabilité" dans sa terminologie [3]. Ensuite, dans les années 1970-1980, les premiers travaux sur la fiabilité des logiciels [23] [33] commencent et de nombreuses études sont menées dans le domaine du nucléaire.

La décennie 80 voit l'approfondissement dans plusieurs directions :

- collecte de données de fiabilité,
- mise au point de nouvelles méthodes d'analyse de la fiabilité et de la disponibilité des systèmes (par exemple les réseaux de Pétri),
- méthodes de prise en compte du facteur humain (méthode HCR : "Human Cognitive Response technique", méthode HEART: "Human Error Assessment and Reduction Technique", ...etc).

Par la suite, les techniques de sûreté de fonctionnement vont convenablement se diffuser et se prolonger dans d'autres domaines tels que la chimie, la pétrochimie, le transport ferroviaire, l'automobile, le traitement et l'épuration de l'eau et l'ensemble des grands secteurs industriels.

La finalité de tout cet effort est d'aboutir à des systèmes et des équipements sûrs et efficaces pour les fabricants afin de minimiser les temps d'arrêt et assurer une disponibilité maximale de leurs équipements.

## 2.3 Quelques notions

### 2.3.1 La sûreté de fonctionnement

La Sûreté de Fonctionnement (notée SdF) (en anglais, « dependability ») [25] est définie par la Commission Électrotechnique Internationale (CEI) comme l’ensemble des propriétés qui décrivent la disponibilité et les facteurs qui la conditionne : fiabilité, maintenabilité et logistique de maintenance est l'aptitude d'une entité à satisfaire une ou plusieurs fonctions requises dans des conditions données [25]. Elle est définie par Villemeur [34] comme la

science des défaillances. Au sens plus strict, la sûreté de fonctionnement est l'aptitude d'une entité à assumer une ou plusieurs fonctions requises dans des conditions données [37].

Au sens de la norme CEI 50 (191) [23] [35], la sûreté de fonctionnement recouvre les concepts de fiabilité, maintenabilité et disponibilité (ou FMD). L'équivalent Anglo-Saxons est le terme dependability, (reliability, maintainability, availability) [25] souvent désigné par l'acronyme RAM. La sécurité est souvent traitée à part. Cependant, l'acronyme RAMS (FMDS en français) est utilisé pour désigner l'ensemble des activités liées à ces quatre concepts présenté dans la figure 2.1.

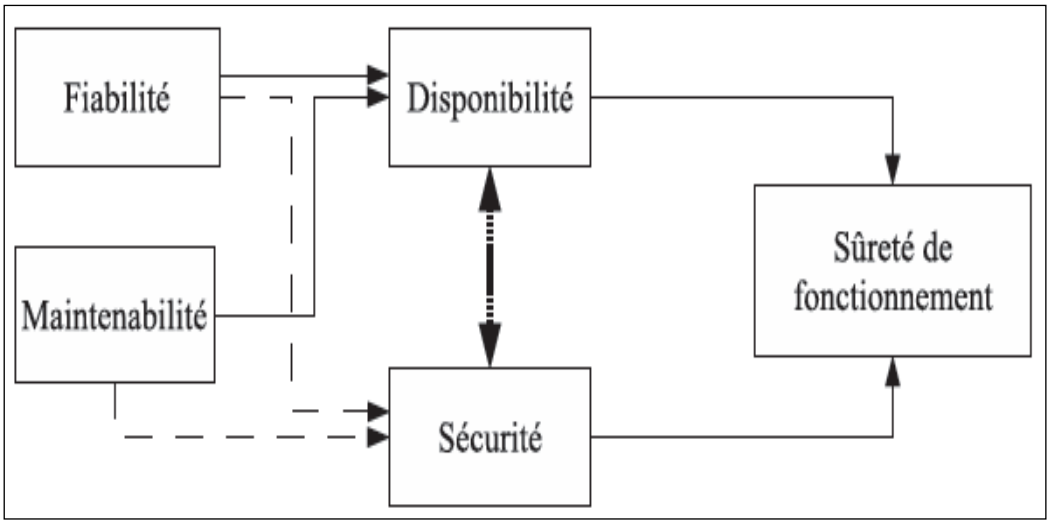



**Figure 2.1** La sûreté de fonctionnement.

### 2.3.2 Fiabilité

La fiabilité (en anglais, « reliability ») [25], Villemeur [34] exprime que la fiabilité est l'aptitude d'un système à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps déterminé. Cette aptitude se mesure par la probabilité qu'une entité réalise une fonction requise dans des conditions données pendant une période de temps donnée [36] [23].

A l'instant t, la fiabilité se mesure par la probabilité que l'entité *E* accomplisse une fonction requise dans les conditions données pendant l'intervalle de temps [*0, t*] [24]. Ainsi,

$$R(t) = P[E \text{ soit non défaillante sur } [0, t]] \qquad (2.1)$$

Ou

$$R(t) = P[E \text{ soit non défaillante sur } [t_1, t_2]] \qquad (2.2)$$

L'aptitude contraire est la probabilité de défaillance de l'entité, quelque fois appelée défiabilité. On écrit :

$$\bar{R}(t) = 1 - R(t) \qquad (2.3)$$

Un équipement est fiable s'il subit peu d'arrêts pour pannes. La notion de fiabilité s'applique :

- ❖ Au système réparable => équipement industriel ou domestique.
- ❖ A des systèmes non réparables => lampes, composants donc jetables.

La fiabilité d'un équipement dépend de nombreux facteurs tel que montré sur le schéma de la figure 2.2 :

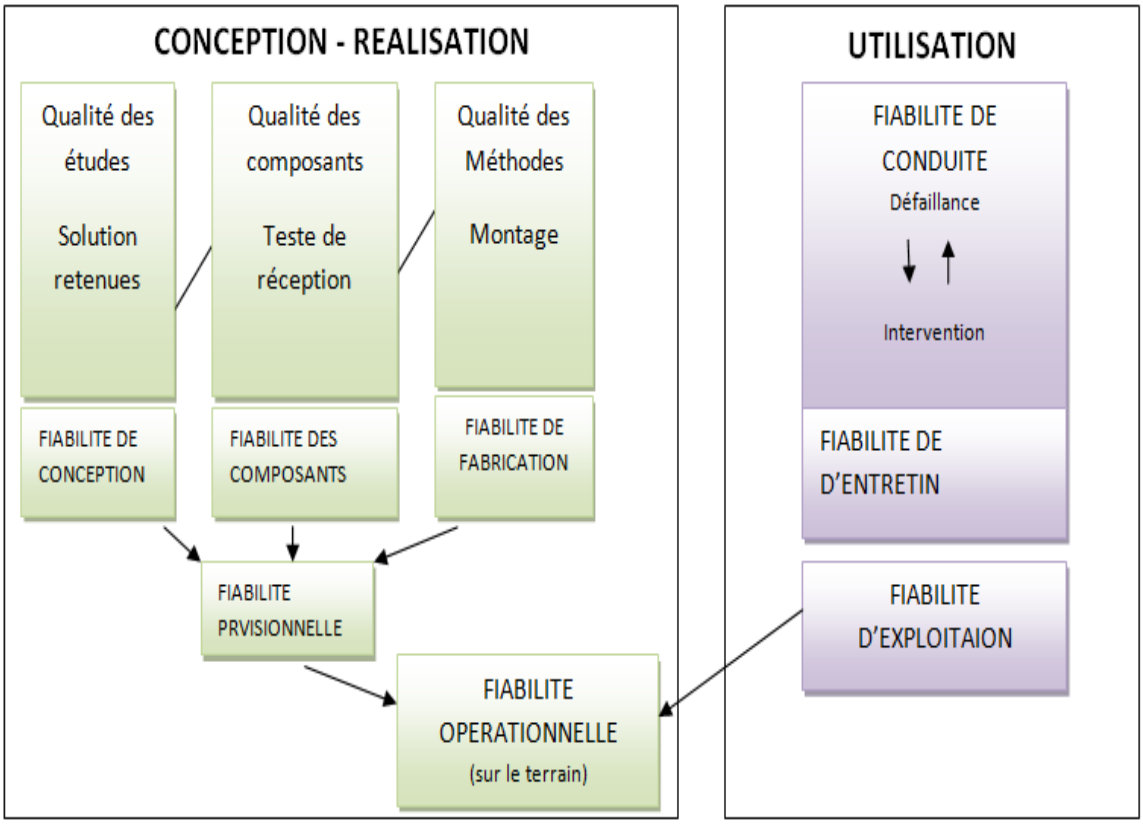



**Figure 2.2** Différentes formes de la fiabilité.

On distingue plusieurs types de fiabilité (termes spécifiques) :

- ➢ La fiabilité opérationnelle (observée ou estimée) déduite de 1' analyse d'entités identiques dans les mêmes conditions opérationnelles à partir de 1'exploitation d'un retour d'expérience.
- ➢ La fiabilité prévisionnelle (prédite) correspondant à la fiabilité future d'un système et

établie par son analyse, connaissant les fiabilités de ses composants.

- La fiabilité extrapolée déduite de la fiabilité opérationnelle par exploitation ou interpolation pour des conditions ou des durées différentes.
- La fiabilité intrinsèque ou inhérente qui découle directement des paramètres de conception sans un niveau de fiabilité au plus égal à la fiabilité intrinsèque.

La fiabilité d'un instrument intelligent peut tirer avantage de certaines fonctionnalités numériques lorsque, par exemple, des corrections d'erreurs de mesure et des auto-ajustages permettent de prévenir l'occurrence de dérives ou d'autres défauts ou défaillances qui apparaissent avec la durée. De plus, certains défauts peuvent en partie être compensés par l'utilisation de techniques de tolérance aux défauts (reconfigurations). Lorsque des défaillances se produisent au bout d'une échéance quasidéterministe (par exemple, épuisements de ressources), on évoquera alors plus justement des questions de durabilité (aptitude d'une entité à accomplir une fonction requise, dans des conditions données d'emploi et de maintenance, jusqu'à ce qu'un état limite soit atteint [IEC90]) qui peut, elle aussi, bénéficier de reconfigurations fonctionnelles en ligne du instrument intelligent (par exemple, pour une gestion optimisée des ressources). La communication numérique est, quant à elle, souvent considérée comme plus fiable que l'analogique. En revanche, la plus grande quantité d'électronique, d'unités programmées, et de logiciels, (nécessaires aux traitements des données, aux calculs, à l'exécution des fonctionnalités, à la communication, etc.), implique de nouvelles causes et de nouveaux modes de défaillance qui sont généralement difficiles à connaître et à appréhender. De plus, chaque défaut ou défaillance peut affecter plusieurs fonctions d'instrument intelligent, ainsi que plusieurs informations transmises par celui-ci. Enfin, la communication numérique fait encore l'objet de plusieurs interrogations au regard de la fiabilité, notamment face aux causes communes de défaillance.

### 2.3.3 Maintenabilité

La maintenabilité (en anglais, « maintainability »)[25] est l'aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données avec des procédures et des moyens prescrits [34] [23].

Elle est généralement mesurée par la probabilité que la maintenance d'une entité *E*, soit achevée au temps *t*, sachant que l'entité est défaillante au temps t = 0.

L'évaluation de cette probabilité est liée à la manière dont est effectuée la remise en état de fonctionnement de l'entité.

$$M(t) = P[E \text{ est réparé sur } [0, t]] \quad (2.4)$$

### 2.3.4 Disponibilité

la disponibilité (en anglais, « availability »)[25], C'est l'aptitude d'un système à être en état d'accomplir une fonction requise, dans des conditions données, à un instant donné [34] [24]. Elle est généralement mesurée par la probabilité qu'une entité *E* soit en état d'accomplir une fonction requise dans des conditions données à l'instant *t*.

$$A(t) = P[E \text{ non défaillante à l'instant } t] \quad (2.5)$$

Cette caractéristique est appelée disponibilité instantanée. L'aptitude contraire sera dénommée indisponibilité ; sa mesure est notée $\bar{A}(t)$ :

$$\bar{A}(t) = 1 - A(t) \quad (2.6)$$

### 2.3.5 Sécurité

Nous définirons ici la sécurité (en anglais, « safety ») [25] comme l'aptitude d'un système à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques [34] [24]. En fait, le concept de sécurité est probablement le plus difficile à définir et à évaluer, car il englobe des aspects très divers. Cependant, la norme EN 292 – 1 [38] sur la sécurité des machines donne cette définition :

"C'est l'aptitude d'une machine à accomplir sa fonction, à être transportée, installée, mise au point, entretenue, démontée et mise au rebut dans les conditions d'utilisation normales spécifiées dans la notice d'instructions, sans causer de lésions ou d'atteinte à la santé."

Les bénéfices apportés à la sécurité, par les fonctionnalités numériques au sein des capteurs intelligents, résident principalement dans les capacités plus complètes d'autodiagnostics, qui permettent ainsi une meilleure détection des défauts et défaillances. De plus, des états « sûrs » peuvent être définis avec plus de détails et obtenus plus justement par des reconfigurations. La centralisation de certaines informations, permise par la communication numérique, peut également contribuer à une maîtrise des risques plus efficace. En revanche, les capteurs intelligents deviennent de plus en plus des « boites noires », qu'il convient donc d'évaluer avec des outils appropriés [25].

### 2.3.6 Défaillance

Une défaillance (en anglais, « failure ») [25], Selon Villemeur [34], une défaillance est la cessation de l'aptitude d'une entité à accomplir une fonction requise. La défaillance d'une entité résulte de causes qui peuvent dépendre des circonstances liées à la conception, la fabrication ou l'emploi et qui ont entraîné la défaillance. Enfin, le mode de défaillance est l'effet par lequel une défaillance est observée.

Le taux de défaillance peut être rapproché de la probabilité pour que le composant soit défaillant à l'instant t+dt sachant qu'il n'est pas défaillant à l'instant t. On le note λ et il s'exprime à partir de la fiabilité selon la relation suivante :

$$\lambda(t) = -\frac{d}{dt}(log\, R(t)) \qquad (2.7)$$

### 2.3.7 Reconfiguration

C'est l'action de modifier la structure d'un système qui a défailli, de telle sorte que les composants non-défaillants permettent de délivrer un service acceptable, bien que dégradé. [40].

## 2.4 Les temps caractéristiques pour la Sûreté de Fonctionnement

Les différents temps caractérisant la SdF se définissent en fonction de leur état de fonctionnement : avant défaillance, entre défaillance, entre défaillance et réparation, etc. Ces temps dépendent des probabilités d'occurrences des divers événements comme les défaillances et les réparations des composants. Ce sont des variables aléatoires que l'on cherche à caractériser par leurs espérances mathématiques [26].

Certains indicateurs vont caractériser le fonctionnement prévu du système, tels que le MTTF, le MDT et le MUT.

- Le MTTF (Mean Time To [first] Failure) est la durée moyenne de fonctionnement avant défaillance, espérance mathématique de la durée de fonctionnement avant défaillance [26]. L'expression du MTTF est :

$$MTTF = \int_0^{\infty} R(t)dt \qquad (2.8)$$

- Le MDT est le temps moyen séparant la survenance d'une panne et la remise en état opérationnel du système. Il se décompose en plusieurs phases lesquelles sont présentées par la figure 2.3 :
    - durée de détection de la panne (1);
    - durée de diagnostic de la panne (2);
    - durée d'intervention jusqu'au début de la réparation (3);
    - durée de la réparation (4);
    - durée de remise en service du système (5).

- Le MUT est le temps moyen qui sépare une remise en service opérationnelle du système de la survenance de la panne suivante.

Ces deux derniers indicateurs ne sont pertinents que dans le cas de systèmes réparables. Leur somme MUT+MDT représente le temps moyen qui sépare deux pannes consécutives du système. On le note MTBF, comme Mean Time Between Failures.

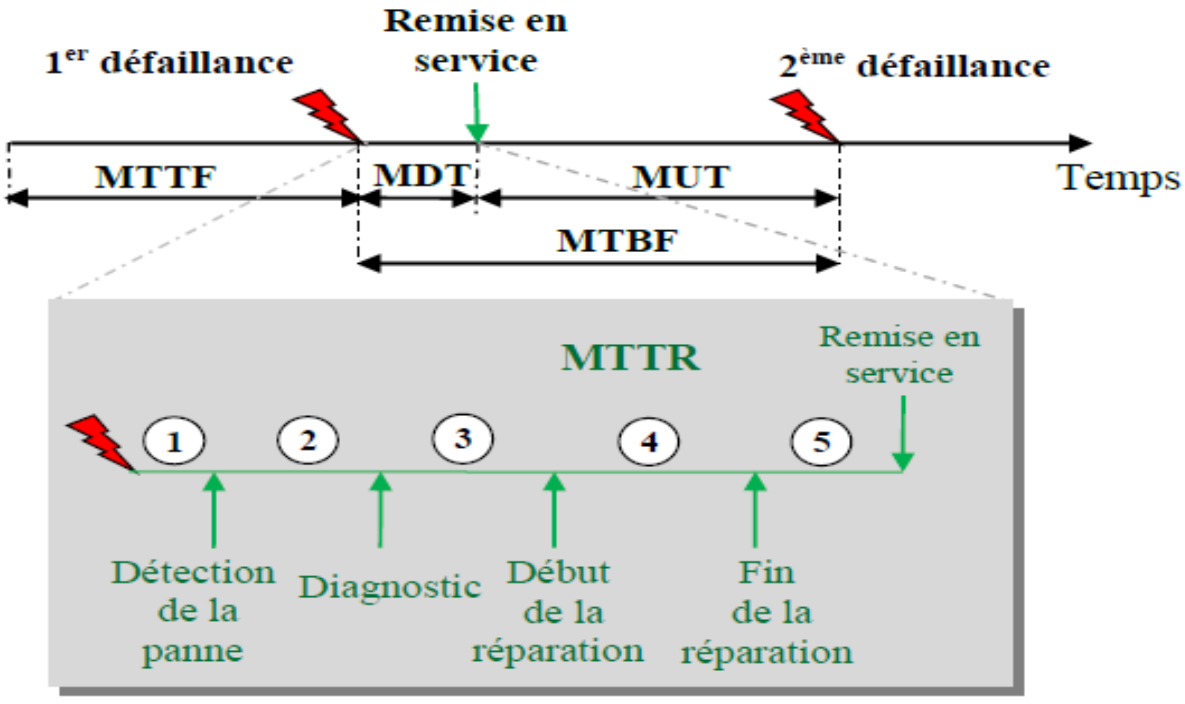



**Figure 2.3** Quelques indicateurs de la sûreté de fonctionnement.

## 2.5 Enjeu de la sûreté de fonctionnement

L'enjeu de la sûreté de fonctionnement est d'identifier les risques au plus tôt dans la phase de développement du produit. Plus une erreur de conception est découverte tardivement, plus le risque technique induit peut être lourd et entraîner des surcoûts et des retards considérables pour le projet. L'apparition du risque peut notamment conduire à la mise en cause de la sécurité des personnes et des biens, à la dégradation de l'environnement, à la perte de fonctions.

La sûreté de fonctionnement est une activité d'ingénierie système. Elle peut être qualitative ou quantitative. La part qualitative correspond à l'optimisation des études et elle représente environ 70% de l'activité totale. Les 30% restants représentent la partie quantitative consacrée à la maîtrise des risques avant fabrication à partir des architectures déjà élaborées. C'est donc une phase d'optimisation des architectures des systèmes et de leur mise en œuvre de façon à maximiser, à moindre coût, leur robustesse aux aléas.

En résumé, l'analyse de la sûreté de fonctionnement est une action de réduction des risques et donc du coût à l'achèvement. Elle s'exerce essentiellement pendant les premières phases des projets, jusqu'à la mise en production [37].

## 2.5 Quelques approches d'analyse

D'après la figure 2.4, les principales méthodes d'analyse de la sûreté de fonctionnement sont les suivantes :

- L'Analyse Fonctionnelle (AF).
- L'Analyse des Modes de défaillances, de leurs Effets et de leurs Criticité (AMDEC).
- L'arbre de défaillance (AdD),
- Le réseau de pétri (RdP),
- Le Bloc Diagramme de Fiabilité (BDF).
- .....

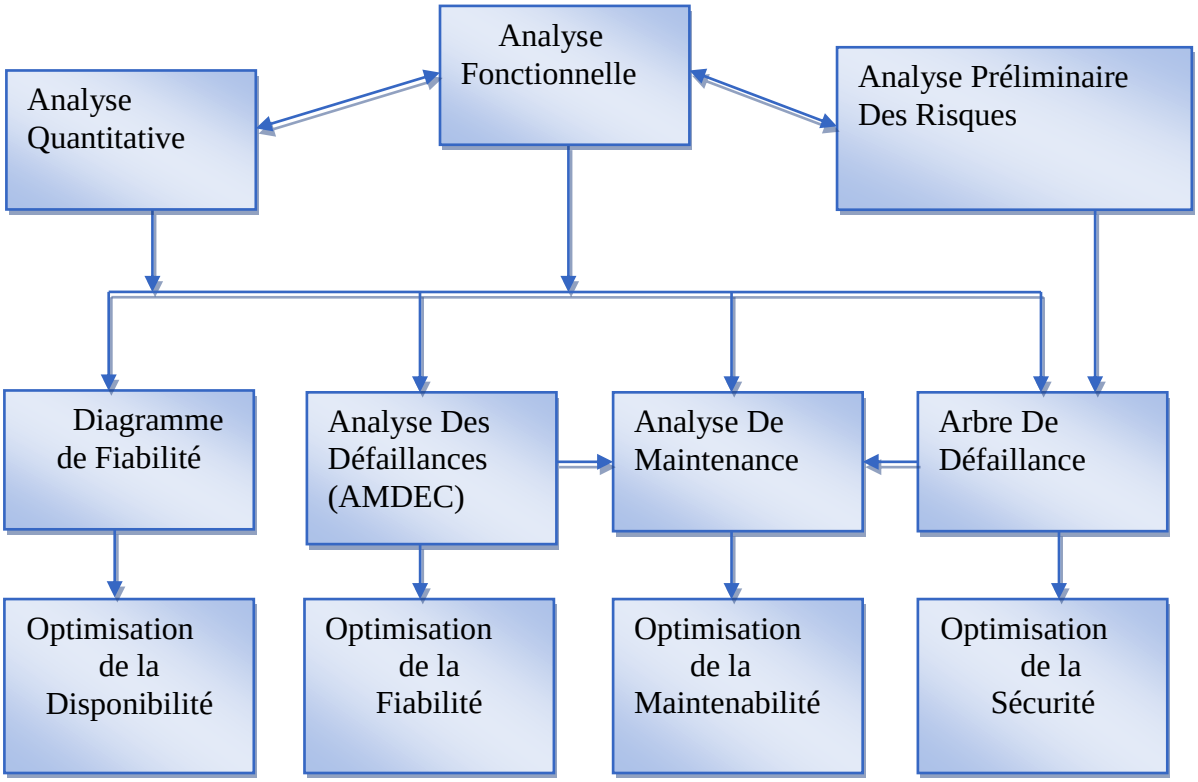



**Figure 2.4** Méthodes d'analyse de la SdF.

### 2.5.1 L'Analyse Fonctionnelle (AF)

L'analyse fonctionnelle est une étape qui s'utilise au début d'un projet pour créer ou améliorer un produit ou un service. Pour analyser les défaillances d'un système, il est nécessaire auparavant de bien identifier à quoi doit servir ce système : c'est à dire de bien identifier toutes les fonctions que le système doit remplir durant sa vie de fonctionnement et de stockage [3].

D'après la norme (AFNOR NF X 50-151), 1'analyse fonctionnelle est une démarche qui consiste à rechercher, ordonner, caractériser, hiérarchiser et / ou valoriser les fonctions du produit (matériel, logiciel, processus, service) attendues par 1'utilisateur. Une analyse fonctionnelle, précède donc une étude de sûreté de fonctionnement. Une première analyse fonctionnelle dite externe permet de définir avec précision les limites matérielles du système étudie, les différentes fonctions et opérations réalisées par le système ainsi que les diverses configurations d'exploitation. L'analyse fonctionnelle interne permet de réaliser une

décomposition arborescente et hiérarchique du système en éléments matériels et/ou fonctionnels. Elle décrit également des fonctions dans le système [3].

### 2.5.2 L'Analyse préliminaire des risques

Selon la norme CEI-300-3-9 (CEI 300-3-9, 1995), l'**Analyse Préliminaire des Risques** (APR) « est une technique d'identification et d'analyse de la fréquence du danger qui peut être utilisée lors des phases amont de la conception pour identifier les dangers et évaluer leur criticité ». Elle est réalisée après 1'analyse fonctionnelle. Elle a pour but d'établir une liste aussi exhaustive que possible des incidents ou accidents pouvant avoir des conséquences sur la sécurité du personnel ou du matériel. Un autre objectif de l'APR est d'évaluer la gravite des conséquences liées aux situations dangereuses et les accidents potentiels [3].

La méthode permet de recenser les dangers et déduire ensuite tous les moyens et toutes les actions correctrices permettant d'éliminer ou de maitriser les situations dangereuses et les accidents potentiels. Il est recommandé de commencer 1'APR dès les premières phases de la conception. Cette analyse sera vérifiée et complétée au fur et à mesure de l'avancement dans la réalisation de système. L'APR permet de mettre en évidence les événements redoutés critiques qui devront être analysés en détail dans la suite de 1'étude de sûreté de fonctionnement, en particulier par la méthode des arbres de défaillances [29].

### 2.5.3 L'Analyse des Modes de défaillances, de leurs Effets et de leurs Criticités (AMDEC)

L'AMDEC a été développée initialement par 1'armée américaine. La référence Militaire MIL-P-1629, intitule "Procédures pour 1'Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticités", date du 9 Novembre 1949. C'est une extension de 1'analyse des Modes de Défaillance et de leurs Effets (AMDE) [34].

Cette méthode était employée comme une technique d'évaluation des défaillances afin de déterminer la fiabilité d'un équipement et d'un système. L'AMDEC à été employée pour la première fois dans les années 1960 dans le domaine de 1'aéronautique pour 1'analyse de la sécurité des avions. La mise en œuvre s'est longtemps limitée à 1'utilisation dans le cadre d'études de fiabilité du matériel. Son utilisation s'est depuis largement répandue à d'autres secteurs d'activités telles que 1'industrie chimique, pétrolière ou le nucléaire. De fait, elle est essentiellement adaptée à 1'étude des défaillances de matériaux et d'équipements et peut

s'appliquer aussi bien à des systèmes de technologies différents (systèmes électriques, mécaniques, hydrauliques..,) qu'a des systèmes alliant plusieurs techniques [36].

L'AMDEC est une démarche inductive. Donc c'est une identification prédictive des causes de problèmes.

Cause (fait particulier) ⟹ Effet (conclusion générale)

Cependant, cette méthode a des limites qui sont :

- n'est pas une méthode de résolution de problèmes,
- ne permet pas l'étude des combinaisons de défaillances (plutôt réservée aux Arbres de Défaillances, Graphe de Markov,…),
- ne peut pas garantir l'exhaustivité de l'étude,

### 2.5.4 L'Arbre de Défaillance (AdD)

L'arbre de défaillance est une représentation graphique de type arbre généalogique. Il représente une démarche d'analyse d'événement. L'arbre de défaillance est construit en recherchant l'ensemble des événements élémentaires, ou les combinaisons d'événements, qui conduisent à un **E**vénement **R**edouté (**ER**). L'analyse par arbre de défaillances est une méthode de type déductif. Elle permet de remonter de causes en causes jusqu'aux évènements de base susceptibles d'être à l'origine de l'événement redouté [35].

Ainsi, 1'analyse par arbre des défaillances permet d'identifier les successions et les combinaisons d'évènements qui conduisent des évènements de base jusqu'à 1'événement indésirable retenu. Les liens entre les différents événements identifiés sont réalisés grâce à des portes logiques (de type « ET » et « OU » par exemple). Cette méthode utilise une symbolique graphique particulière qui permet de présenter les résultats dans une structure arborescente. A l'aide de régies mathématiques et statistiques, il est alors théoriquement possible d'évaluer la probabilité d'occurrence de l'événement final à partir des probabilités des événements de base identifiés [34]. L'analyse par arbre des défaillances d'un évènement redouté peut se décomposer en trois étapes successives :

- Définition de 1'événement redoute (ER) étudié.
- Elaboration de 1'arbre.
- Exploitation de 1'arbre.

Il existe d'autre type d'événements définis par la norme; leurs symboles ainsi que leurs significations sont répertoriés dans le tableau 2.1 :

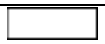
| Symbole | Nom | Signification |
|---|---|---|
|  | Rectangle | Evénement redouté ou événement intermédiaire |
|  | Cercle | Evénement intermédiaire |
|  | Losange | Evénement élémentaire non développé |
|  | Double losange | Evénement élémentaire dont le développement est à faire ultérieurement |
|  | Maison | Evénement de base survenant normalement pour le fonctionnement du système |

**Tableau 2.1** Symboles des événements.

Il existe pour les arbres de défaillances une symbolique normalisée qui permet de faire référence à des parties de l'arbre qui se répète de manière identique ou de manière semblable pour éviter de les redéfinir, le tableau 2.2 montre ces symboles avec leurs significations :

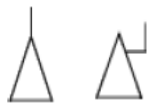
| Symbole | Nom | Signification |
|---|---|---|
|  | Triangle | La partie de l'arbre qui suit le premier symbole se retrouve **identique**, sans être répétée, à l'endroit indiqué par le second symbole. |
|  | Triangle inversé | La partie de l'arbre qui suit le premier symbole se retrouve **semblable** mais non identique à l'endroit indiqué par le second symbole. |

**Tableau 2.2** Symboles et signification.

### 2.5.5 Le Bloc Diagramme de Fiabilité (BDF)

Le bloc diagramme de fiabilité est une représentation graphique sous la forme de boite ou de blocs. Il représente une démarche d'analyse par décomposition fonctionnelle du système en sous fonction ou mission [37].

Le bloc diagramme de fiabilité est construit en recherchant la mission de chaque sous ensemble qui permet d'atteindre la mission globale du système, les boites peuvent représenter des fonctions ou des composant.

Les intérêts généraux du bloc diagramme de fiabilité sont :

- ✓ Identifier aisément les composants critiques,
- ✓ Calculer la fiabilité et mettre en évidence les évolutions défavorables et les dégradations,
- ✓ Fournir une aide à la maintenance préventive pour la détermination de périodes optimales entre interventions,
- ✓ Quantifier les gains de fiabilité à la suite d'un remplacement ou d'une modification.

Les limites de la méthode BDF sont :

- C'est un modèle reposant sur la logique et non pas sur les états,
- Modèle Statique : pas de représentation du temps ni de l'ordre entre des événements successifs,
- Hypothèse d'Independence des pannes des différents composants,
- Pas de pannes arrivant conjointement ou de pannes provoquées par la panne d'un autre composant [36].

### 2.5.6 Réseau de Pétri (RdP)

Les réseaux de Pétri constituent un outil graphique et mathématique qui permet de simuler et modéliser des systèmes dans lesquels la notion d'événements et d'évolution sont importants [39]. Ces réseaux présentent des caractéristiques intéressantes telles que la modélisation et la visualisation de comportements parallèles, de la synchronisation et partage de ressources.

Un réseau de Pétri est composé :

- d'un ensemble de place
- d'un ensemble de transitions
- d'un ensemble d'arcs qui associent les places (d'entrée) aux transitions et les transitions aux places (de sortie)
- de poids (entiers) associés aux arcs

L'état d'un réseau est défini par son marquage. Un marquage associe à chaque place un nombre entier positif, que l'on représente graphiquement par des jetons. Il existe différents types de réseaux de Pétri : temporisés, interprétés, stochastiques, colorés, continus et hybrides. C'est un outil assez général pour modéliser des phénomènes très variés [41]. Il permet notamment :

- ✓ la modélisation des systèmes informatiques,
- ✓ l'évaluation des performances des systèmes discrets, des interfaces homme-machine,
- ✓ la commande des ateliers de fabrication,
- ✓ la conception de systèmes temps réel,
- ✓ la modélisation des protocoles de communication,
- ✓ la modélisation des chaines de production (de fabrication).

## 2.6 Les études de sûreté de fonctionnement

L'étude de la sûreté de fonctionnement constitue une étape préalable indispensable à la conception d'un système sûr [31], et permet d'aider à la prise de décision, figure 2.5 :

- comprenant et identifiant les risques ;
- optimisant l'architecture et comparant des solutions différentes ;
- optimisant les moyens de soutien en comparant des solutions ;
- justifiant les choix de façon rationnelle et démontrée ;
- vérifiant la bonne atteinte des objectifs de sûreté de fonctionnement.

Elles peuvent aussi aider à l'optimisation en :

- diminuant le nombre de pannes qui seront observées durant la vie du système;
- optimisant économiquement la conception par le dimensionnement des équipements et des architectures au "juste nécessaire";
- rendant la maintenance plus ciblée et plus efficace;
- dimensionnant au plus juste les moyens de soutien nécessaires (stocks de pièces de rechange par exemple).

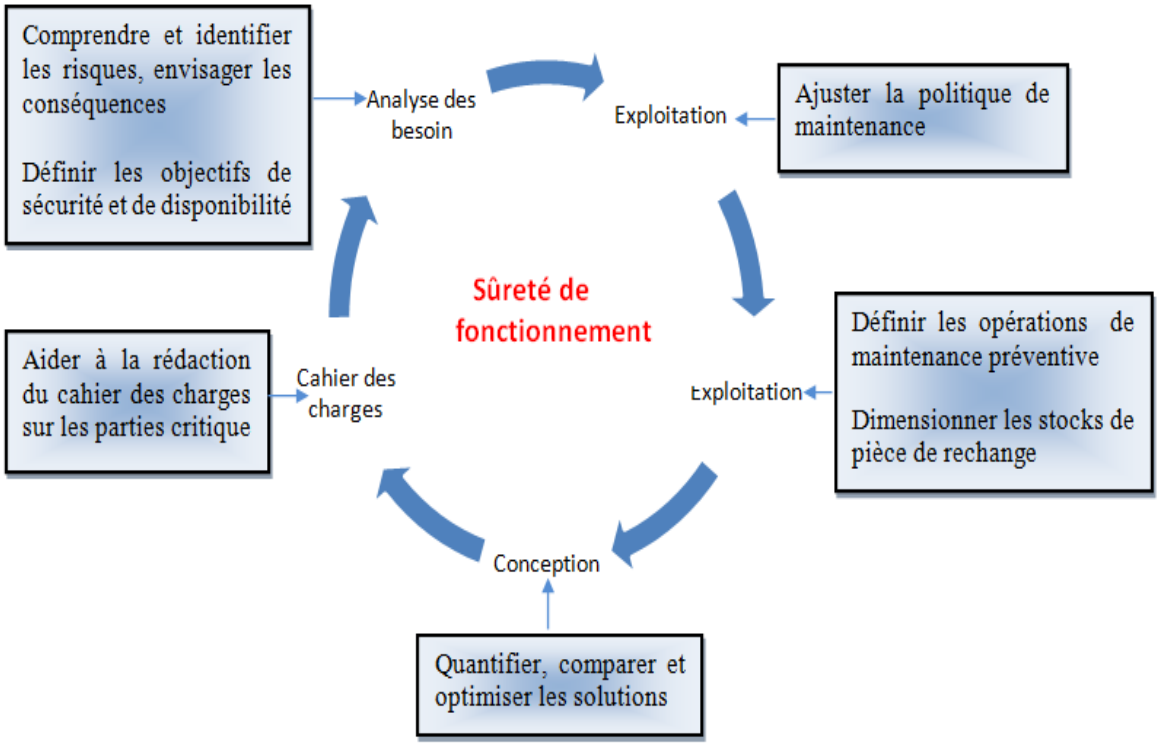



**Figure 2.5** Les études de sûreté de fonctionnement. [39]

### 2.7.1 Étape par étape

La première étape consiste à analyser rigoureusement le besoin pour comprendre et identifier l'ensemble des risques, et envisager leurs conséquences. Ensuite, des niveaux d'acceptabilité sont attribués pour ces risques (on parle d'objectifs de F, M, D et/ou S selon les systèmes).

L'identification précise de ces risques va aider à la rédaction du cahier des charges du système, précisément sur ses parties critiques. Il faudra alors imaginer des solutions techniques, des architectures adaptées qui, toutes, seront quantifiées d'un point de vue sûreté de fonctionnement, comparées entre elles et, si nécessaire, optimisées. Une fois la solution retenue, il sera nécessaire de préciser les conditions d'une exploitation la plus efficace possible en :

- définissant les opérations de maintenance préventive nécessaires pour maintenir les caractéristiques de sûreté de fonctionnement au niveau voulu, sans dégradation des équipements préjudiciable à l'une des quatre composantes;
- dimensionnant les stocks de pièces de rechange au plus juste, sans dégrader la disponibilité du système.

### 2.7.2 Études périphériques

Cette partie, s'intéresse à la recherche d'une méthodologie d'approche globale, complémentaire aux études de sûreté de fonctionnement dans les milieux industriels. Par exemple la recherche de l'optimisation des tailles de stocks de pièces de rechange a fait l'objet d'études particulières où ce souci d'optimisation est couplé avec une démarche analogue sur :

- la maintenance des équipements;
- l'ordonnancement des transports de pièces.

### 2.7.3 En pratique

L'étude de sûreté de fonctionnement comporte deux volets complémentaires représentes par la figure 2.6.

- une analyse fonctionnelle qui va détailler la manière dont le système va opérer dans toutes ses phases de vie ainsi que les autres systèmes avec lesquels il va pouvoir interagir,
- une analyse dysfonctionnelle qui vise à imaginer l'ensemble des défaillances pouvant survenir n'importe où dans le système, seules ou combinées entre elles, et à analyser l'impact de ces pannes.

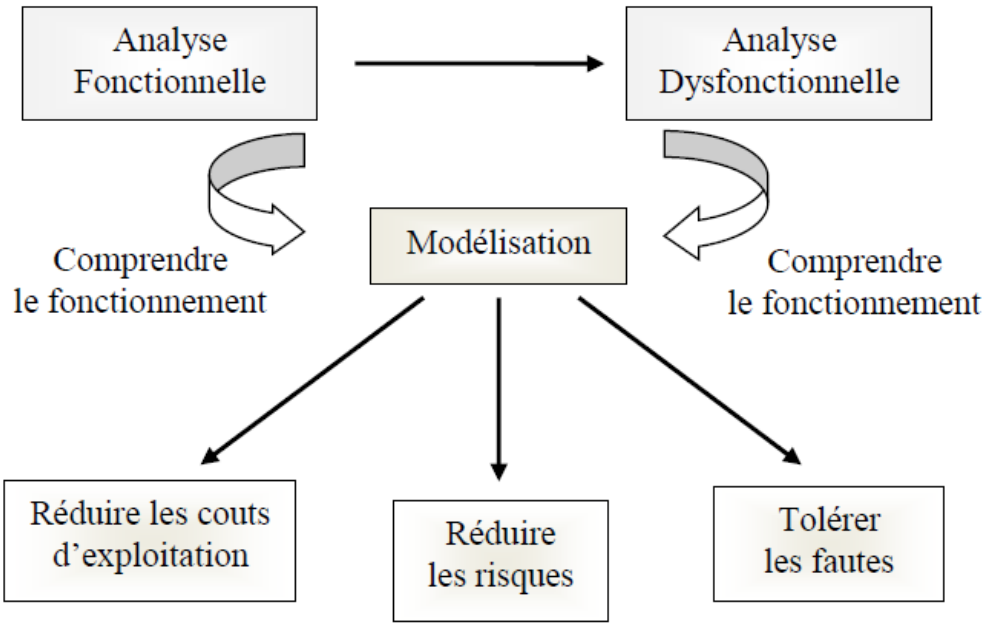



**Figure 2.6** Analyse de la sûreté de fonctionnement. [39]

Les résultats de ces deux études sont mis en commun dans une modélisation du système qui va représenter virtuellement celui-ci avant sa réalisation, tant dans son fonctionnement attendu que dans les pannes susceptibles de lui arriver, comme décrit dans la figure 2-7.

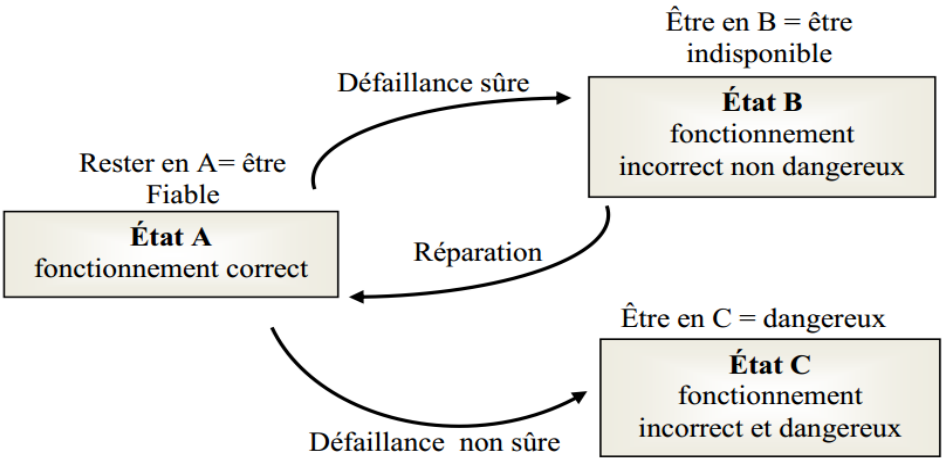



**Figure 2.7** Relation entre la défaillance et l'état d'un système [39].

En étudiant cette modélisation, il devient alors possible de valider ou invalider une solution technique, optimiser des choix architecturaux, remplacer des composants critiques, ceci dont le but de :

- ✓ Réduire au maximum les risques;
- ✓ Réduire au maximum les coûts d'exploitation;
- ✓ Tolérer, dans la mesure du possible, certaines fautes en autorisant un fonctionnement en mode dégradé sous certaines conditions.

## 2.8 La normalisation

Dans cette section, on évoquera quelques normes génériques pour la sûreté de fonctionnement [42].

### 2.8.1 ARP-4754

La norme de sûreté ARP-4754 [43], dont l'intitulé est « Certification Considerations for Highly-Integrated or Complex Aircraft Systems » est un standard de la Society of Automotive Engineers (SAE). Elle traite de processus de développement de systèmes aéronautiques en se focalisant sur les aspects de sûreté.

La norme fait référence à d'autres standards bien connus, comme le DO-178B «Software Considerations in Airborne Systems and Equipment Certification» [44], pour le

développement de logiciel dans le domaine aéronautique, ou encore le DO-254 «Design Assurance Guidance for Airborne Electronic Hardware Considerations in Airborne Systems and Equipment Certification» [45], pour le développement de matériel. Pour beaucoup de techniques d'ingénierie pour la sûreté, l'ARP-4754 [43], fait aussi référence à un autre standard l'ARP-4761 présenté dans la section suivante.

### 2.8.2 ARP-4761

L'ARP-6761 «Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment » [46], il est destiné à être utilisé conjointement avec l'ARP-4754 pour démontrer la conformité du système en court de conception.

### 2.8.3 CEI-61508 et ses dérivées

La norme CEI-61508 [47], est une norme générique de sûreté de fonctionnement du CEI (International Electrotechnical Commission), elle est utilisée comme référentiel par tous les grands secteurs industriels. Elle traite de la sécurité fonctionnelle des systèmes Electriques/Electroniques et Electroniques Programmables (E/E/PE).

En fait, cette norme a révolutionné le monde de la sûreté de fonctionnement, car elle a su amener des nouveautés dans la façon d'intégrer et de réaliser les activités de sûreté de fonctionnement dans le cycle de développement d'un système E/E/PE. Entre autres, la norme a permis de définir des niveaux d'intégrité pour des systèmes E/E/PE qui prennent en compte aussi bien les aspects quantitatifs que qualitatifs dans la gestion du risque.

Par son aspect générique, la norme CEI 61508 reste brève sur la description des outils, méthodes et les techniques à mettre en œuvre. Mais depuis sa création, plusieurs dérivés de cette norme ont vu le jour dans le but de la rendre applicable pour les différents secteurs concernés, (figure 2.8) [42].

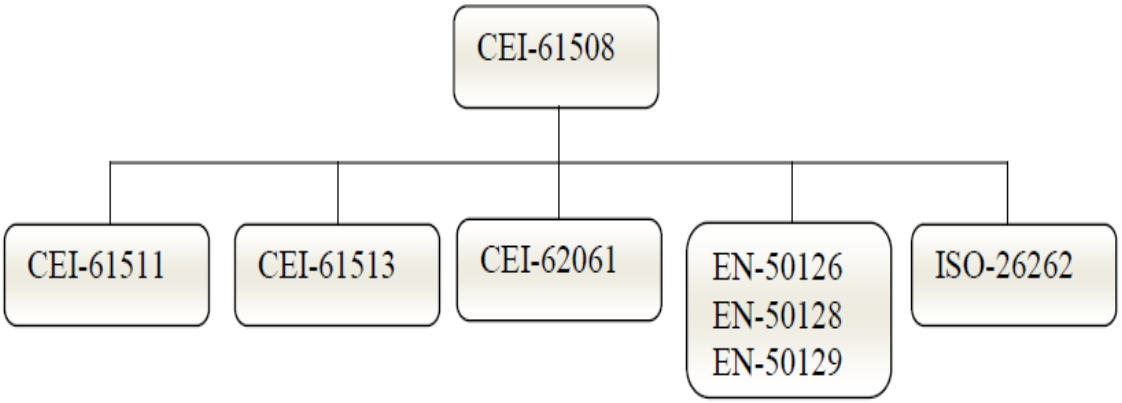



**Figure 2.8** Norme CEI-61508 et ses dérivées.

Ces normes dérivées sont les suivantes :

- La norme CEI 61511[13], créée en 2003, est adaptée pour les procédés industriels.
- La norme CEI 61513[69], créée en 2001, est adaptée pour le secteur du nucléaire.
- La norme CEI 62061[70], créée en 2005, est adaptée pour la sécurité des machines.
- Les normes EN 50126 [71] / EN 50128 [72] / EN 50129 [73], créées respectivement pour les dernières versions, en 1999/2001/2003, sont adaptées pour le secteur du ferroviaire.
- La norme ISO 26262[48], qui devrait être publiée en tant que standard en 2011, sera adaptée pour le secteur de l'automobile [48].

Cette dernière section a permis de conclure que les normes de sûreté aident énormément à comprendre quels sont les objectifs et les activités pour obtenir un système sûrs. Par exemple, l'ARP-4754 fournit une très bonne vision des activités de sûreté de fonctionnement. Mais en soit, ces normes ne définissent pas une approche globale et unifiée avec les activités de conception nominales. Il était nécessaire de définir une approche globale pour la prise en compte de la sûreté de fonctionnement.

## 2.8 Conclusion

Après un historique de la sûreté de fonctionnement, nous avons passé en revue dans ce chapitre les principales méthodes d'analyse et outils de la sûreté de fonctionnement.

L'étude de la sûreté de fonctionnement d'un système vise, d'une part à déterminer ses modes de défaillance, les scénarios susceptibles de conduire aux défaillances et les

conséquences associées. D’autre part, elle vise à évaluer quantitativement les probabilités d'occurrence des différents événements indésirables et des scénarios associés. Parmi les outils de la sûreté de fonctionnement que nous avons évoqués précédemment, nous choisissons l’outil réseaux de Petri stochastique pour étudier les performances de la SdF d’un système instrument de sécurité, De nos études à deux indicateurs de sécurité, la probabilité de défaillance dangereuse (PFD) et la probabilités de défaillance en sécurité (sûres) (PFS).C'est ce que nous étudierons dans le prochain chapitre.

# CHAPITRE 3

## SYSTEME INSTRUMENTE DE SECURITE

# Chapitre 3

# Système instrumenté de sécurité

## 3.1 Introduction

Les Systèmes Instrumentés de Sécurité (SIS) sont des systèmes utilisés comme moyens de protection pour réaliser des fonctions de sécurité et mettre le procédé surveillé dans une position de repli de sécurité (c'est-à-dire un état stable ne présentant pas de risque pour les personnes, l'environnement ou les biens) [28]. L'objet de ce chapitre est de présenter les définitions nécessaires que l'on rencontrera au cours de cette étude, telles que la notion de Système Instrumenté de Sécurité et déférent type de SIS, la fonction de sécurité, la sécurité fonctionnelle, l'évolution des deux performances en termes de sûreté de fonctionnement des systèmes instrumentés de sécurité (SIS) disposant d'instruments d'intelligents en conformité avec les normes de sécurité fonctionnelle , Ces deux paramètres utilisés pour l'évaluation de la sûreté de fonctionnement des SIS se réfèrent à deux modes de défaillances mentionnés par les normes de sécurité. Ces modes sont le mode de défaillances dangereuses et le mode de défaillances sûres. Ces indicateurs sont donnés sous forme de probabilités de défaillance dangereuse (PFD) et de défaillance en sécurité (PFS).

Le présent travail dans ce chapitre a pour objectif de réaliser la fonction de sécurité des systèmes instrumentés de sécurité (SIS) à partir de l'étude des deux indicateurs. La méthodologie utilisée consiste en la modélisation de l'aspect fonctionnel et dysfonctionnel des systèmes instrumentés de sécurité (SIS). L'approche utilisée s'appuie sur les réseaux de Petri stochastiques. L'outil logiciel de simulation utilisé est GRIF (**Gr**aphiques **I**nteractif pour la **F**iabilité).

## 3.2 Concept d'un Système instrumenté de sécurité

Un système instrumenté de sécurité (SIS) est un système visant à mettre le procédé en état stable ne présentant pas de risque pour l'environnement et les personnes et l'équipement matériel lorsque le procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement (explosion, feu…) [8].

Un SIS appelé aussi boucle de sécurité [4], est un ensemble d'éléments (matériels et logiciels) assurant la mise en état de sécurité des procèdes lorsque des conditions prédéterminées sont atteintes [4]. Il est composé d'un ensemble de capteurs, d'unités de traitement et d'éléments finaux [5].

### 3.2.1 Constitution d'un SIS

L'architecture type d'un SIS est donnée à la figure 3.1. Voici un descriptif succinct de chacune de ses parties :

- Sous-système EE (Eléments d'Entrée ou S pour *Sensors*) : constitué d'un ensemble d'éléments d'entrée (capteurs, détecteurs) qui surveillent l'évolution des paramètres représentatifs du comportement du procédé surveillé (température, pression, débit, niveau, …) [4].

- Sous-système UL (Unité logique ou LS pour *Logic Solver*) : comprend un ensemble d'éléments logiques (PLC, API) qui récoltent l'information en provenance du sous-système S et réalisent le processus de prise de décision qui s'achève éventuellement, si l'un des paramètres dévie au-delà d'une valeur-seuil, par l'activation du sous-système FE.
- Sous-système EF (Eléments Finaux ou FE pour Final Element) : agit directement (vanne d'arrêt d'urgence) ou indirectement (vanne solénoïdes, alarme) sur le procédé pour neutraliser sa dérive en le mettant, en général, dans un état sûr. L'évaluation quantitative des performances des systèmes instrumentés de sécurité constitue une étape indispensable pour leur validation, tel que prescrit dans la norme CEI 61508 [12] dédiée aux SIS. Cette validation n'est autre que l'assurance que ces derniers peuvent exécuter correctement les fonctions de sécurité qui leurs sont assignées [4].

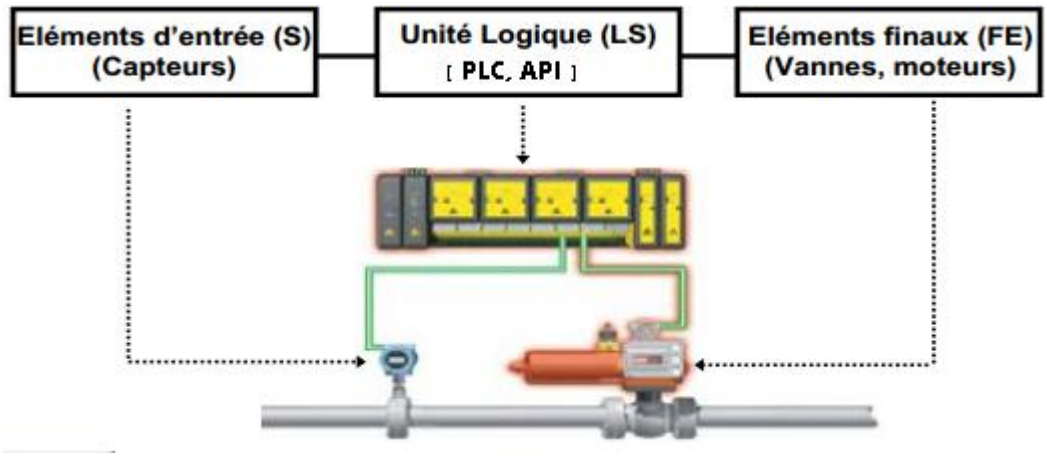



**Figure 3.1** Architecture type d'un SIS [4].

Donc un SIS est un système visant à mettre le procédé en position de repli de sécurité (c'est à dire un état stable ne présentant pas de risque pour l'environnement et les personnes), lorsque le procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement [9]. Il se compose de trois parties:

- Une partie capteur qui mesure l'état du processus,
- Une unité logique qui exécute la fonction de sécurité (automate programmable par exemple) [3],
- Une partie actionneur chargée de mettre le procédé dans sa position de sécurité et de la maintenir [6].

La combinaison de ces trois éléments a pour objectif de remplir une fonction ou sous-fonction de sécurité. Les sous fonctions que l'on peut trouver dans un SIS sont ***la détection*** par le capteur, ***le traitement de l'information*** par l'unité logique et ***l'action*** par l'actionneur. Les éléments d'un SIS sont reliés entre eux par des moyens de transmission. Au minimum, on retrouve en série un capteur, une unité de traitement et un actionneur qui vient commander un élément terminal décrit selon le schéma de la figure 3.2 [7] [9].

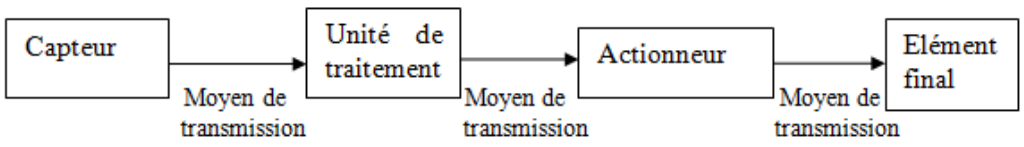



**Figure 3.2** : Schéma d'un SIS simple [7] [9].

La figure 3.3 montre le schéma d'un SIS effectuant plusieurs tâches.

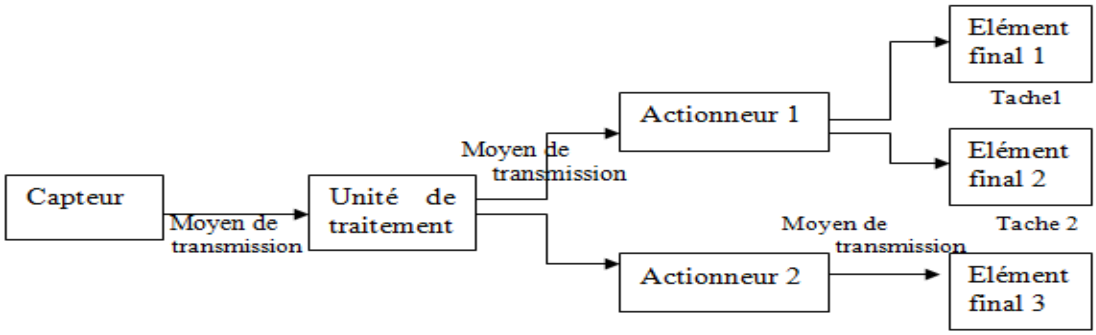



**Figure 3.3** : Schéma d'un SIS effectuant plusieurs tâches [7] [9].

La figure 3.4 montre le schéma d'un SIS recevant plusieurs informations.

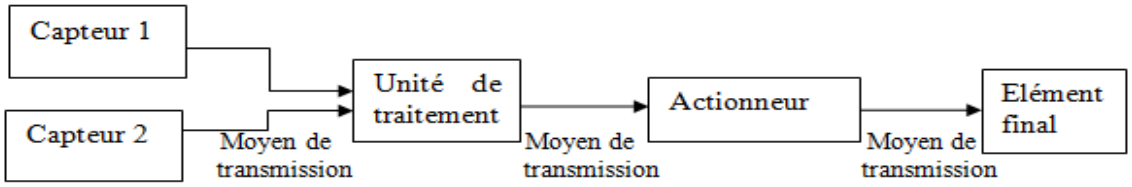



**Figure 3.4** : Schéma d'un SIS recevant plusieurs informations [7].

### 3.2.2 Fonction Instrumentée de Sécurité

Les principales étapes de la norme IEC 61508 [12] et ses normes filles sont déclinées dans ce qu'on appelle le cycle de vie, c'est-à-dire que ces normes traitent depuis l'analyse des risques jusqu'à l'exploitation des fonctions de sécurité instrumentées SIF (Safety Instrumented Functions). Une SIF est définie pour obtenir un facteur de réduction du risque mise en œuvre pour un SIS. Lorsque le SIS est considéré comme un système réalisant une barrière de protection fonctionnelle, cette barrière est considérée comme une fonction de sécurité [59], [60]. Un SIS contient généralement plus qu'une SIF. Si les exigences d'intégrité de la sécurité pour ces SIF diffèrent, alors les exigences applicables au niveau d'intégrité de la sécurité le plus élevée s'appliquent au SIS. Pour une situation donnée, plusieurs fonctions de sécurité peuvent conduire à la réduction de la fréquence d'occurrence du danger.

L'architecture fonctionnelle d'un SIS est un ensemble de SIF qui comprend trois fonctionnalités de base, la d´détection, le traitement(ou la décision) et l'actionnement [8].

### 3.2.3 Sécurité fonctionnelle

La norme CEI 61508[12] dans sa partie 4 définit la sécurité fonctionnelle comme un sous ensemble de la sécurité globale qui se rapporte au système commandé (EUC, Equipement Under Control) et qui dépend du fonctionnement correct du système E/E/EP relatif à la sécurité, des systèmes relatifs à la sécurité basée sur une autre technologie et des dispositifs externes de réduction de risque.

La norme CEI 61511[13] définit la sécurité fonctionnelle comme un sous-ensemble de la sécurité globale qui se rapporte au processus et au système de commande de processus de base (BPCS, Base Process Control System) et qui dépend du fonctionnement correct du système instrumenté de sécurité et d'autres couches de protection. Ce terme diffère de la définition donnée par la CEI 61508 pour refléter les différences dans la terminologie du domaine des processus [8].

La sécurité fonctionnelle permet alors de contrôler les risques inacceptables qui pourraient engendrer des blessures, porter atteinte à la santé des personnes, dégrader l'environnement ou altérer des biens [3].

Les normes de sécurité fonctionnelle IEC 61508 et IEC 61511 définissent une démarche d'analyse du niveau d'intégrité de sécurité (SIL) d'un système. Elles permettent de définir le niveau SIL qui doit être atteint par un SIS qui réalise la fonction de sécurité suite à une analyse de risque, [61] [62]. Plus le SIL à une valeur élevée plus la réduction du risque est importante. Les SIS sont classés en quatre niveaux SIL qui se caractérisent par des indicateurs discrets positionnés sur une échelle de un à quatre niveaux (Tableau 3.1). Les SILs sont employés pour spécifier les exigences de sécurité des fonctions de sécurité réalisées par des systèmes E/E/EP relatifs à la sécurité selon la norme IEC 61508 [12]. Le SIL "quatre" désigne le degré de sécurité le plus élevé du fait de l'exigence forte de sécurité imposée et le niveau SIL "un" désigne l'exigence la plus faible [62].

| **Sollicitation** | **Demande faible** | **Demande élevée** |
|---|---|---|
| **Niveau d'intégrité SIL** | $\boldsymbol{PFD_{avg}}$ | $\boldsymbol{PFH}$ |
| **1** | $\boldsymbol{PFD_{avg}} \in [10^{-2}, 10^{-1}]$ | $\boldsymbol{PFH} \in [10^{-6}, 10^{-5}]$ |
| **2** | $\boldsymbol{PFD_{avg}} \in [10^{-3}, 10^{-2}]$ | $\boldsymbol{PFH} \in [10^{-7}, 10^{-6}]$ |
| **3** | $\boldsymbol{PFD_{avg}} \in [10^{-4}, 10^{-3}]$ | $\boldsymbol{PFH} \in [10^{-8}, 10^{-7}]$ |
| **4** | $\boldsymbol{PFD_{avg}} \in [10^{-5}, 10^{-4}]$ | $\boldsymbol{PFH} \in [10^{-9}, 10^{-8}]$ |

**Tableau 3.1** Les différents niveaux de SIL définis par la norme IEC 61508 [8].

*PFDavg* est La probabilité moyenne de défaillance à la demande. Cette probabilité représente tout simplement l'indisponibilité moyenne d'un système E/E/EP relatif à la sécurité, qui rend ce dernier incapable d'effectuer correctement sa fonction de sécurité, lorsqu'il est faiblement sollicité [74]. La *PFDavg* (Average Probability of Failure on Demand) est la mesure d'une indisponibilité moyenne sur une période spécifiée [8].

La probabilité d'une défaillance dangereuse par heure (*PFH*) :Probability of a dangerous Failure per Hour, est parfois appelée " fréquence des défaillances dangereuses ", ou " taux de défaillances dangereuses ", ou nombre de défaillances dangereuses par heure "[8].

### 3.2.4 Classification des défaillances dans la norme IEC 61508

Généralement un système peut se trouver dans l'un des quatre états suivants :

- ✓ **un état normal :** La fonction de sécurité est valide dans cet état et peut être activée en cas de sollicitation et il n'existe pas de défaillance [8].
- ✓ **Etat normal dégradé** : Dans l'état normal dégradé, la fonction de sécurité est valide, des composants de systèmes pouvant être défaillants. Le système peut réagir lors de l'avènement d'un événement dangereux. En effet, il y a plus d'un moyen pour exécuter la fonction de sécurité. C'est le cas de l'existence de la redondance [75] [65].
- ✓ **Etat de défaillances sûres** : Dans l'état sûr, la sécurité est assurée pour le système [65]. Cet état peut faire suite à l'apparition d'un événement dangereux (débordement du réservoir) ayant entraîné la demande d'activation de la fonction de sécurité, on est donc dans le fonctionnement nominal du système. Il peut aussi faire suite à une défaillance d'un ou de plusieurs composants. Le système peut entrer dans cet état lorsque :

  - il y a eu détection de la défaillance.

  - il y a eu déclenchement intempestif auquel cas la défaillance n'a pas eu d'action néfaste vis-à-vis de la sécurité et le système est placé dans un état sûr ou de sécurité [12].
- ✓ **Etat de défaillances dangereuses** : C'est un état du système où la fonction de sécurité ne peut plus être exécutée. Un ou plusieurs composants sont défaillants. Le système ne peut plus répondre à une demande d'activation de la fonction de sécurité lors de l'arrivée d'un événement dangereux et il y a risque d'accident [12] [65].

Après interaction entre les différents composants du système global, celui-ci peut se trouver dans quatre états possibles présentées dans la figure 3.5 suivante :

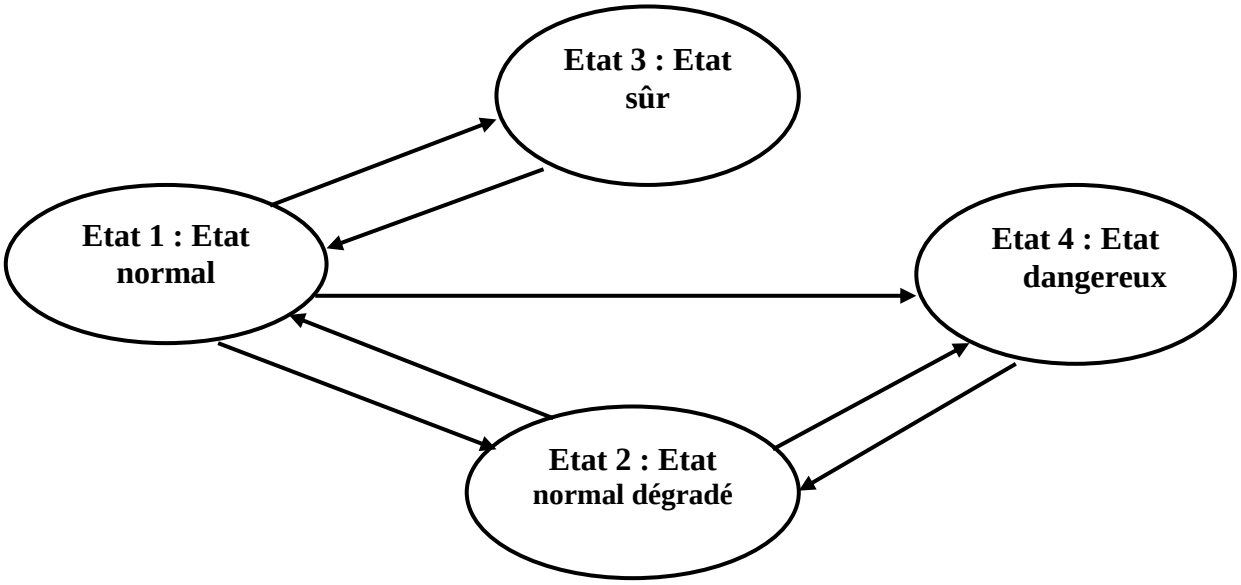



**Figure 3.5** : Etats du système.

La norme IEC 61508 [12] distingue les défaillances aléatoires du matériel des défaillances systématiques. La norme distingue les défaillances dangereuses, des défaillances sûres. Toutes les défaillances détectées en ligne par test de diagnostic sont qualifiées de défaillances détectées [8], [65]. Celles qui ne sont pas détectées sont qualifiées de défaillances non détectes [65]. Les défaillances peuvent être comme suit :

– Les défaillances sûres et détectées font passer le système de l'état normal à l'état de sécurité, leur taux de défaillance est noté $\boldsymbol{\lambda_{SD}}$.

– Les défaillances sûres et non détectées font passer le système de l'état normal à l'état dégradé, leur taux de défaillance est noté $\boldsymbol{\lambda_{SU}}$.

– Les défaillances dangereuses détectées auraient la potentialité de faire passer le système de l'état normal à l'état de défaillance dangereuse mais leur détection associée à une stratégie sécuritaire (arrêt, alarme) permet au système de passer à l'état de sécurité, leur taux de défaillance est noté $\boldsymbol{\lambda_{DD}}$ [65], [64].

– Les défaillances dangereuses non détectées font passer le système de l'état normal `a l'état de défaillance dangereuse, leur taux de défaillance est noté $\boldsymbol{\lambda_{DU}}$, [64].

La somme des taux des défaillances sûres détectées et non détectées représente le taux de défaillances sûres, noté $\boldsymbol{\lambda_S}$ :

$$\lambda_S = \lambda_{SD} + \lambda_{SU} \quad (3.1)$$

La somme des taux des défaillances dangereuses détectées et non détectées donne le taux de défaillances dangereuses, noté $\lambda_D$ :

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \quad (3.2)$$

La figure 3.6 représente la Classification des défaillances.

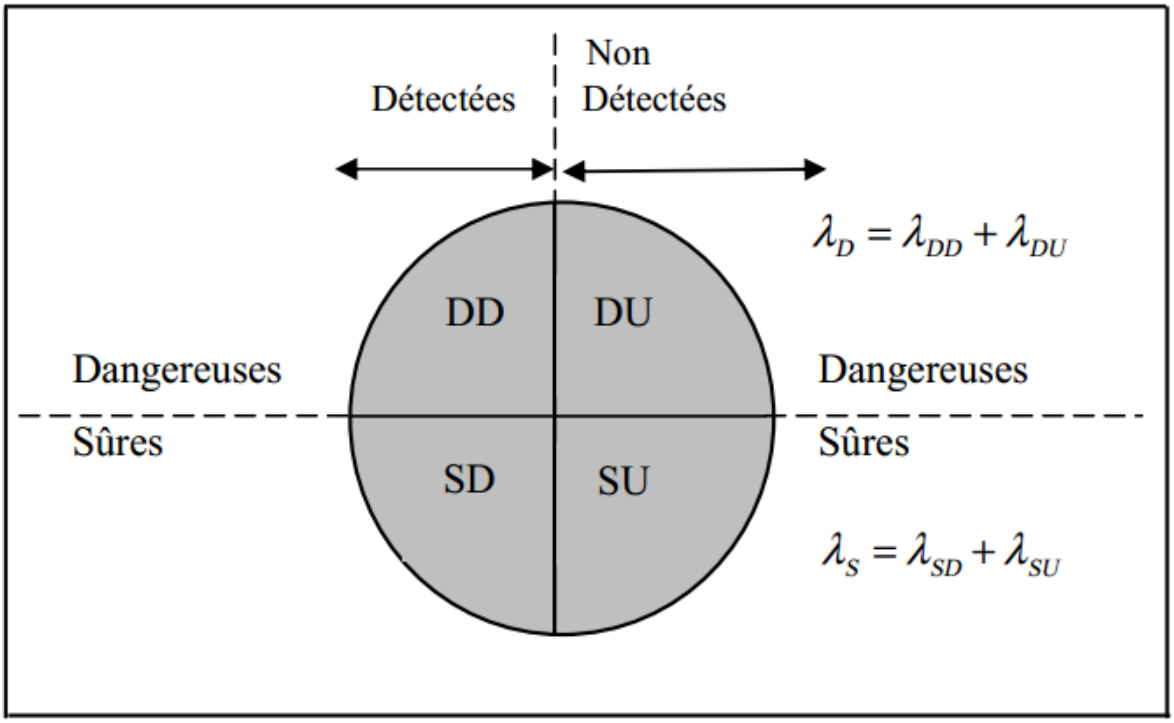



**Figure 3.6** : Classification des défaillances. [66].

### 3.2.5 Taux de couverture de diagnostic

La norme IEC 61508 [12] permet d'estimer la probabilité de défaillance de la fonction de sécurité due à des défaillances matérielles aléatoires. Les calculs font intervenir un grand nombre de paramètres : architecture, taux de défaillance des composants, intervalle des tests, taux de couverture de diagnostic ***DC***. La norme IEC 61508 [12] définit le taux de couverture comme étant le rapport du taux de défaillance des pannes dangereuses détectées $\lambda_{DD}$ (par un test de diagnostic) et du taux de défaillance totale des pannes dangereuses $\lambda_D$ (détectées et non détectées), [60], [65], [66] présenté dans l'équation 3.3 suivante :

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{dangerous}} \quad (3.3)$$

Le taux de couverture *DC* intervient dans la détermination des taux de défaillances dangereuses ; détectées et non détectées.

Pour la vérification des SIS plusieurs tests ont été définis et peuvent être classés en fonction de leur mode de sollicitation (en ligne ou hors ligne) [8]
– Les tests de diagnostic en ligne (on-line diagnostic), sont des tests en ligne qui détectent essentiellement les défaillances aléatoires d'un composant, d'un module de système. Ils sont le plus souvent exécutes dés la mise sous tension, puis périodiquement [8].

## 3.3 Normes relatives aux systèmes instrumentés de sécurité

La norme internationale de sécurité IEC 61508 est une des dernières normes dédiées à la sécurité fonctionnelle. Elle est devenue avec ses normes filles les plus récentes et les plus connues des acteurs de la sécurité dans les secteurs industriels.

### 3.3.1 Norme CEI 61508

La norme CEI 61508[12] est la base d'autres normes sectorielles (ex : machines, procédés continus, ferroviaire, nucléaire) ou de produits (ex : variateurs de vitesse). Elle influence donc le développement des systèmes E/E/PE et des produits concernés par la sécurité à travers tous les secteurs [8]. Elle repose sur deux concepts fondamentaux vis-à-vis de son application : le cycle de vie en sécurité et les niveaux d'intégrité de sécurité. Cette norme s'applique aux systèmes relatifs à la sécurité lorsque l'un ou plus de ces systèmes comporte des dispositifs électriques/électroniques/électroniques programmables. L'avantage de cette norme est qu'elle propose des moyens de justification sur l'ensemble du cycle de vie d'un produit en fonction du niveau de sécurité que l'on souhaite atteindre. La norme IEC 61508 [12] se compose de sept volets comme suit :

– 61508-1 présente les définitions des prescriptions générales.
– 61508-2 traite les prescriptions spécifiques aspect matériel des systèmes E/E/EP.
– 61508-3 dédiée `a la présentation des prescriptions spécifiques, aspect logiciel, des Systèmes E/E/EP. Elle est développée dans la troisième partie de la norme.
–61508-4 présente les définitions et les abréviations utilisées.
– 61508-5 donne des exemples de méthode pour la détermination des niveaux d'intégrité de

sécurité.

– 61508-6 fournit les guides d'application des parties 2 et 3 de la norme.

– 61508-7 présente les techniques et les mesures recommandées lors de la validation des systèmes E/E/EP.

La figure 3.7 montre la norme CEI 61508 générique et ses normes filles par secteur d'activité.

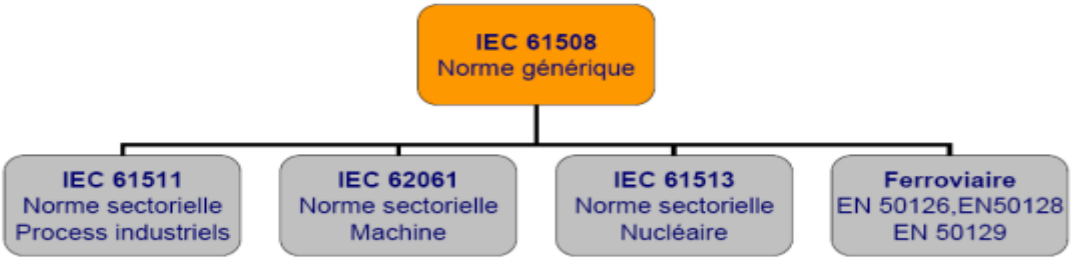



**Figure 3.7**: Norme CEI 61508 et normes dérivées [28]

### 3.3.1.1 Norme CEI 61511

L'IEC 61511[13], s'intéresse à la sécurité fonctionnelle des SIS pour le secteur de l'industrie

des procédés continus. Les remarques faites ci-dessus pour l'IEC 61508 [12] s'appliquent également à l'IEC 61511 [13]. Cette norme est composée de trois grandes parties:

– 61511-1 présente les définitions et les exigences des systèmes (matériel et logiciel).

– 61511-2 traite les lignes directrices pour l'application de la première partie de la norme.

– 61511-3 fournit des conseils pour la détermination des niveaux d'intégrité de sécurité.

L'IEC 61511 [13] détaille les définitions et les prescriptions relatives au cycle de vie en sécurit´e contenant la spécification, la conception, l'exploitation et la maintenance d'un système instrumenté de sécurit´e, afin de maintenir le procédé dans une position de sécurité convenable.

La norme IEC 61511 est l'une des déclinaisons de la norme IEC 61508. Les SIS constituent l'objet principal de ces deux normes, mais ils y sont considérés différemment selon les métiers auxquels elles s'adressent par la figure 3.8 suivante [66] :

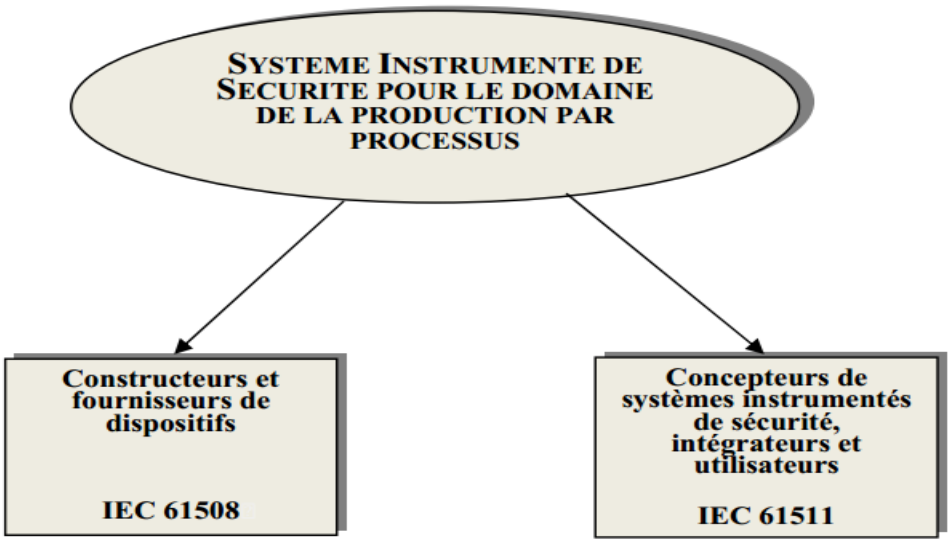



**Figure 3.8**: Utilisateurs de l'IEC 61508 et l'IEC 61511 [68].

L'IEC 61508 [12] est une norme complexe, difficile `a mettre en œuvre, elle est destinée surtout aux fabricants et fournisseurs de systèmes E/E/EP [28], alors que la norme IEC 61511 est plus facile `a utiliser, elle présente une simplification de l'IEC 61508, en se limitant aux éléments nécessaires pour l'industrie de process [28].

### 3.3.1.2 La norme IEC 62061

L'IEC 62061 [70] repose sur les mêmes concepts que ceux de l'IEC 61508 [12]. Elle est destinée à être utilisée par les concepteurs de machines et les fabricants de systèmes de commande électroniques relatifs à la sécurit´e de machines [70]. Elle concerne la spécification des prescriptions et fait des recommandations pour la conception, l'intégration et la validation de ces systèmes [28].

### 3.3.1.3 La norme IEC 61513

L'IEC 61513 [69] concerne le secteur de la sûreté des centrales nucléaires. Elle présente les prescriptions relatives aux systèmes de contrôle commande utilisés pour accomplir les fonctions de sécurité des centrales nucléaires. La conception des systèmes de contrôle commande peuvent être réalisés à l'aide d'une combinaison de composants traditionnels câbles à des composants informatiques. La conformité à l'IEC 61513 facilite la compatibilité avec les exigences de l'IEC 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire.

#### 1.3.1.4 La norme EN 50126

La norme EN 50126 [71] s'intéresse essentiellement aux applications ferroviaires. Elle permet de spécifier les principaux concepts de la sûreté de fonctionnement des systèmes tels que : la fiabilité, la disponibilité et la sécurité. Cette norme est constituée de deux normes filles. L'EN 50128 [72] est destinée à la partie logicielle des systèmes de protection ferroviaire. L'EN 50129 [73] concerne les systèmes électroniques de sécurité pour la signalisation [28].

## 3.4 Performance en sécurité d'un système instrumenté de sécurité

La norme CEI 61508 [12] spécifie deux indicateurs de la sécurité relatifs aux systèmes électroniques programmables dédiés aux applications de sécurité. Ces deux paramètres utilisés pour l'évaluation de la sûreté de fonctionnement des SIS se réfèrent à deux modes de défaillances mentionnés par les normes de sécurité. Ces modes sont le mode de défaillances dangereuses et le mode de défaillances sûres [60] [65] [66]. Ces indicateurs sont donnés sous forme de probabilités de défaillance dangereuse (PFD) et de défaillance en sécurité (sûres) (PFS). Leur évaluation comme l'exige la norme CEI 61508[12] pose quelques problèmes liés à leur spécificité. Une défaillance dangereuse est une défaillance ayant la capacité de mettre le système instrumenté de sécurité dans l'impossibilité d'exécuter une fonction de sécurité [1].

Une défaillance sûre, quant à elle, n'a pas la potentialité de mettre le système instrumenté de sécurité dans un état dangereux [1].

Les défaillances dangereuses mettent le système dans un état de défaillance dangereuse. Dans ce cas, la fonction de sécurité n'est plus réalisée. Un ou plusieurs composants sont alors défaillants.

En effet, les systèmes instrumentés de sécurité intègrent de manière obligatoire en fonction du niveau de sécurité requis, des auto-tests systématiques et des redondances permettant la détection et/ou la tolérance à certaines défaillances afin de garantir l'effectivité de la fonction de sécurité. Un système est sûr si ses défaillances ne sont pas dangereuses.

A partir de l'architecture du système instrumenté de sécurité réalisant la fonction instrumentée de sécurité faiblement sollicitée, la moyenne de la probabilité de défaillance à la demande PFDavg (Average Probability of Failure on Demand) est évaluée sur un intervalle [0, t]. La performance d'une fonction de sécurité peut être exprimée comme la probabilité de défaillance à la demande (PFD), et la probabilité de défaillances sûres (PFS) ou de déclenchements intempestifs. Ces deux attributs sont importants dans le monde de la sécurité

et leurs valeurs représentent respectivement une mesure pour le niveau de sécurité atteint et coût financier causé par le système de sécurité en raison de déclenchements intempestifs. La valeur de la PFD est une exigence pour répondre à l'intégrité de la sécurité au niveau de la norme CEI 61508 [12]. Pour la valeur PFS il n'y a pas actuellement de prescriptions internationales en matière de sécurité dans le monde, même si les utilisateurs finaux du système de sécurité exigent une valeur de PFS aussi faible que possible.

Plusieurs utilisateurs sont à la recherche de systèmes qui soient à la fois fiables et sûrs. Un système est fiable s'il ne tombe pas en panne fréquemment. La figure 3.7 montre le diagramme de Venn d'un système incluant le bon fonctionnement et les deux modes primaires de défaillances, le mode de défaillances sûres et le mode de défaillances dangereuses [63].


**Figure 3.9**: Système avec modes de défaillances [1].

Pour les deux modes de défaillances, les défaillances dangereuses sont beaucoup plus graves puisque les systèmes de protection ne peuvent assurer la mise en sécurité du processus et défaillances ne peuvent être révélées. Les systèmes nouvellement conçus disposent d'autodiagnostic et d'autotests internes qui permettent de déceler un certain nombre de défaillances par la désactivation des sorties lorsque des défauts internes sont détectés. Cette fonctionnalité peut être exploitée par les systèmes instrumentés de sécurité pour permettre de convertir les défaillances dangereuses en défaillances sûres. L'effet global des autodiagnostics sur le système avec ses modes de défaillances peut être décrit par la figure 3.10 suivante :

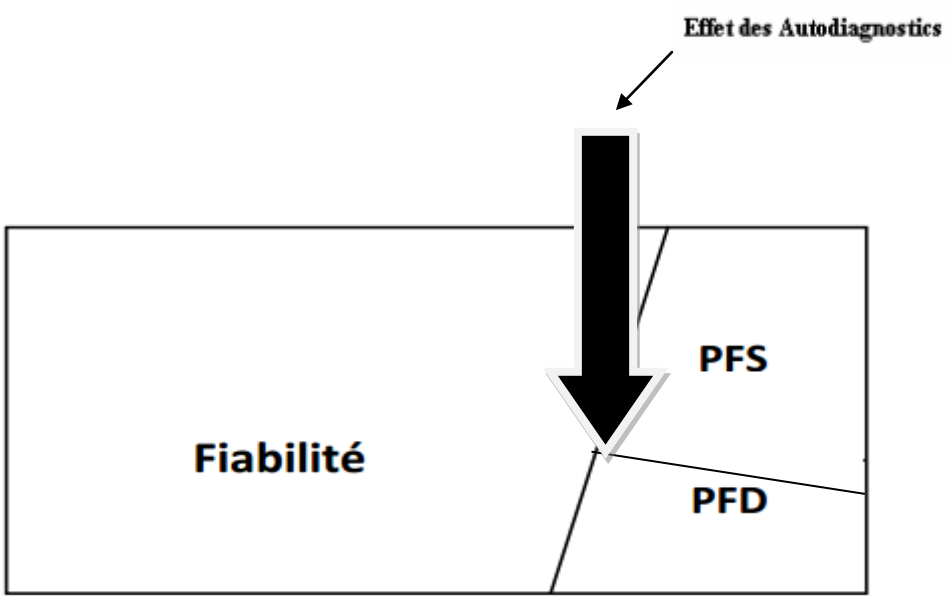



**Figure 3.10**: Effet des autodiagnostics sur le système instrumenté de sécurité.

La figure 3.10 montre l'effet de la fonctionnalité d'autodiagnostic sur le système instrumenté de sécurité. Cet effet peut être exprimé par la conversion de la probabilité de défaillances dangereuses (PFD) en probabilité de défaillances sûres (PFS).

De ce fait,

➡ **L'autodiagnostic** est la capacité d'un instrument à effectuer l'évaluation de son état de fonctionnement et de diagnostiquer l'élément éventuellement en dysfonctionnement [56].

**-Exemple de montage pour autodiagnostic**

La figure 3.11 représente un exemple de montage pour l'autodiagnostic

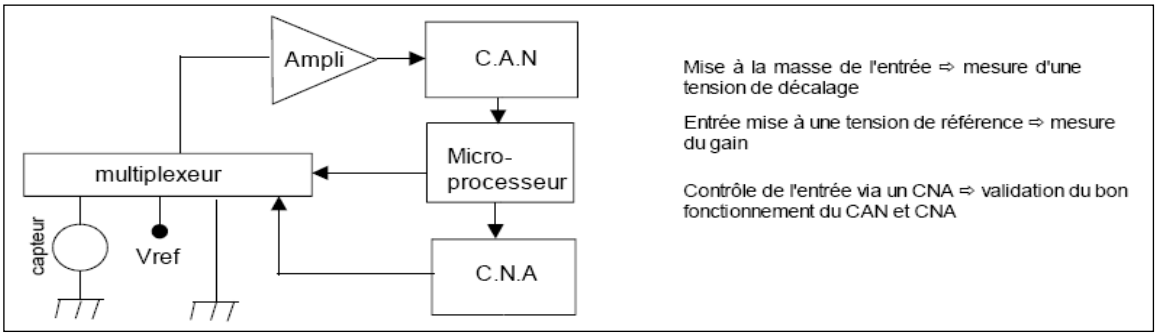



**Figure 3.11**: exemple de montage pour autodiagnostic [56].

## 3.5 Systèmes Instrumentés de Sécurité à Intelligence Distribuée (SISID)

Le concept de sécurité intelligente favorisé par l'évolution grandissante des équipements d'automatisation est matérialisé par l'utilisation des instruments intelligents dans les systèmes instrumentés de sécurité (SIS) avec une distribution de l'intelligence associée à l'utilisation d'un réseau de communication typiquement un réseau de terrain. Les SAID ne sont pas spécifiques aux applications sécuritaires conformes aux normes internationales de sécurité récentes CEI 61508 et CEI 61511. Leur utilisation dans les boucles de sécurité a pour objectif de tirer profit de leurs avantages exprimés dans les applications non relatives à la sécurité notamment en contrôle/commande des systèmes.

Les deux tableaux 3.2 et 3.3 mettent en évidence les correspondances des caractéristiques propres à chacun des deux types de systèmes (SAID et SIS), ainsi que les aspects relatifs à la sûreté de fonctionnement. Les caractéristiques d'un SISID sont une forme d'intersection entre celles des SAID et celles des SIS. L'essentiel est qu'elles respectent les exigences des normes en termes d'architectures et en termes de fonctions. L'aspect relatif à la sûreté de fonctionnement doit être conforme aux normes de sécurité dans la mesure où la détermination des performances doit être relative aux métriques exprimées dans les normes.

| **Système** | **Système d'Automatisation à Intelligence Distribuée (SAID)** | **Système Instrumenté de Sécurité (SIS)** |
|---|---|---|
| **Mission** | Contrôle/Commande des processus industriels | Mise en état de sécurité des processus |
| **Architecture fonctionnelle** | Les fonctionnalités génériques des instruments intelligents se résument comme suit :<br>✓ l'acquisition (mesure et conditionnement)<br>✓ la configuration (paramétrage et réglage)<br>✓ la validation (traitement et prise de décision<br>✓ l'actionnement<br>✓ la communication | L'architecture fonctionnelle d'un système instrumenté de sécurité [28] qui est composée d'un ensemble de fonctions instrumentées de sécurité est constituée de trois fonctionnalités de base :<br>✓ la détection (ou la mesure),<br>✓ la configuration est interdite l'architecture d'un SIS est figée,<br>✓ la décision l'actionnement<br>✓ la communication n'est pas réellement prise en compte dans la norme (seulement quelques recommandations) |
| **Architecture matérielle** | Les constituants des SAID sont:<br>✓ plusieurs unités de traitement<br>✓ des composants intelligents | Les SIS se composent :<br>✓ d'unités logiques<br>✓ de capteurs et d'éléments |

| | | |
|---|---|---|
| | ✓ Un réseau de communication tel qu'un réseau de terrain | terminaux |
| **Architecture opérationnelle** | Projection de l'architecture fonctionnelle sur l'architecture matérielle par allocation de fonctions élémentaires avec respects de contraintes relatives aux capacités des composants. Un exemple est celui d'une optimisation d'architectures basée sur les critères de coût et sûreté de fonctionnement [3].<br>✓ Possibilité de reconfiguration dynamique | Implantation d'une ou de plusieurs SIF (Fonction instrumentée de sécurité) sur l'architecture matérielle qui est un ensemble interconnecté de composants pour satisfaire les exigences d'un SIL (niveau d'intégrité de sécurité) selon les normes CEI 61508[12] et CEI 61511[13].<br>✓ Problème d'activation/désactivation selon les besoins de mode de sécurité (batch) |

**Tableau 3.2** : Différentes caractéristiques des SAID et des SIS

Globalement, nous pouvons dire que les systèmes d'automatisation à intelligence distribuée disposant d'instruments intelligents offrent pour des applications sécuritaires l'avantage de pouvoir améliorer la qualité des mesures avec des diagnostics internes. Relate que les autotests dans les instruments intelligents permettent d'accroître la fraction des défaillances sûres de ces dispositifs [3]. Le pouvoir de validation au regard des conditions environnantes peut aussi être exploité afin d'améliorer les performances en sécurité des systèmes instrumentés de sécurité. Les inconvénients de l'utilisation des SAID qui peuvent altérer les systèmes de sécurité se rapportent aux risques engendrés par des systèmes microprogrammes tels que le potentiel des erreurs systématiques dans les logiciels et aux problèmes dus à la configuration (un utilisateur peut changer des paramètres internes des instruments, ce qui peut nuire à la sécurité).

En se conformant à la norme CEI 61508[12], il est possible d'utiliser les instruments intelligents dans les applications de sécurité à condition de s'en tenir aux exigences et recommandations de cette norme (tolérance aux anomalies…). Les instruments utilisant de l'électronique programmable doivent être fabriqués avec des procédures qui respectent la norme tant pour le matériel que pour le logiciel.

| System | Système d'Automatisation à Intelligence Distribuée (SAID) | Système Instrumenté de Sécurité (SIS) |
|---|---|---|
| **Caractéristiques et aspects relatifs à la sûreté de fonctionnement** | ✓ Architecture distribuée base de beaucoup de systèmes industriels [3],<br>✓ Rapidité de traitement, grande flexibilité [3],<br>✓ Réduction du coût et du câblage, Simplification de la maintenance,<br>✓ Structuration hybride,<br>✓ Reconfigurations offrant un caractère dynamique [3],<br>✓ Coopération des composants, systèmes répartis autour d'un réseau de communication,<br>✓ Contrôle/Commande des processus industriels | ✓ Pas de spécification sur la distribution de l'architecture dansla norme,<br>✓ Traitement au niveau du système logique,<br>✓ Systèmes statiques (dormants)[3],<br>✓ Systèmes centralisés,<br>✓ Moyens de protection du personnel ou de l'environnement, application à de nombreuses industries de processus, Surveillance des procédés, Partie des couches de protection pour les industries de transformation [3]. |
| | Pour ce type de systèmes, on détermine souvent la fiabilité, la disponibilité, la maintenabilité par des métriques telles que : *R(t), A(t), M(t), MTTF, MTTR, MUT* qui désignent respectivement la fiabilité, la disponibilité, la maintenabilité, durée moyenne jusqu'à défaillance, la durée moyenne des temps de réparation et la durée moyenne de bon fonctionnement après réparation [3].<br>R(t) = P[entité non défaillante sur [0,t]]<br>A(t) = P[entité non défaillante à l'instant t]<br>M(t) = 1-P[entité non réparée sur [0,t] ]<br>$MTTF = \int_0^\infty R(t)dt$<br>$MTTR = \int_0^\infty [1 - \mathrm{M(t)}]\,\mathrm{dt}$ | Les deux indicateurs proposés par la norme sont la PFD et la PFS respectivement la probabilité de défaillance dangereuse et la probabilité de défaillance en sécurité. Ils concernent toutes les deux la sécurité.<br>*PFD(t) = 1-R(t)-PFS(t)*<br>*PFD(t) = 1-A(t)*<br>$PFD_{avg}=1/RRF$<br>*RFF :* Facteur de réduction de risque, $PFD_{avg}$ : Probabilité moyenne de défaillance dangereuse. La norme CEI 61508 [12] donne une quantification rendue possible par la connaissance du taux de défaillance (λ), du taux de couverture de chaque composant, ainsi que de l'architecture du système.<br>$PFD_{avg}= \frac{1}{T}\int_0^T PFD(t)dt$ |
| **Evaluation de la sûreté de fonctionnement** | Il existe des méthodes diverses pour l'évaluation de la Sdf de ce type de systèmes :<br>✓ approche dynamique<br>✓ approche statique | La norme propose un certain nombre d'équations mathématiques pour la détermination de la $PFD_{avg}=1/RRF$ [3]. L'évaluation est faite avec la technique des blocs diagrammes de fiabilité. D'autres techniques sont aussi |

| | | |
|---|---|---|
| | | répandues telle que l'approche markovienne. |

**Tableau 3.3**: Aspects relatifs à la sûreté de fonctionnement des SAID et des SIS.

## 3.6 Etude l'Evolution des deux indicateur de sécurité PFD et PFS :

La norme CEI 61508 [12] spécifie deux indicateurs de la sécurité relatifs aux systèmes électroniques programmables dédiés aux applications de sécurité. Ces deux paramètres utilisés pour l'évaluation de la sûreté de fonctionnement des SIS se réfèrent à deux modes de défaillances mentionnés par les normes de sécurité. Ces modes sont le mode de défaillances dangereuses et le mode de défaillances sûres. Ces indicateurs sont donnés sous forme de probabilités de défaillance dangereuse (PFD) et de défaillance en sécurité (PFS).

Pour étudier l'évolution des deux indicateur de sécurité PFD et PFS on va faire la modélisation du comportement fonctionnelle et dysfonctionnelle du système SIS .Cette modélisation fonctionnelle et dysfonctionnelle a pour objectif l'évaluation des performances en fonctionnement normal et en fonctionnement anormal.

### 3.6.1Description de la méthodologie

La méthodologie utilisée pour l'étude des systèmes instrumentés de sécurité (SIS) et les même systèmes à intelligence distribuée (SISID) repose sur la structuration et la modélisation de ces systèmes afin d'en faire la vérification et l'analyse au moyen de réseaux de Petri stochastiques pour exploiter les modèles.

La méthodologie s'appuie sur une structuration hiérarchique et modulaire. Elle permet d'obtenir une architecture détaillée en termes de sous-systèmes de base et de leurs interactions à partir de la vue systémique. Cette structuration s'applique à la fois aux fonctionnalités de mesure, de traitement, d'actionnement et aux mécanismes de communication.

La modélisation est traitée sous la forme d'une approche stochastique utilisant les Réseau de Petri stochastiques (RdPS). Les Réseau de Petri stochastiques présentent également l'intérêt d'être connu des spécialistes de la sûreté de fonctionnement et de pouvoir par conséquent servir non seulement pour modéliser l'aspect fonctionnel mais également pour évaluer les performances de la sûreté de fonctionnement, ces raisons ont guidé notre choix. Les capteurs et actionneurs (intelligents ou non), les unités de traitement et autres fonctions, les moyens de communication, le processus lui-même peuvent être formalisés de la sorte,

avec un point de vue à la fois continu et discret, en fonction des nécessités. Les réseaux de Petri stochastiques assurent aussi le pouvoir de synchronisation et de parallélisme. Ce qui rejoint les caractéristiques de systèmes comportant un réseau de communication. Pour la représentation formelle du comportement de ceux-ci, il doit y avoir un pouvoir d'expression relatif aux aspects de parallélisme et de synchronisation en plus du pouvoir d'analyses qualitative et quantitative. Les dépendances stochastiques qui peuvent résulter des communications entre les différents composants du système sont aussi prises en compte par les réseaux de Petri stochastiques puisqu'ils y sont bien adaptés par la construction de modèles d'évaluation de la sûreté de fonctionnement.

Un RdPS est un RdP temporisé doté d'une mesure de probabilité sur l'espace des trajectoires, c'est à dire que les séquences de franchissement sont mesurables en considérant un espace aléatoire. De façon formelle :

Un RdPS est un couple $S = < R, \phi >$, tel que :

- $R = < P, T, Pré, Post, M_0 >$ est le réseau sous-jacent.
- $\phi : T \rightarrow R^+$, la fonction qui associe à chaque transition un taux de franchissement fixe.
- $M_0$ : marquage initial du réseau [58].

Cette approche nécessite de simuler le fonctionnement du système par des méthodes de Monte Carlo puisque le calcul analytique n'est quasiment jamais possible. Pour réaliser une simulation de Monte-Carlo, deux éléments sont nécessaires :

- ✓ un modèle du comportement (fonctionnement et dysfonctionnement) du système étudié,
- ✓ un logiciel de simulation de Monte-Carlo pour effectuer les tirages au hasard, réaliser des histoires et évaluer les différents scores d'intérêt,
- ✓ une description des données sous forme probabiliste.

Les modèles de comportement du système sont divers et variés : diagrammes, arbres, modèles spécifiques, réseaux, langages de description de comportement, tableurs, etc. Ils doivent être capables de reproduire de manière suffisamment réaliste le comportement du système lorsqu'il évolue au cours du temps en étant soumis à différents aléas comme défaillances, réparations, tests, procédures, événements extérieurs, etc.

Une histoire est une des évolutions possibles du système avec ses défaillances, ses réparations, etc., sur une durée définie. Une fois la première histoire générée, on en génère une seconde qui représente une autre évolution possible, puis une troisième, etc. Au cours de chacune d'elles, on enregistre les paramètres d'intérêt (passage ou temps de séjour dans certains états, nombre d'occurrences de tel événement, coûts, etc.) de manière à constituer des échantillons statistiques.

Le franchissement d'une transition de nature stochastique reflète l'occurrence d'une défaillance modélisée par une loi exponentielle, et le passage d'un état de fonctionnement normal *(place p1OK)* à un état de panne *(place p2 KO)* est présenté sur le schéma de la figure 3.12. La transition ***lambda*** *(exp1E-3)* représente le taux de défaillance, la transition ***mu*** *(exp 0.1*) représente le taux de réparation.

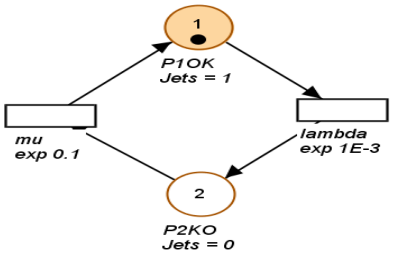



**Figure 3.12** : Modélisation de l'état normal et de défaillance d'un composant.

Pour l'évaluation des paramètres de sûreté de fonctionnement choisis, nous poserons les hypothèses de calcul suivantes :

- ✓ toutes les liaisons (hors réseau de communication) sont supposées présenter une sûreté infinie (probabilité de défaillance nulle),
- ✓ les taux de défaillance des éléments constitutifs des boucles sont supposés constants et connus (on étudiera le système dans sa phase de maturité),
- ✓ les lois de probabilités sont exponentielles,
- ✓ l'intervalle de test de la boucle est choisi de sorte que le SIL reste constant sur toute la durée de vie,
- ✓ la corrélation entre les modules des sous-systèmes est supposée nulle (pas de défaillance de cause commune). Cette hypothèse représente une restriction car il existe toujours des conditions qui peuvent provoquer la défaillance simultanée de plusieurs composants,

- ✓ une défaillance dangereuse se traduit par une absence de réaction du système instrumenté de sécurité à intelligence distribuée,
- ✓ une défaillance sûre se traduit par la mise dans une position de repli du SISID ou par une exécution intempestive de la fonction de sécurité.

### 3.6.2 Modélisation du comportement du SIS classique et avec intelligence distribuée SISID :

Généralement, pour une architecture **MooN,** le premier chiffre désigne le nombre d'éléments que l'on doit avoir en état de marche pour que le système assure la fonction de sécurité et le second chiffre indique le niveau de redondance [12]. Dans cette étude, on choisit un SIS à une architecture 1oo1 (un parmi un) dans laquelle toute défaillance dangereuse entraîne la défaillance du système, et une défaillance sûre se traduit par la mise dans une position de repli prédéfinie ou par une exécution intempestive de la fonction de sécurité. Cette architecture comprend un seul canal et donc un seul chemin matériel que peut parcourir un signal dans la chaîne de traitement d'une demande [3]. La figure 3.13 montre un SIS à une architecture 1oo1 (un parmi un).

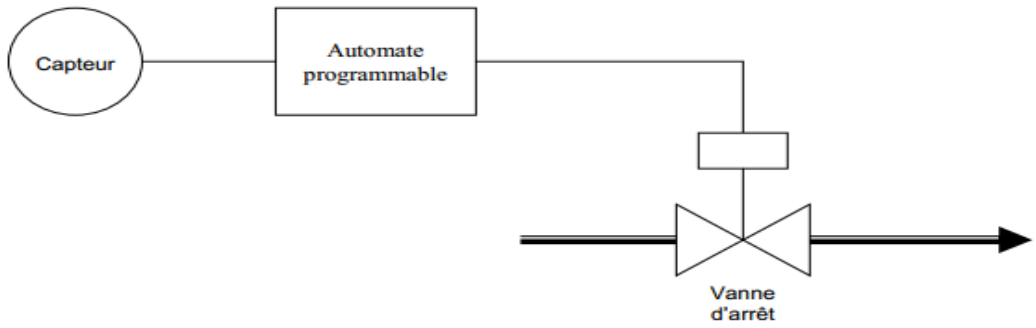



**Figure 3.13** : Système instrumenté de sécurité (Architecture 1oo1).

Le SIS est composé d'un capteur, d'un automate programmable et d'un actionneur. La détection des défaillances par autodiagnostic des dispositifs a pour objectif d'atteindre la fiabilité des équipements requise par le niveau d'intégrité des fonctions (de sécurité).

La figure 3.14 montre un Système instrumenté de sécurité à intelligence distribué à une architecture 1oo1D (un parmi un).

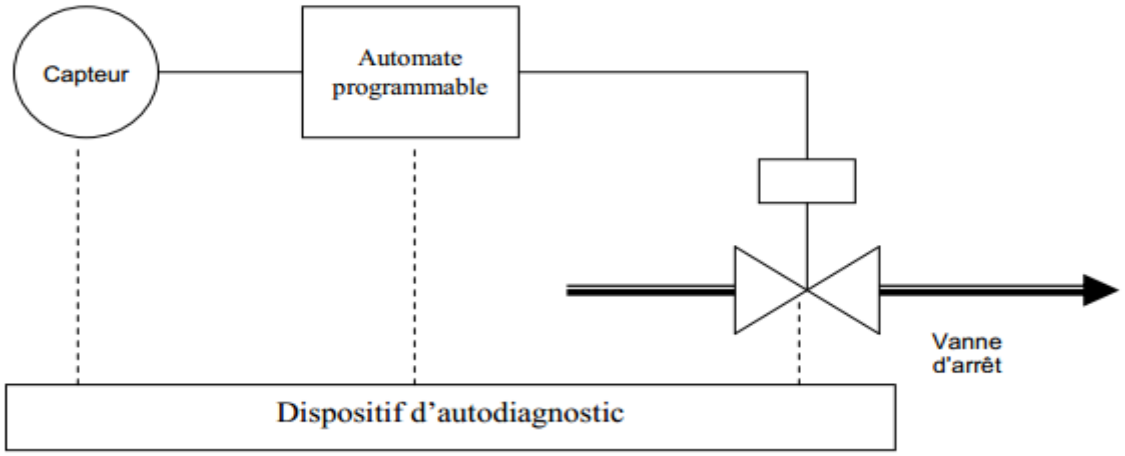



**Figure 3.14** : Système instrumenté de sécurité à intelligence distribué à une architecture 1oo1D (un parmi un) [1].

Une défaillance dangereuse se traduit par une absence, potentielle ou avérée, de réaction de la fonction de sécurité. Une défaillance sûre se traduit par la mise dans une position de repli prédéfinie du système ou par une exécution intempestive de la fonction de sécurité. La détection d'une défaillance, sûre ou dangereuse, se traduit par une mise en position sûre du système ou une exécution forcée de la fonction de sécurité [3].

La modélisation du comportement du système complet est l'ensemble des modèles du capteur et de l'automate et de l'actionneur relient ente eux dans le cas classique et avec intelligence. L'outil logiciel de simulation utilisé est petri net GRIF (**Gr**aphiques **I**nteractif pour la **F**iabilité). Ce logiciel permet :

- ✓ L'utilisation d'une interface graphique pour la construction des réseaux de Petri.
- ✓ La saisie des paramètres de simulation (nombre d'histoire, durée d'une histoire).
- ✓ Le lancement des simulations de Monte-Carlo.
- ✓ L'obtention, à l'aide d'un code de calcule, des résultats statistiques des simulations.

### 3.6.2.1. Modèle du capteur

#### 3.6.2.1.1 Modèle du capteur classique

Le modèle  classique du capteur est décrit par le schéma de la figure 3.15.

Dans ce modèle les places **P1** et **P2** représentent respectivement l'état de fonctionnement et de dysfonctionnement du capteur. Les places **P3** jusqu'à **P5** représentent la partie de qualification de défaillance du capteur dans un état danger ou sûr, la place **P6** (Tc) représente l'état de test du capteur par l'automate, donc Les défaillances non détectées ***DND*** peuvent être qualifiées de sûres ou de dangereuses suite à l'exécution du test par l'automate, dans ce cas là le système passer vers un état de sécurité ou un état dangereuse non détecté. Un taux de couverture de diagnostic ***DC*** est représenté par la transition ***DC***. Après l'occurrence d'une défaillance sûre, il y a possibilité de restaurer le système par le franchissement de la transition déterministe (***SD***) dont la durée est égale au temps nécessaire à la restauration complète du système, ***SD*** le taux de restauration.

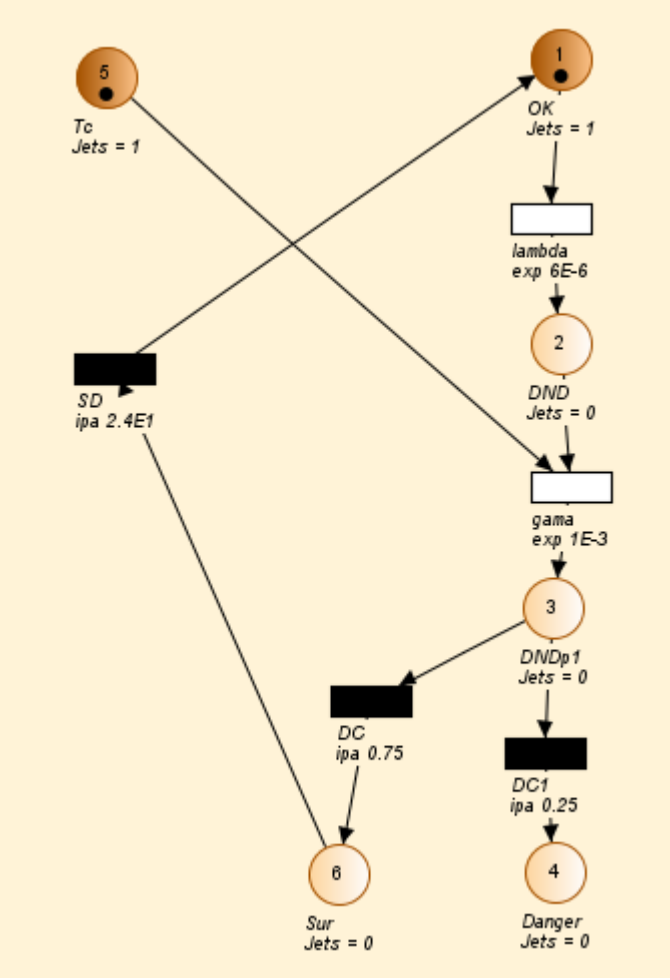



**Figure 3.15** : Modèle du capteur classique.

Le modèle de l'actionneur est équivalent au modèle du capteur de la figure 3.15, mais chacun avec ses propres paramètres. La transition *gama (1E-3)* représente la transition stochastique (défaillance aléatoire).

Les taux de défaillance de chaque élément (capteur, actionneur) sont : *lambda-capteur* est égal à 6E-6 $h^{-1}$ et *lambda-actionneur* est égal à 9E-6 $h^{-1}$ [9] [14].

#### 3.6.2.1.2 Modèle du capteur intelligent

Le modèle du capteur intelligent est décrit par le schéma de la figure 3.16. La partie fonctionnelle est décrite respectivement par l'ensemble des places et des transitions allant de ***P1*** à ***P6*** et de ***T1*** à ***T9***. La présence du jeton dans la partie gauche représente le bon fonctionnement du capteur. Les transitions de la partie fonctionnelle ne sont pas stochastiques puisque l'évolution est liée à des phénomènes déterministes. La dynamique de cette partie est beaucoup plus rapide que la dynamique des défaillances.

Dans ce modèle du capteur, un certain nombre de défaillances sont exprimées. Il s'agit des défaillances sûres (place ***Sûr***) et défaillances dangereuses (place ***Danger***). Un taux de couverture de diagnostic ***DC*** est représenté par la transition ***DC***.

Les défaillances non détectées ***DND*** peuvent être qualifiées de sûres ou de dangereuses suite à l'exécution de l'autotest des capteurs [9] [14].

La norme IEC 61508 [12] défini le taux de couverture de diagnostic (***DC***) comme étant le rapport entre le taux de défaillances dangereuses détectées (par un test de diagnostic) et le taux total des défaillances dangereuses (détectées et non détectées) [8] [14].on traduise la partie d' intelligence par la fonctionnalité de l'autodiagnostic par le capteur intelligent donc faire la détection des défaillances dangereuses et les défaillances sûres dans ce cas là le taux de défaillances dangereuses détectées $\boldsymbol{\lambda_{DD}}$ est élevé lors de l'occurrence de défaillances qui conduite à l'augmentation du taux de couverture de diagnostic (***DC***) . Ce taux est représenté par la relation 3.3 dans la section (3.2.5) [8].

$$\boldsymbol{DC} = \frac{\sum \boldsymbol{\lambda_{DD}}}{\sum \boldsymbol{\lambda_{dangerous}}} \qquad (3.3)$$

Plus ce taux est important, plus grande est la confiance dans le système instrumenté de sécurité du fait que les situations sûres prédominent par rapport aux situations dangereuses lors de l'occurrence de défaillances donc une transformation de défaillances dangereuses en défaillances sûres cette conversion est représente l'effet d'autodiagnostic du capteur intelligent.

La relation de proportionnalité entre les défaillances sûres et les défaillances dangereuses est donnée par la relation :

***DC1 =1-DC*** (3.4)

Après l'occurrence d'une défaillance sûre, il y a possibilité de restaurer le système par le franchissement de la transition déterministe (***SD***) dont la durée est égale au temps nécessaire à la restauration complète du système, on définit ***SD*** est le taux de restauration. La présence d'une marque dans la place ***P6*** autorise un autotest du capteur géré localement.

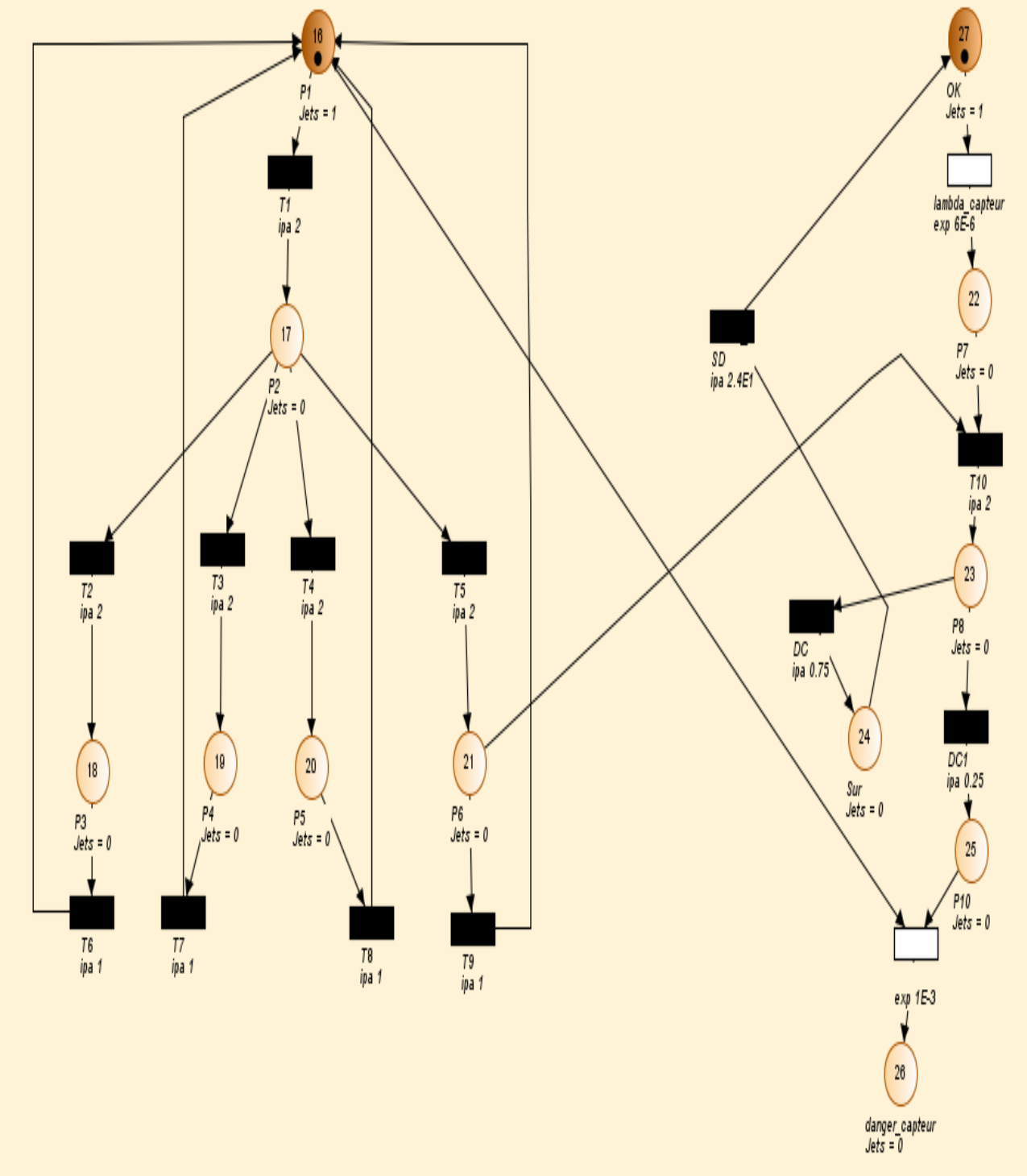



**Figure 3.16** : Modèle du capteur intelligent.

Le modèle de l'actionneur intelligent est équivalent au modèle du capteur intelligent de la figure 3.16, mais chacun avec ses propres paramètres.

### 3.6.2.2 Modèle de l'automate

Le modèle de l'automate de la figure 3.17 montre une représentation de deux parties, l'une fonctionnelle et l'autre dysfonctionnelle.

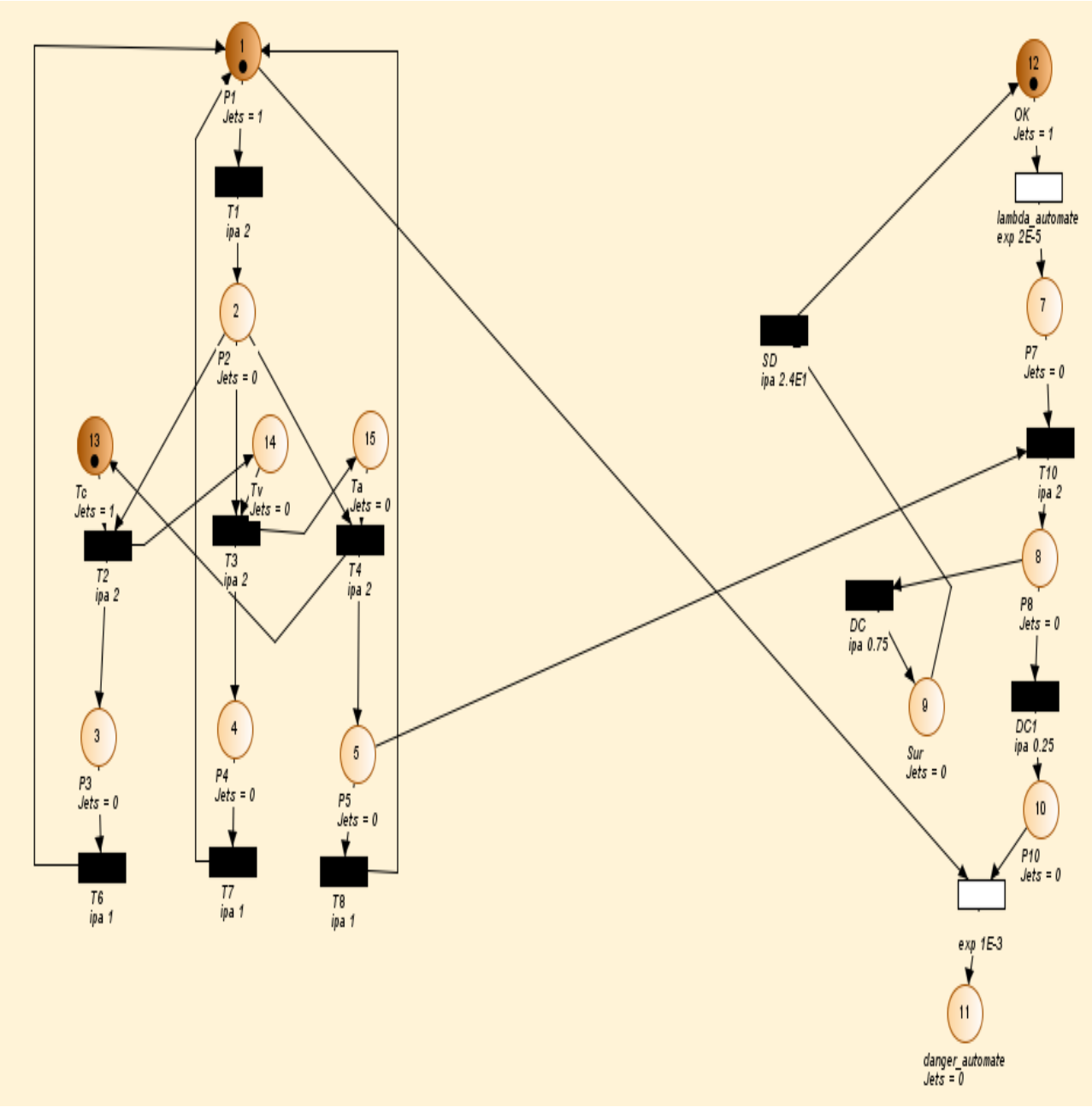



**Figure 3.17**: Modèle de l'automate.

La partie fonctionnelle est décrite par l'ensemble des places et des transitions allant respectivement de ***P1*** à ***P5*** et de ***T1*** à ***T7***. Cycliquement, l'automate réalise ses propres autotests ainsi que des autotests du capteur et de l'actionneur.

La présence d'un jeton dans les places ***P3***, ***P4*** ou ***P5*** autorise l'autotest de l'un des dispositifs précités selon une politique de test gérée par l'automate lui même.

Les autotests des différents dispositifs sont gérés localement suivant une politique de test qui consiste à allouer la même durée de test pour les différents dispositifs et à commencer par le test du capteur (***Tc***), puis l'actionneur (***Tv***) et enfin l'automate (***Ta***). Pour la partie dysfonctionnelle, il faut s'assurer que le jeton est soutiré de la partie fonctionnelle là où il se trouve lorsque le système tombe en panne sûre ou dangereuse. Le taux de défaillance de l'automate est : *lambda-automate* est égal à 2E-5 $h^{-1}$[9] [12]. L'automate peut être également restauré en cas de défaillance sûre.

La modélisation du système classique est équivalente aux relier les modèles classique des éléments du système entre eux suivant : l'automate, le capteur, l'actionneur, selon les Figures 3.13, 3.14. Dans le cas du système intelligent la modélisation est la même mais remplace les modèles classiques par les modèles intelligent des éléments du système étudié.

Le diagnostic permet la conversion de défaillances dangereuses détectées en défaillances sûres.

### 3.6.3. Simulation et analyse

Le but de la simulation est d'observer le comportement d'un système instrument de sécurité, classique et avec intelligence par l'approche des réseaux de Petri stochastique (RdPS). L'outil logiciel GRIF (**Gr**aphiques **I**nteractif pour la **F**iabilité) adapté pour l'étude des deux indicateurs de sécurité PFD et PFS a été utilisé. Le taux de couverture de diagnostic ***DC*** dans cette étude est égal à 0.75 et le taux de restauration ***SD*** est égal 0.24, la période d'échantillonnage est égale 0.5 pour l'ensemble des dispositifs (capteur, automate, actionneur). La durée de simulation de 10000 heures qui correspond à un intervalle entre deux tests périodiques [9] [14].

Pour apprécier l'apport des systèmes intelligents, nous soumettons le système en situation classique et intelligent à une défaillance provoquée. L'injection d'une défaillance selon les deux situations (classique et intelligent) et pour les trois éléments considérés (capteur, actionneur, automate) [9] [14]. Cela se traduit par le franchissement de la transition

*lambda_automate* pour l'automate par exemple. La partie dysfonctionnelle de l'automate est alors représentée à droite de la figure 3.17.

Après le lancement de simulation par la fonction MOCA (Monte Carlo), on calcule les valeurs de PFD et PFS à partir du temps de séjour dans les places P11 (*Danger-automate)* et *P9 (Sûr)* respectivement de la figure 3.17, voir l'annexes C, puis calculé indisponibilité selon la relation suivante :

L'indisponibilité(%) = temps de séjour(h)/durée d'histoire(h).

Temps de séjour(h) : la durée de présence des jetons dans la place P11 (*Danger-automate).*

Durée d'histoire(h) : le temps total de simulation.

Une histoire est une des évolutions possibles du système avec ses défaillances, ses réparations, sur une durée définie.

Les valeurs relevées des PFD et PFS pour un SIS classique et un SIS à intelligence distribuée (SISID) sont données respectivement sur les tableaux 3.4 et 3.5.

| Temps(h) | PFD | PFS |
|---|---|---|
| 1000 | $0,72.10^{-2}$ | $1,16.10^{-2}$ |
| 4380 | $2,848.10^{-2}$ | $4,5472.10^{-2}$ |
| 5000 | $3,2428.10^{-2}$ | $5,159.10^{-2}$ |
| 8760 | $5,527.10^{-2}$ | $8,764.10^{-2}$ |
| 10000 | $6,256.10^{-2}$ | $9,909.10^{-2}$ |

**Tableau 3.4** : PFD et PFS pour un SIS classique

| Temps(h) | PFD | PFS |
|---|---|---|
| 1000 | $0,012.10^{-2}$ | $1,88.10^{-2}$ |
| 4380 | $0,017.10^{-2}$ | $7,225.10^{-2}$ |
| 5000 | $0,19.10^{-2}$ | $8,11.10^{-2}$ |
| 8760 | $0,27.10^{-2}$ | $13,4.10^{-2}$ |
| 10000 | $0,351.10^{-2}$ | $15,06.10^{-2}$ |

**Tableau 3.5** : PFD et PFS pour un SIS à intelligence distribuée (SISID).

On traduit les valeurs dans les deux tableaux 3.4 et 3.5 par la figure 3.15 suivante :

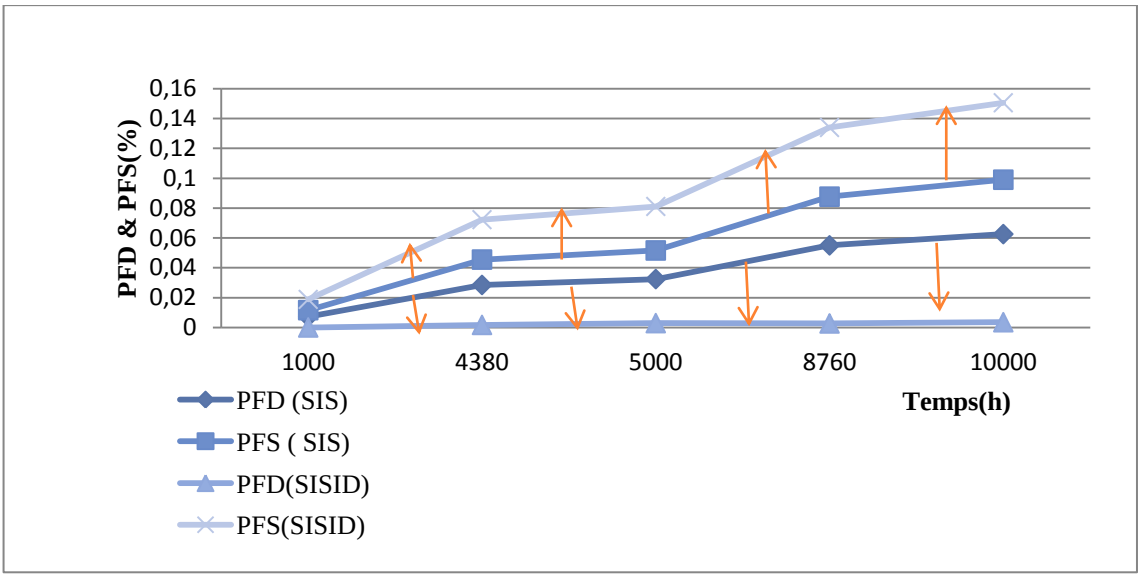



**Figure 3.18**: Evolution des deux indicateurs de sécurité PFD et PFS du système en fonction du temps.

La courbe de la figure 3.18 montre l'evolution des deux métriques principales des performances en sécurité PFD et PFS pour une durée de 10000 heures qui est un peu supérieure a une année (8670 heures). Les deux courbes font état d'allures exponentielles, Le taux de couverture de diagnostic dans cet exemple est égal à 75 % pour l'ensemble des dispositifs [9] [14].

- Nous relevons une diminution de la valeur de la PFD et une augmentation de la valeur de la PFS par rapport aux valeurs du système classique, car des défaillances dangereuses se transforment en défaillances sûres.
- La conversion de la probabilité de défaillances dangereuses (PFD) en probabilité de défaillances sûres (PFS) peut être exprimée par l'effet de la fonctionnalité d'autodiagnostic d'un instrument intelligent.

Pour faire l'analyse du niveau d'intégrité de sécurité (SIL) du système instrument de sécurité (SIS) dans le cas classique et le même système avec intelligence distribuée (SISID) on va calculer la valeur moyenne de PFD ($PFD_{moy}$), cette valeur représente la probabilité moyenne de défaillance à la demande ($PFD_{avg}$). Cette probabilité représente tout simplement l'indisponibilité moyenne du système sur une période spécifiée.

- ✓ ***Dans le cas d'un SIS classique***

On relève les valeurs de $PFD_{moy}$ à partir de tableau 3.4.

$PFD_{moy} = PFD_{avg} = (0,0072+0,02848+0,032428+0,05527+0,06256) / 5$

$PFD_{avg} = 0,0371876 = 3,71876 .10^{-2}$, donc la valeur de $\boldsymbol{PFD_{avg}} \in [10^{-2}, 10^{-1}]$.

La valeur de $PFD_{avg}$ correspond à un SIL 1 selon le tableau 3.1.

- ✓ ***Dans le cas d'un SIS à intelligence distribuée (SISID)***

On relève les valeurs de $PFD_{moy}$ à partir de tableau 3.5.

$PFD_{moy} = PFD_{avg} = (0.00012+0,00017+0,0019+0,0027+0,00351) / 5$

$PFD_{avg} = 0,00841 = 8,41 .10^{-3}$, donc la valeur de $\boldsymbol{PFD_{avg}} \in [10^{-3}, 10^{-4}]$.

La valeur de $PFD_{avg}$ correspond à un SIL 2 selon le tableau 3.1.

- ➢ Nous constatons que le système instrument de sécurité (SIS) est passé de niveau d'intégrité de sécurité SIL 1 au niveau d'intégrité de sécurité SIL 2 , le niveau de SIL a changé et il est amélioré. Plus le SIL à une valeur élevée plus la réduction du risque est importante et le SIS qui réalise la fonction de sécurité suite à une analyse de risque, [61] [62]. Ce résultat confirme l'importance et la contribution de l'utilisation des instruments intelligents dans l'approche SIS (les boucles de sécurité).

## 3.7 Conclusion

Ce travail a porté sur une étude d'évaluation des deux indicateurs de sécurité d'un système SIS basé sur une étude comparative entre un système instrument de sécurité (SIS) classique et le même système à intelligence distribué(SISID). Le travail mené a confirmé l'intérêt de l'approche SIS avec outils intelligent. Les systèmes instrumentés de sécurité (SIS) sont souvent utilisés comme moyens de protection pour réaliser des fonctions de sécurité et utilisés pour détecter des situations dangereuses.

La diminution de la valeur de la probabilité de défaillance dangereuse (PFD) et l'augmentation de la valeur de la probabilité de défaillance sûre (PFS) confirme les avantages d'utilisation des instruments intelligents.

La conversion de la probabilité de défaillances dangereuses (PFD) en probabilité de défaillances sûres (PFS) peut être exprimée par l'effet de la fonctionnalité d'autodiagnostic d'un instrument intelligent.

L'amélioration de niveau d'intégrité de sécurité SIL du système dans le cas de l'intelligence (SISID) confirme la contribution des instruments intelligents dans l'amélioration de la sécurité dans l'approche SIS (les boucles de sécurité).

Les bénéfices apportés à la sécurité, par les fonctionnalités numériques au sein des Capteurs Intelligents, résident principalement dans les capacités plus complètes d'autodiagnostics, qui permettent ainsi une meilleure détection des défauts et défaillances.

Finalement, le travail mené a confirmé l'intérêt de l'approche RdPS qui est bien adaptée à la modélisation du comportement fonctionnel et dysfonctionnel du système étudié dans le cas classique et avec intelligence.

# CHAPITRE 4
## AMELIORATION DE LA SURETE DE FONCTIONNEMENT D'UN SYSTEME MECATRONIQUE

# Chapitre 4

## Amélioration la sûreté de fonctionnement d'un système mécatronique

### 4.1 Introduction

Les systèmes mécatroniques sont de plus en plus utilisés dans l'industrie. Tous les secteurs sont concernés: l'automobile, l'aéronautique, le nucléaire, le spatial et même des domaines comme le bancaire ou le médical. Le développement d'un système mécatronique est envisagé selon l'approche de l'ingénierie concourante dans le cadre d'un cycle de développement, est une démarche méthodologique pour maîtriser la conception des systèmes et produits complexes.

Les instruments intelligents jouent un rôle très important dans l'amélioration de la sûreté de fonctionnement des systèmes industriels, car ils intègrent des fonctionnalités supplémentaires. Pour cette raison, nous avons étudié l'apport de ces instruments intelligents dans l'amélioration de la sûreté de fonctionnement d'un système mécatronique. Pour ce faire, trois approches de modélisation du comportement fonctionnel et dysfonctionnel du système étudié dans le cas classique et avec intelligence sont confrontées, à savoir : arbre de défaillance, diagramme de fiabilité et Réseau de petri stochastique.

Il convient de déterminer l'approche qui sera la mieux adaptée à la modélisation du cas d'étude et à la prise en charge de l'aspect dynamique. L'outil logiciel de simulation utilisé est GRIF (**Gr**aphiques **I**nteractif pour la **F**iabilité). Les paramètres de la sûreté de fonctionnement traités sont alors : la fiabilité, la disponibilité et les deux indicateurs de sécurité PFD et PFS.

## 4.2 Les systèmes mécatroniques

### 4.2.1 Contexte historique:

Avant de donner les nombreuses définitions et de résumer certaines notions, il est bon de rappeler l'historique des évolutions industrielles ou autres qui ont amené à préciser ces notions. Avant les années 1950, les machines sont des ensembles électromécaniques. Dans les années 50, on assiste à l'apparition des semi-conducteurs, l'électronique est née. Dans les années 60-70, l'apparition de calculateurs fiables permet le contrôle des machines par logiciel. Une étude concernant les innovations technologique publiée en 2002, déclare que sur 100 projets innovants en mécanique, la majorité est à l'interface de la mécanique et de l'électronique. La mécatronique se définit alors comme la combinaison synergique et systémique de la mécanique, de l'électronique et de l'informatique. L'intérêt de ce domaine d'ingénierie multidisciplinaire est de concevoir des systèmes complexes et de permettre leur contrôle. Le terme « mechatronics » a été introduit pour la première fois par un ingénieur de la compagnie japonaise «YASKAWA» en 1969, pour désigner le contrôle des moteurs électriques par ordinateur [39]. Ce terme a par la suite évolué, pour apparaitre officiellement dans le Larousse en 2005. Plusieurs définitions sont données pour définir les systèmes mécatroniques. Isermann [17] résume les définitions données à la mécatronique dont « La mécatronique est l'intégration synergique de l'ingénierie mécanique avec l'électronique et le contrôle intelligent de calculateurs dans la conception et la fabrication de produits et processus industriels » [39]. Il estime que toutes les définitions sont d'accord pour dire que la mécatronique est un domaine interdisciplinaire dans lequel les disciplines suivantes agissent ensemble :

- ✓ Systèmes mécaniques (éléments mécaniques, machines, mécanique de précision).
- ✓ Systèmes électroniques (micro-électronique, électronique de puissance, capteurs et actionneurs).
- ✓ Technologie de l'information (théorie des systèmes, automatisation, génie logiciel, intelligence artificielle).

### 4.2.2 Concepts d'un système mécatronique :

La norme NF E 01 -010 [15], définit la mécatronique comme une « démarche visant l'intégration en synergie de la mécanique, l'électronique, l'automatique et l'informatique dans la conception et la fabrication d'un produit en vue d'augmenter et/ou d'optimiser sa

fonctionnalité ». La mécatronique n'est pas intrinsèquement une science ou une technologie, elle doit être considérée comme une attitude, une manière fondamentale de regarder et de faire des choses et exige, par sa nature une approche unifiée [16].

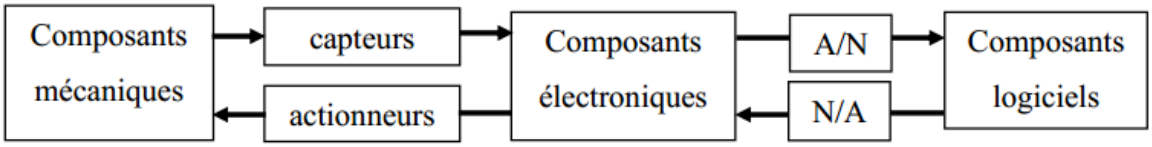



**Figure 4.1**: Système mécatronique [39].

Le Système Mécatronique (SM) de la figure 4.1 intègre de la mécanique, de l'électronique et du logiciel, mais également des systèmes hydrauliques, pneumatiques et des systèmes thermiques. Cet exemple montre qu'il est important que le système soit conçu comme un ensemble autant que possible. La synergie induite par les systèmes mécatroniques conduit à une combinaison intelligente de technologies [39]. Elle mène alors à des solutions et à des performances supérieures, qui ne pourraient pas être obtenues par des applications séparées [39].

L'avènement des systèmes mécatroniques dans l'industrie, en particulier dans l'industrie automobile, a entraîné de nouvelles contraintes [22], telles que :

- l'assimilation de plusieurs technologies;
- les interactions entre les différentes entités fonctionnelles;
-la prise en compte de la dynamique du système (le fonctionnement en temps réel, événementiel et l'intégration des nombreux états possibles);
- l'impossibilité de réaliser des tests exhaustifs. Malgré ces contraintes, la mécatronique apporte des avantages indéniables comme la baisse des coûts, la satisfaction client par les solutions innovantes proposées, la réponse positive à des exigences sociétales de plus en plus importantes ;
- pollution, consommation, sécurité des passagers et piétons [39].

En conclusion, Un système mécatronique est un système complexe pluridisciplinaire à dominante mécanique et électronique avec contraintes temps réel [19]. Il est complexe car il est composé d'un grand nombre d'entités en interaction locale et simultanée où il y a des boucles de rétroaction. L'état d'une entité a une influence sur son état futur via l'état Composants mécaniques capteurs actionneurs Composants électroniques Composants logiciels A/N N/A d'autres entités. De plus, c'est un système ouvert et soumis à un extérieur,

par le biais des flux d'énergie et d'information sur la frontière. Il est pluridisciplinaire car plusieurs domaines technologiques sont mis en œuvre pour les parties commande et opérative. Il est composé d'éléments de différents domaines : mécaniques, électroniques ainsi que des technologies de l'information comme c'est indiqué dans la figure 4.2. Finalement la mécatronique est une symbiose de ces différentes disciplines au service de la conception de produits intégrés.

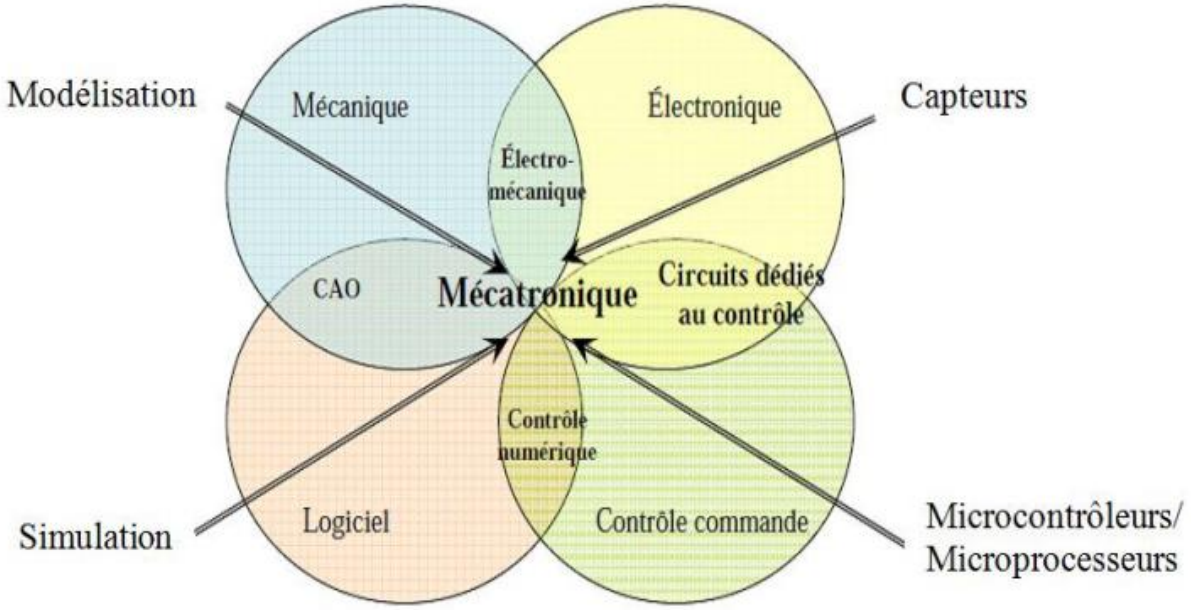



**Figure 4.2** : Interactions entre systèmes et technologies.

Il est à contraintes temps réel car il est le plus souvent immergé dans son environnement et doit permettre une automatisation d'un ensemble de tâches. Le respect des contraintes temporelles dans l'exécution des tâches est aussi important que le résultat de ces tâches pour permettre aux clients de ces derniers de les exploiter correctement [24].

## 4.3 Matériels et méthodes

### 4.3.1 Descriptions du cas d'étude

Le système étudier est un système mécatronique concerne la régulation de volume de deux réservoirs en redondance passive avec utilisation d'un seul réservoir à la fois.

La figure 4.3 présente l'ossature d'un tel système qui est constitué d'un automate programmable, de deux pompes 1 et 2, de trois électrovannes EV1, EV2 et EV3 (électrovanne de secours), de deux capteurs de niveau, des deux réservoirs (Réservoir 1 et Réservoir 2) régulés en volume et d'un troisième réservoir de vidange [20].

Les deux réservoirs régulés alimentent des utilisateurs selon un besoin prédéfini (fonction du temps). Le rôle de l'automate est de maintenir le volume entre deux valeurs prédéfinies : Vmin et Vmax. Pour ce faire, il dispose de l'information fournie par les deux capteurs et commande les électrovannes principales EV1 et EV2.

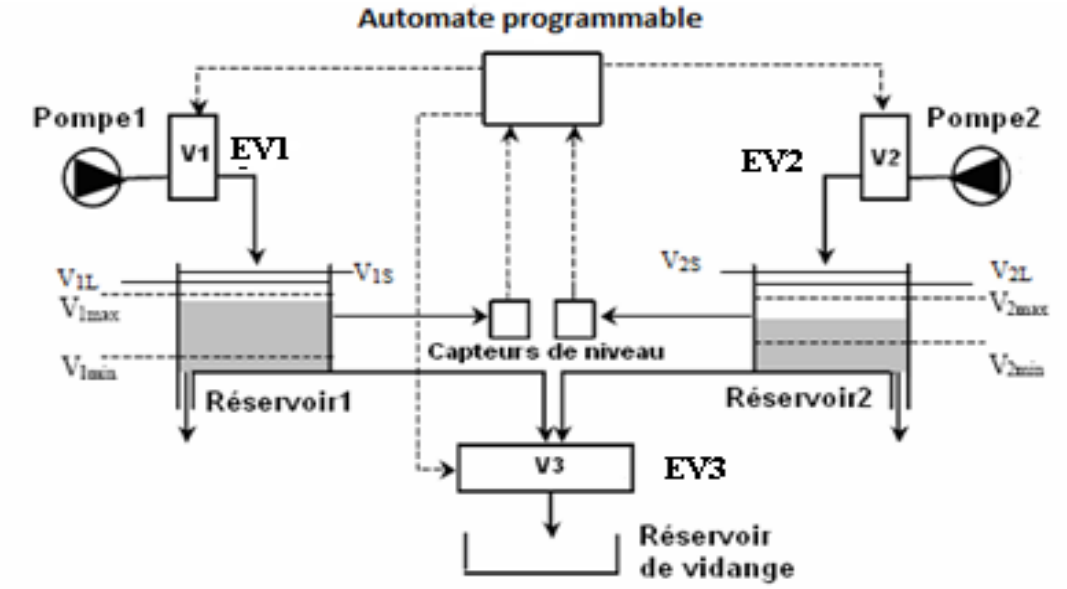



**Figure 4.3** Système de régulation de volume de deux réservoirs à redondance passive.

Si les électrovannes EV1 ou bien EV2 tombent en panne, l'automate programmable peut encore agir sur le volume de liquide dans le réservoir par l'intermédiaire de l'électrovanne de secours (EV3) destinée à la vidange, tant que celle-ci reste opérationnelle. Si l'électrovanne EV3 aussi tombe en panne, cela conduit au débordement du réservoir. Pour simplifier, nous supposons que :

- seules les trois électrovannes, (EV1, EV2 et EV3) et les deux capteurs de 1et 2 peuvent subir des défaillances [20],
- les électrovannes EV1 et EV2, prévues pour l'alimentation des réservoirs correspondants, peuvent être bloquées en ouverture,
- la défaillance de l'électrovanne EV3 (hors service) conduit le système vers un état de défaillance dangereuse (débordement du réservoir).

Le réservoir 1 travaille comme suit : quand le volume dans le réservoir est égal à Vmax, l'automate programmable fait l'option de fermeture de l'électrovanne EV1. Si l'électrovanne EV1 est défaillante et le volume dans le réservoir dépasse la limite supérieure de sécurité ($V_{1L}$), l'automate exécute l'ouverture de l'électrovanne EV3 pour faire le vidange du réservoir 1.

Si les deux électrovannes EV1 et EV3 sont défaillantes et le volume dans le réservoir dépasse le seuil de sécurité ($V_{1S}$), alors le réservoir 1 déborde.

Le même principe de fonctionnement pour le réservoir 2.

La fonction de sécurité réalisée alors est la protection du système de passer dans un état de débordement du réservoir, donc réduire les défaillances dangereuses dans le système.

### 4.3.2 Modélisation du comportement du système

Les principales méthodes abordées dans ce travail lors d'une analyse de la sûreté de fonctionnement sont : arbre de défaillance, diagramme de fiabilité, réseau de Petri stochastique.

#### 4.3.2.1 Modélisation par l'Arbre de Défaillance

La figure 4.4 illustre l'arbre de défaillances classique relatif aux états de fonctionnement du système étudié sous GRIF (**Gr**aphiques **I**nteractif pour la **F**iabilité) [14].

Le système de régulation de niveau de la figure 4.3 est régi par l'expression logique **R** associée à l'arbre de défaillance de la figure 4.4.

***R**= (((DEF1 **OU** DEF2) **ET** (DEF3 **OU** DEF4)) **OU** DEF5)*

Noté :
DEF1 : défaillance 1, DEF2 : défaillance 2, DEF3 : défaillance 3, DEF4 : défaillance 4, DEF5 : défaillance 5.

Le modèle est constitué à des porte logique ET et OU et des bloques représentent les états des éléments défaillantes capteur 1 ou actionneur 1 qui conduisent la défaillance du réservoir 1. La défaillance du capteur 2 ou actionneur 2 qui conduisent la défaillance du réservoir 2. La défaillance du réservoir 1 et défaillance du réservoir 2 conduisent la défaillance du système.

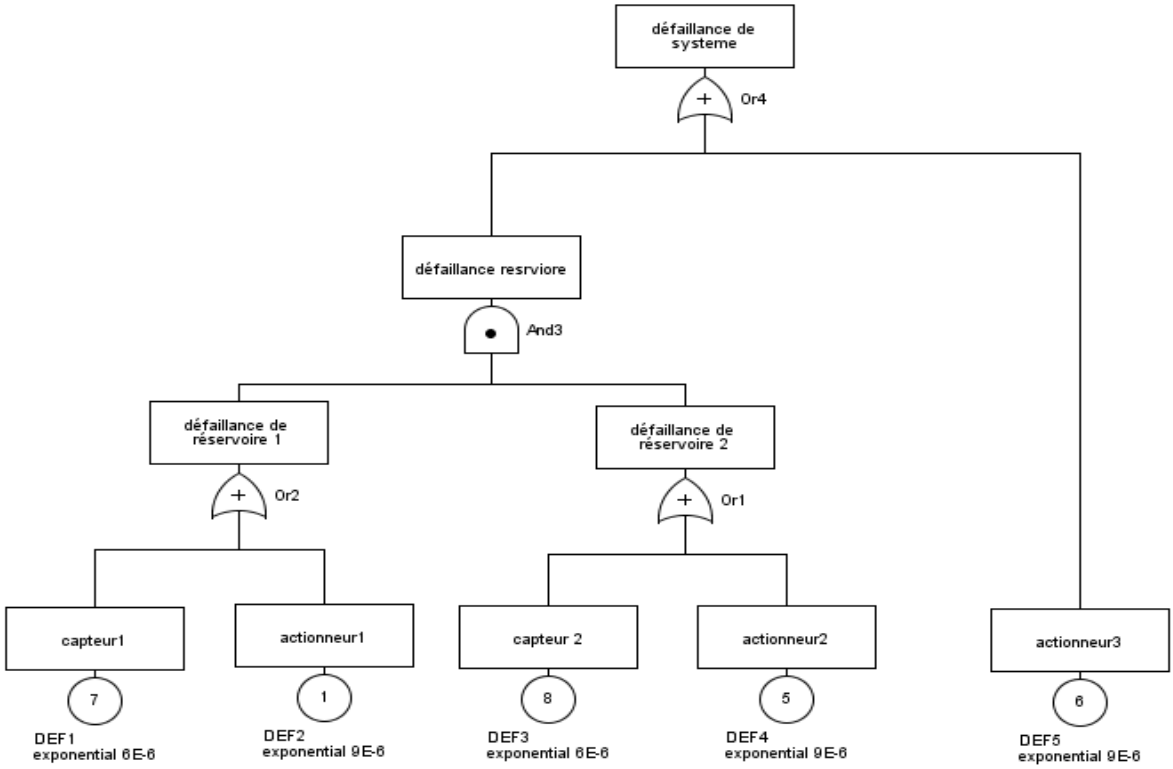



Figure 4.4 : Arbre de défaillances classique du système à deux réservoirs

### 4.3.2.2 Modélisation par diagramme de fiabilité

La figure 4.5 montre la modélisation du système par le diagramme de fiabilité sous GRIF (**Gr**aphiques **I**nteractif pour la **F**iabilité). Le modèle est équivalent au modèle de l'arbre de défaillance de la figure 4.4.

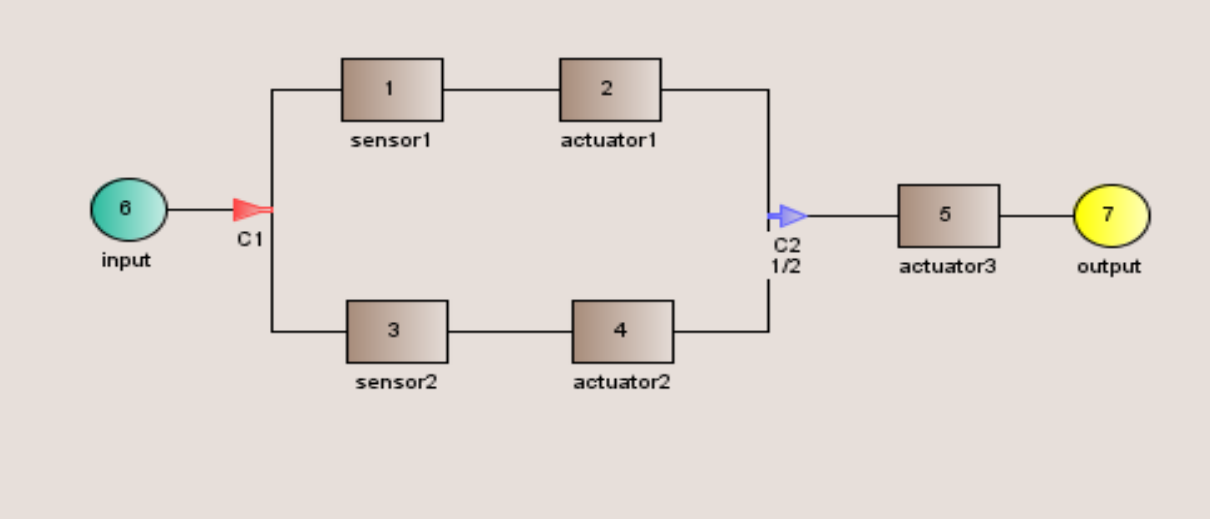



**Figure 4.5** : Diagramme de fiabilité du système à deux réservoirs.

La méthode de bloc diagramme de fiabilité est une représentation logique du fonctionnement du système. Les composants du système sont modélisés par des blocs reliés par des arcs au sens qu'il y a un chemin dans le graphe entre l'entrée et la sortie pour que le système soit fonctionnelle [49].

#### 4.3.2.3 Modélisation par réseau de Petri stochastique

Pour modéliser les comportements aléatoires, discret ou contenu ; ce qui est le cas dans le système mécatronique [20], l'outil RdPS est le mieux adapté sous GRIF (**Gr**aphiques **I**nteractif pour la **F**iabilité) [55]. Dans le cas d'étude, nous procédons à l'injection des défaillances. Les systèmes mécatroniques sont des systèmes hybrides comprenant à la fois des variables continues et discrètes. La dynamique continue est généralement fournie par différentielle et algébrique tandis que la partie discrète est modélisée par des automates ou des transitions vers des états [53]. Les systèmes mécatroniques sont des systèmes fiables et protègent dans début temps mais après plusieurs utilisation dans long temps (10000 heur) la fiabilité et la disponibilité de ces systèmes est diminué dans ce cas la en remplace les éléments du système classique (capteur, actionneur) par des instruments intelligents (capteur, actionneur) donc on résulte un système mécatronique intelligent sur et plus fiable que le système classique.

La modélisation du comportement du système complet est l'ensemble des modèles du capteur et de l'automate et de l'actionneur relient ente eux dans le cas classique et avec intelligence. Dans ce cas d'étude il ya une redondance du capteur (deux capteurs de niveau), une redondance de l'actionneur (trois électrovannes EV1, EV2, EV3).

##### 4.3.2.3.1 Modèle du capteur

###### 4.3.2.3.1.1 Modèle du capteur classique

Le modèle classique du capteur est décrit par le schéma de la figure 4.6. Dans ce modèle les places **P1** et **P2** représentent respectivement l'état de fonctionnement et de dysfonctionnement du capteur. Les places **P3** jusqu'à **P5** représentent la partie de qualification de défaillance du capteur dans un état danger ou sur, la place **P6**(Tc) représente l'état de test du capteur par l'automate.

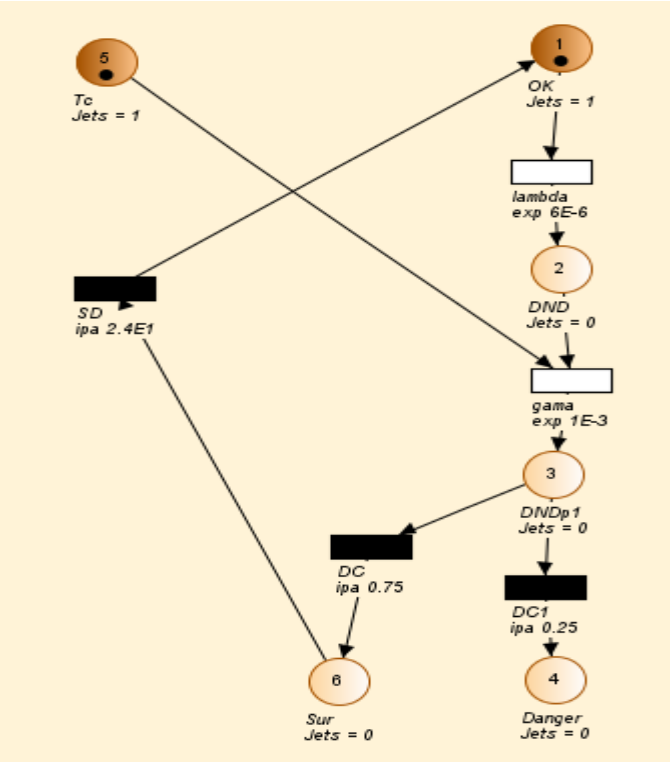



**Figure 4.6** : Modèle du capteur classique.

Le modèle de l'actionneur est équivalent au modèle du capteur de la figure 4.6, mais chacun avec ses propres paramètres. Les taux de défaillance de chaque élément (capteur, actionneur) [54] sont : *lambda-capteur* est égal à 6E-6 $h^{-1}$ et *lambda-actionneur* est égal à 9E-6 $h^{-1}$ [3] [9][14][21].

#### 4.3.2.3.1.2Modèle du capteur intelligent

Le modèle du capteur intelligent est décrit par le schéma de la figure 4.7. La partie fonctionnelle est décrite respectivement par l'ensemble des places et des transitions allant de ***P1*** à ***P6*** et de ***T1*** à ***T9***. La présence du jeton dans la partie gauche représente le bon fonctionnement du capteur.

Dans ce modèle du capteur, un certain nombre de défaillances sont exprimées. Il s'agit des défaillances sûres (place ***Sûr***) et défaillances dangereuses (place ***Danger***). Un taux de couverture de diagnostic ***DC*** est représenté par la transition ***DC***.

La norme IEC 61508 [12] défini le taux de couverture de diagnostic (***DC***) comme étant le rapport entre le taux de défaillances dangereuses détectées (par un test de diagnostic) et le taux total des défaillances dangereuses (détectées et non détectées) [8] [14].on traduise la

partie d' intelligence par la fonctionnalité de l'autodiagnostic par le capteur intelligent donc faire la détection des défaillances dangereuses et les défaillances sûres dans ce cas là le taux de défaillances dangereuses détectées $\boldsymbol{\lambda_{DD}}$ est élevé lors de l'occurrence de défaillances qui conduite à l'augmentation du taux de couverture de diagnostic (***DC***). Ce taux est représenté par la relation 3.3 dans la section (3.2.5) [8].

La relation de proportionnalité entre les défaillances sûres et les défaillances dangereuses est donnée par la relation 3.4 dans la section (3.6.2.1.2).

Plus ce taux est important, plus grande est la confiance dans le système instrumenté de sécurité du fait que les situations sûres prédominent par rapport aux situations dangereuses lors de l'occurrence de défaillances.

Après l'occurrence d'une défaillance sûre, il y a possibilité de restaurer le système par le franchissement de la transition déterministe (***SD***) dont la durée est égale au temps nécessaire à la restauration complète du système. La présence d'une marque dans la place ***P6*** autorise un autotest du capteur géré localement. Les défaillances non détectées ***DND*** peuvent être qualifiées de sûres ou de dangereuses suite à l'exécution de l'autotest [3] [9] [14][21].

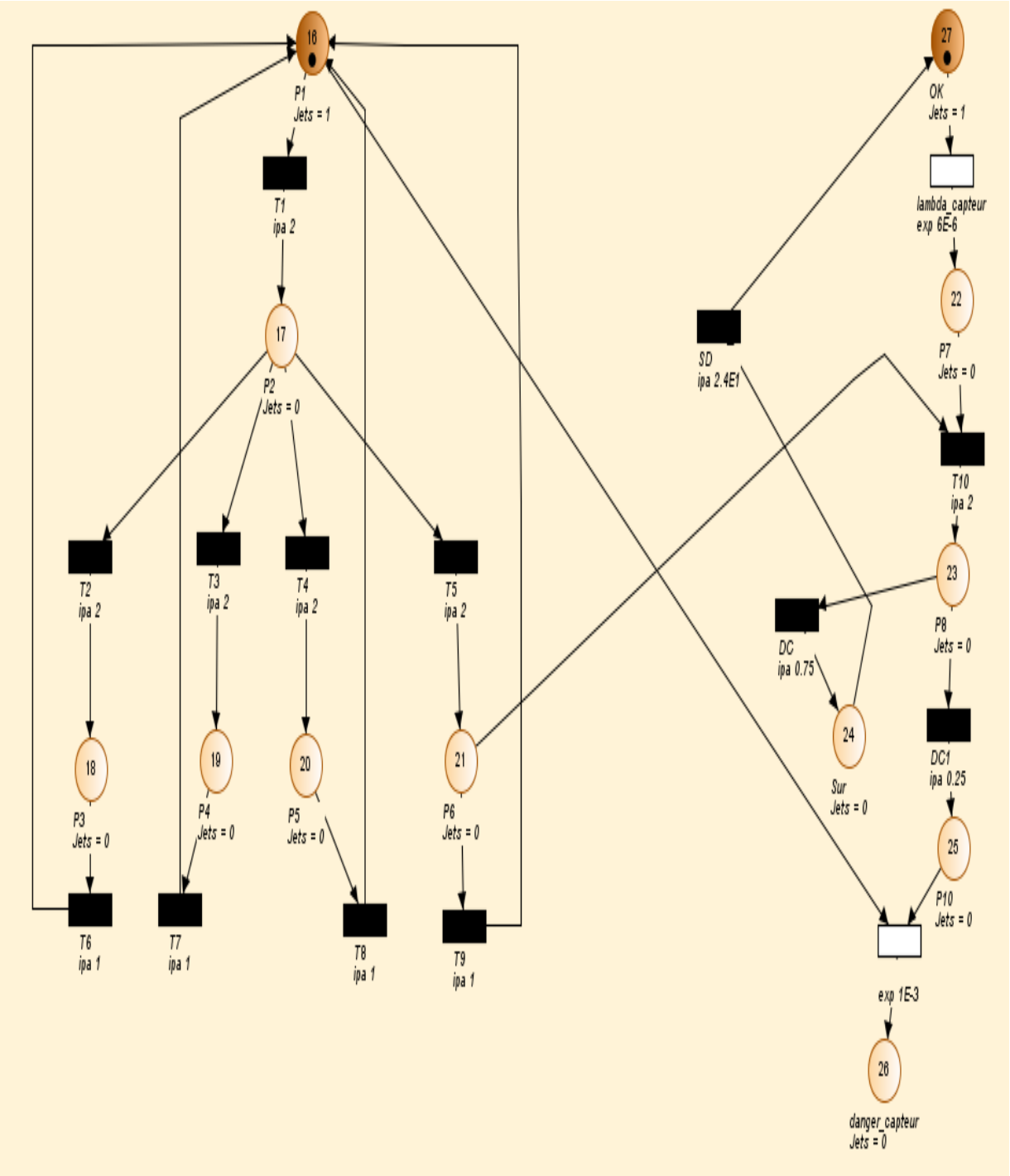



**Figure 4.7** : Modèle du capteur intelligent.

Le modèle de l'actionneur intelligent est équivalent au modèle du capteur de la figure 4.7, mais chacun avec ses propres paramètres.

#### 4.3.2.3.2 Modèle de l'automate

Le modèle de l'automate de la figure 4.8 montre une représentation de deux parties, l'une fonctionnelle et l'autre dysfonctionnelle.

La partie fonctionnelle est décrite par l'ensemble des places et des transitions allant respectivement de ***P1*** à ***P5*** et de ***T1*** à ***T8***. Cycliquement, l'automate réalise ses propres autotests ainsi que des autotests du capteur et de l'actionneur.

La présence d'un jeton dans les places ***P3, P4*** ou ***P5*** autorise l'autotest de l'un des dispositifs précités selon une politique de test gérée par l'automate lui même.

Les autotests des différents dispositifs sont gérés localement suivant une politique de test qui consiste à allouer la même durée de test pour les différents dispositifs et a commencer par le test du capteur (***Tc***), puis l'actionneur (***Tv***) et enfin l'automate (***Ta***). Pour la partie dysfonctionnelle, il faut s'assurer que le jeton est soutiré de la partie fonctionnelle là où il se trouve lorsque le système tombe en panne sûre ou dangereuse. Le taux de défaillance de l'automate est : *lambda-automate* est égal à 2E-5 $h^{-1}$[9][14] .L'automate peut être également restauré en cas de défaillance sûre [9][14].

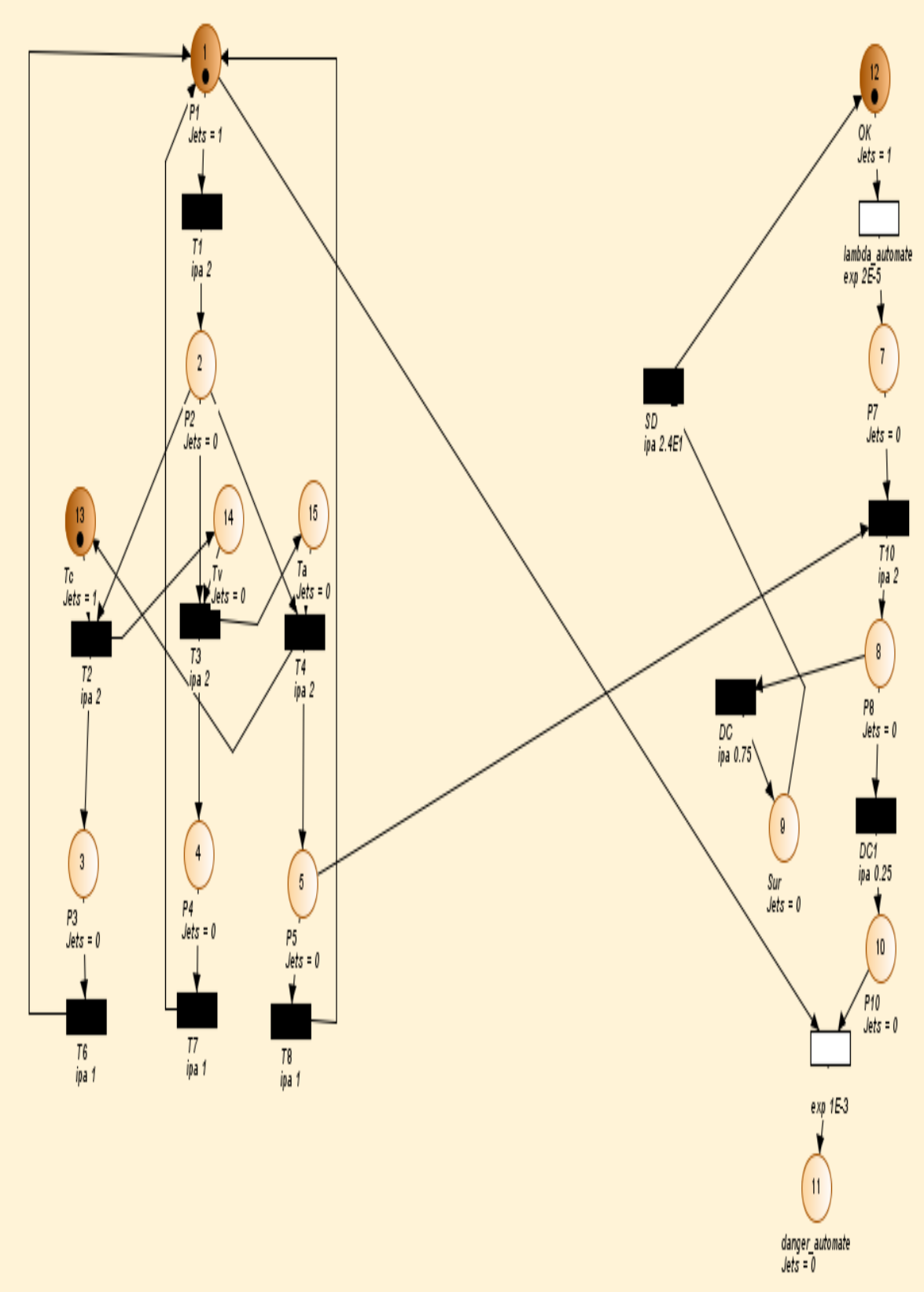



**Figure 4.8** : Modèle de l'automate.

#### 4.3.2.3.3 Modèle du réservoir 1

Le modèle  classique de réservoir 1 est décrit par le schéma de la figure 4.9.

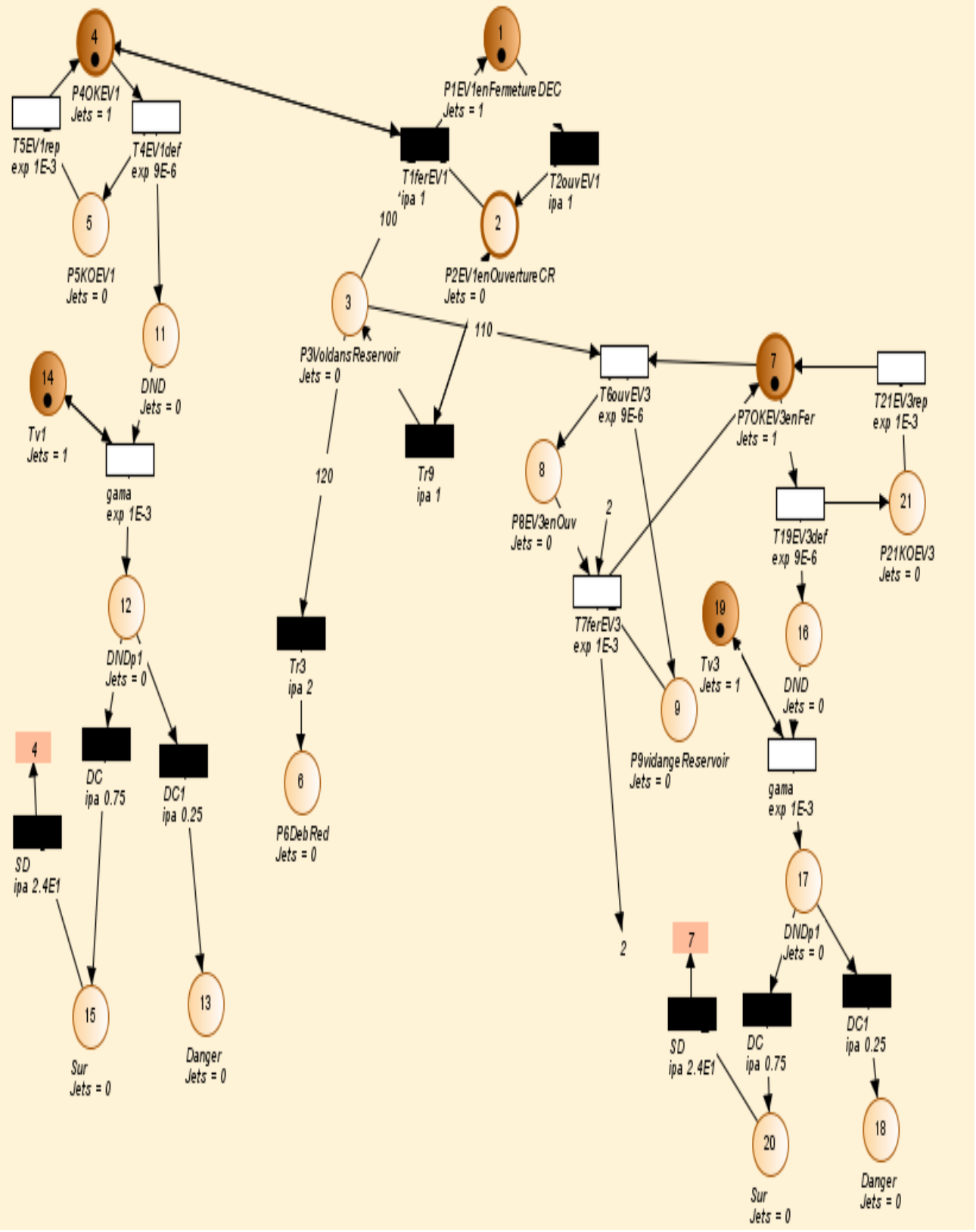



**Figure 4.9** : Modèle de réservoir 1.

Le modèle du réservoir 2 est identique à celui du réservoir 1.

Dans ce modèle les places **P1**et **P2** représentent respectivement l'état de fermeture et de l'ouverture de l'électrovanne EV1 du réservoir 1. La place **P3** représente l'état du remplissage de l'eau dans le réservoir 1. Les places **P4**, **P5** représentent respectivement l'état de bon fonctionnement et de panne de l'électrovanne EV 1. Les places **P11** jusqu'a **P15** représentent la partie de qualification de défaillance de l'électrovanne EV1dans un état danger ou sûr [9] [14].

Les places **P7** et **P8** représentent respectivement l'état de fermeture et de l'ouverture de l'électrovanne EV 3 du réservoir 1, les places **P7**, **P21** représente respectivement l'état de bon fonctionnement et de panne de l'électrovanne EV 3, la place **P9** représente l'état de vidange du réservoir 1. Les places **P16** jusqu'a **P20** représentent la partie de qualification de défaillance de l'électrovanne EV3 dans un état danger ou sûr. La place **P6** représente l'état de débordement du réservoir 1[9] [14].

La modélisation du système classique est équivalent aux relier les modèles classique des éléments du système entre eux suivant : l'automate, les deux capteurs de niveau, les deux électrovannes, les deux réservoirs selon la Figure 4.3. Dans le cas du système intelligent la modélisation est la même mais remplace les modèles classiques par les modèles intelligent des éléments du système étudier [9] [14].

### 4.3.3 Simulation et analyses

Le but de la simulation est d'observer le comportement du système étudié selon la structure classique comparativement avec la structure intelligence. On utilise alors l'approche des réseaux de Petri stochastique (RdPS) pour modéliser le comportement du système car nous avons remplacé les modèles des capteurs et des actionneurs (électrovannes) classiques par des modèles intelligents. L'outil logiciel de simulation est utilisé GRIF (**Gr**aphiques **I**nteractif pour la **F**iabilité), adapté pour l'étude de la fiabilité et la disponibilité avec les deux indicateurs de sécurité PFD et PFS. Le taux de couverture de diagnostic ***DC*** dans cette étude est égal à 0.75 et le taux de restauration ***SD*** est égal 0.24, la période d'échantillonnage est égale 0.5 pour l'ensemble des dispositifs (capteur, automate, actionneur). La durée de simulation de 10000 heures qui correspond à un intervalle entre deux tests périodiques [9] [14].

Pour apprécier l'apport des systèmes intelligents nous soumettons le système en situation classique et intelligent à une défaillance provoquée.

L'injection d'une défaillance selon les deux situations (classique et intelligent) et pour les trois éléments considérés (capteur, actionneur, automate). Cela se traduit par le franchissement de la transition lambda_aut pour l'automate par exemple. La partie dysfonctionnelle de l'automate est alors représentée à droite de la figure 4.8.

Les méthodes d'analyse utilisées sont :

- ✓ ***Pour la disponibilité* :**

À partir des résultats de simulation du modèle du système, nous considérons la disponibilité selon le ratio suivant :

La disponibilité(%) = temps de séjour(h)/durée d'histoire(h)

Le temps de séjour dans la place (27) correspondant à (OK_capteur) de la figure 7 ; il en est de même pour l'actionneur. Le temps de séjour dans la place (12) correspondant à (OK_Automate) de la figure 4.8 [9] [14]

La disponibilité du système est égale au produit des disponibilités du capteur, de l'automate et de l'actionneur [9] [14].

Ou bien :

Le calcul de la disponibilité se fait par l'équation suivante :

$$A(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} \qquad (4.3)$$

- ✓ ***Pour la fiabilité:***

***DH*** = durée d'histoire en heures (h)

***MTTF*** = durée avant la première panne en heures (h)

Le calcul de la valeur du MTTF dans la place (27) par exemple correspondant à (OK_capteur) dans la figure 4.7, est réalisé par la relation suivante :

*MTTF = DH- Temps de séjour dans la place (27)* (4.4)

A partir de la valeur du MTTF, nous pouvons déduire facilement le taux de défaillance $\boldsymbol{\lambda}$ qui s'exprime sous la forme :

$\lambda$ ($h^{-1}$)=1/MTTF(h) (4.5)

La fiabilité peut être exprimée selon une loi exponentielle. Elle est utilisée pour la période de vie utile c'est-à-dire pour λ constant. Son expression est donnée par l'équation suivante :

$$R(t)(\%) = e^{-\lambda t} \quad (4.6)$$

La fiabilité d'un ensemble de n composants montés en parallèle s'exprime par :

$$R(t) = 1 - \prod_{i=1}^{n}(1 - R_i\,(t)) \quad (4.7)$$

Si les n composants sont en série, la fiabilité résultante devient :

$$R(t) = \prod_{i=1}^{n} R_i\,(t) \quad (4.8)$$

Après le lancement de simulation, par la fonction MOCA, On calcule les valeurs de PFD et PFS à partir du temps de séjour dans les places P11 (*Danger-automate)* et *P9 (Sûr)* respectivement de la figure 4.8, voir l'annexes C, puis calculé indisponibilité selon la relation :

L'indisponibilité(%) = temps de séjour(h)/durée d'histoire(h).

Les valeurs relevées des PFD et PFS pour système classique et un système avec intelligence sont données respectivement sur les tableaux 4.1 et 4.2.

| Temps (h) | **PFD** | **PFS** |
|---|---|---|
| **1000** | $0{,}521.10^{-2}$ | $1{,}48.10^{-2}$ |
| **4380** | $1{,}65.10^{-2}$ | $2{,}81.10^{-2}$ |
| **5000** | $1{,}85.10^{-2}$ | $4{,}25.10^{-2}$ |
| **8760** | $2{,}21.10^{-2}$ | $6{,}15.10^{-2}$ |
| **10000** | $3{,}82.10^{-2}$ | $9{,}25.10^{-2}$ |

**Tableau 4.1** : PFD et PFS pour un système classique.

| Temps (h) | **PFD** | **PFS** |
|---|---|---|
| **1000** | $0{,}0112.10^{-2}$ | $1{,}91.10^{-2}$ |
| **4380** | $0{,}0172.10^{-2}$ | $8{,}52.10^{-2}$ |
| **5000** | $0{,}0191.10^{-2}$ | $13{,}1.10^{-2}$ |
| **8760** | $0{,}25.10^{-2}$ | $17{,}2.10^{-2}$ |
| **10000** | $0{,}425.10^{-2}$ | $22{,}5.10^{-2}$ |

**Tableau 4.2** : PFD et PFS pour un système avec intelligence.

A partir des résultats des tableaux 4.1 et 4.2 on va calculer la valeur moyenne de PFD ($PFD_{moy}$) pour analysé le niveau d'intégrité de sécurité (SIL) du système.

- ✓ ***Dans le cas du système classique***

On relève les valeurs de $PFD_{moy}$ à partir de tableau 4.1.

$PFD_{moy} = PFD_{avg} = (0{,}00521+0{,}0165+0{,}0185+0{,}0221+0{,}0382) / 5$

$PFD_{avg}= 0{,}020102=2{,}0102.10^{-2}$, donc la valeur de $\boldsymbol{PFD_{avg}} \epsilon [10^{-2}, 10^{-1}]$.

La valeur de $PFD_{avg}$ correspond à un SIL 1 selon le tableau 3.1.

- ✓ ***Dans le cas du système avec intelligence***

On relève les valeurs de $PFD_{moy}$ à partir de tableau 4.2.

$PFD_{moy} = PFD_{avg} = (0{,}000112+0{,}000172+0{,}000191+0{,}0025+0{,}00425) / 5$

$PFD_{avg}= 0{,}007225=7{,}225 .10^{-3}$, donc la valeur de $\boldsymbol{PFD_{avg}} \epsilon [10^{-3}, 10^{-4}]$.

La valeur de $PFD_{avg}$ correspond à un SIL 2 selon le tableau 3.1.

- ➢ Nous constatons que le système est passé de niveau d'intégrité de sécurité SIL 1 au niveau d'intégrité de sécurité SIL 2 , le niveau de SIL a changé et il est amélioré. Plus le SIL à une valeur élevée plus la réduction du risque est importante et le système étudier qui réalise la fonction de sécurité suite à une analyse de risque, [61] [62]. Ce résultat confirme l'importance et la contribution de l'utilisation des instruments intelligents dans l'amélioration de la sécurité du système.

Les résultats des calcules de la fiabilité et de la disponibilité du système classique et avec intelligence en fonction du temps sous l'outil GRIF est présentées dans les tableaux 4.3 et 4.4 respectivement suivant :

| Temps(h) | Disponibilité du système classique(%) | Disponibilité du système avec intelligence(%) |
|---|---|---|
| **0** | 100 | 100 |
| **1** | 96,4484 | 98,5789 |
| **5** | 94,3679 | 97,8526 |
| **50** | 91,388 | 97,1524 |
| **100** | 91,3398 | 97,0127 |
| **200** | 91,3396 | 97,0127 |
| **500** | 91,3396 | 97,0127 |
| **1000** | 91,3396 | 97,0127 |
| **2000** | 91,3396 | 97,0127 |

**Tableau 4.3** disponibilité du système (%).

| Temps(h) | Fiabilité du système classique(%). | Fiabilité du système avec intelligence(%). |
|---|---|---|
| **0** | 100 | 100 |
| **1** | 99,32 | 99,8 |
| **5** | 96,64 | 99,06 |
| **50** | 71,16 | 88,33 |
| **100** | 50,56 | 73,97 |
| **200** | 25,66 | 46,77 |
| **500** | 3,33 | 7,86 |
| **1000** | 0,11 | 0,25 |
| **2000** | 0 | 0 |

**Tableau 4.4** Fiabilité du système(%).

Les résultats de simulation sont présentés dans les figures 4.10, 4.11 et 4.12.

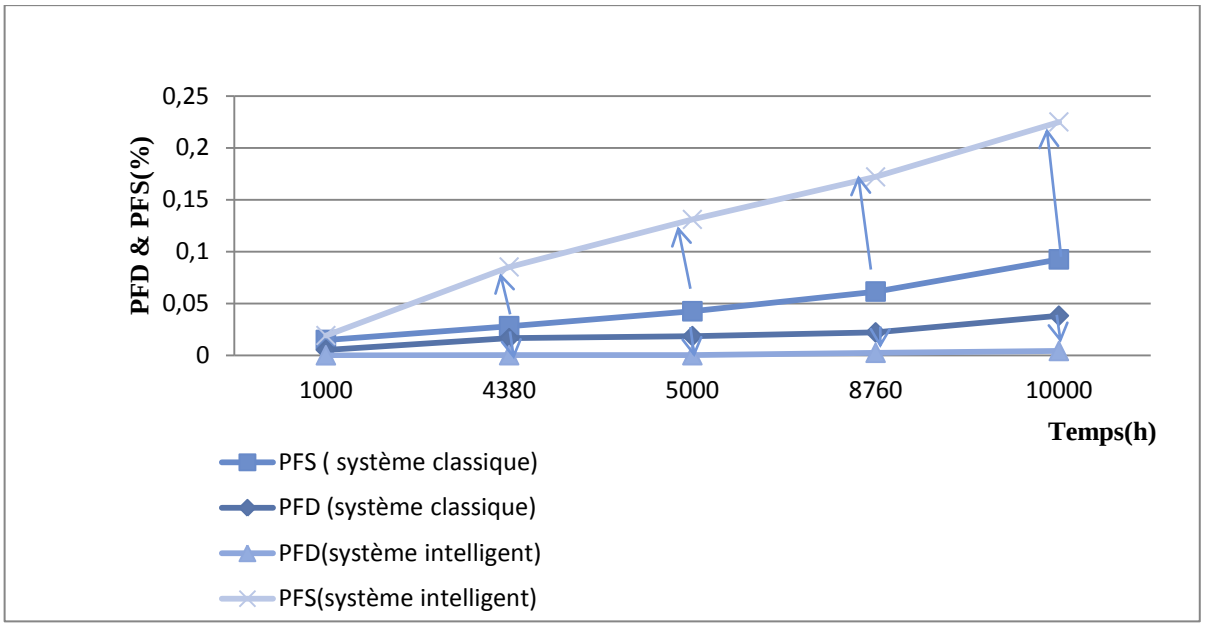



**Figure 4.10** : Evolution des deux indicateurs de sécurité PFD et PFS du système classique et avec intelligence en fonction du temps.

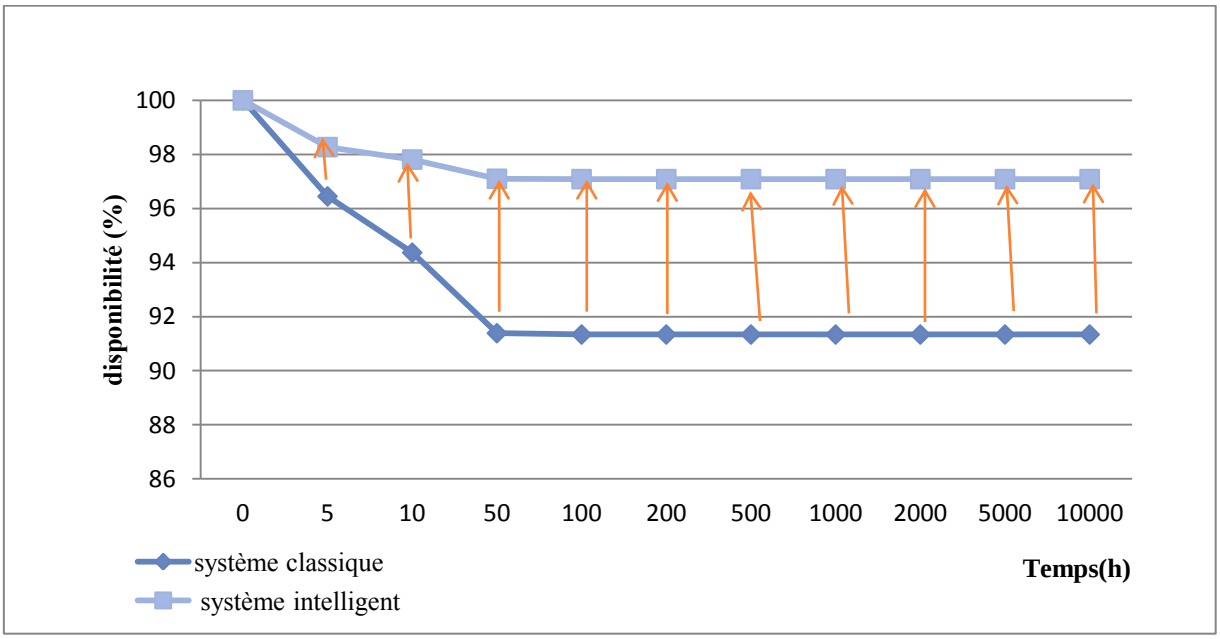



**Figure 4.11** : Evolution de la disponibilité du système en fonction du temps.

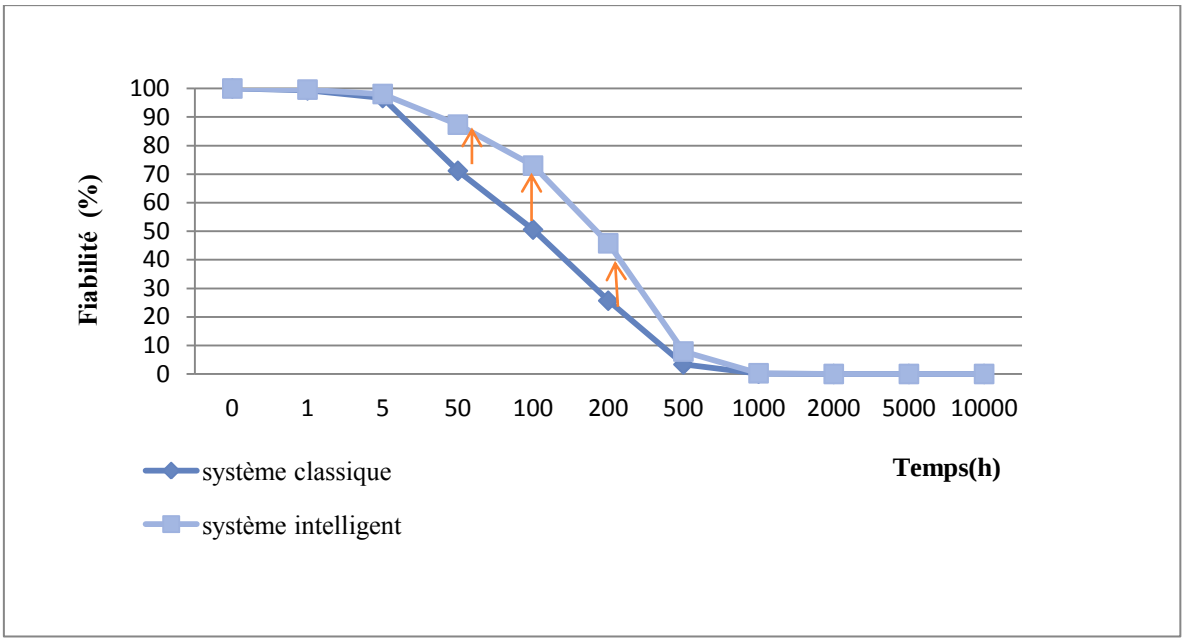



**Figure 4.12** : Evolution de la fiabilité du système en fonction du temps.

La courbe de la figure 4.10 montre l'evolution des deux métriques principales des performances en sécurité PFD et PFS pour une durée de 10000 heures qui est un peu supérieure à une année (8670 heures). Les deux courbes font état d'allures exponentielles. Nous relevons une diminution de la valeur de la PFD et une augmentation de la valeur de la PFS par rapport aux valeurs du système classique, car des défaillances dangereuses se transforment en défaillances sûres.

La conversion de la probabilité de défaillances dangereuses (PFD) en probabilité de défaillances sûres (PFS) peut être exprimée par l'effet de la fonctionnalité d'autodiagnostic d'un instrument intelligent.

L'autodiagnostic capacité d'un instrument à effectuer l'évaluation de son état de fonctionnement et de diagnostiquer l'élément éventuellement en dysfonctionnement.

Les figures 4.11 illustrent l'évolution temporelle de la disponibilité du système étudié classique et avec intelligence pour une durée de 10000 heures qui est un peu supérieure à une année (8670 heures). Cette disponibilité décroissante dans le temps vers une valeur fixe est appelée disponibilité asymptotique. Pour le système classique, la disponibilité asymptotique tend vers la valeur de 91,3396 %. Après l'intégration de l'intelligence la disponibilité asymptotique devient 97,0127%. On constate alors une amélioration sur la disponibilité pour

le système à intelligence distribuée a cause de l'apport d'utilisation des instruments intelligents.

La figure 4.12 illustrent l'évolution temporelle de la fiabilité du système étudié classique et avec intelligence pour une durée de 10000 heures qui est un peu supérieure à une année (8670 heures). La variation de la fiabilité suit elle aussi, la même déclinaison dans le temps. Partant d'une valeur maximale, la courbe décroit selon une exponentielle. Après comparaison entre la courbe de fiabilité du système classique et avec intelligence, nous remarquons qu'il y a une amélioration de la fiabilité pour le système à intelligence distribuée confirme les avantages d'utilisation des instruments intelligents.

## 4.4 Conclusion

Ce travail basé sur une étude d'évaluation des paramètres de sûreté de fonctionnement d'un système mécatronique basé sur une étude comparative entre un système classique et le même système à intelligence distribué.

Les mesures de la disponibilité et de la fiabilité du système étudié sont des indicateurs de l'état de bon fonctionnement ou de dysfonctionnement.

La diminution de la valeur de la probabilité de défaillance dangereuse (PFD) et l'augmentation de la valeur de la probabilité de défaillance sûre (PFS) confirme les avantages d'utilisation des instruments intelligents.

La conversion de la probabilité de défaillances dangereuses (PFD) en probabilité de défaillances sûres (PFS) peut être exprimée par l'effet de la fonctionnalité d'autodiagnostic d'un instrument intelligent.

L'amélioration de niveau d'intégrité de sécurité SIL du système dans le cas de l'intelligence confirme la contribution des instruments intelligents dans l'amélioration de la sécurité du système.

Finalement, le travail mené a confirmé l'intérêt de l'approche RdPS qui est bien adaptée à la modélisation du comportement fonctionnel et dysfonctionnel du système étudié dans le cas classique et avec intelligence par apport aux les deux autre méthodes diagramme de fiabilité et l'arbre de défaillance.

# CONCLUSION GENERALE

# Conclusion générale

Le travail présenté dans cette thèse a contribué à l'analyse de la sûreté de fonctionnement (SdF) des systèmes instruments de sécurité dans le but principale est d'exprimé l'apport des instruments intelligents dans l'amélioration de la SdF de ces système.

La méthodologie, que nous avons utilisée, a consisté en la modélisation de l'aspect fonctionnel et dysfonctionnel de ces systèmes en adoptant le formalisme basé sur les réseaux de Petri stochastiques qui assurent la représentation du comportement dynamique de ce type de systèmes. La modélisation est traitée sous la forme d'une approche stochastique utilisant l'outil GRIF (**Gr**aphiques **I**nteractif pour la **F**iabilité).

Les réseaux de Petri stochastiques nous ont permis une représentation du comportement dysfonctionnel du capteur intelligent par un nombre réduit d'élément de base (places, transitions, jetons). GRIF nous permet d'avoir le marquage moyen pour chaque place ainsi que l'écart type associé. Il nous permet aussi de calculer le séjour moyen dans chaque place.

Parmi les avantages de l'utilisation des RDPS, ils peuvent être utilisés au long du cycle de développement d'un processus et décrivent l'aspect architectural et le comportement des systèmes ainsi qu'ils permettent la modélisation des comportements défaillants.

Nous avons pu construire un modèle de simulation d'un système instrumenté de sécurité (SIS)
auquel nous avons incorporé quelques fonctionnalités des instruments intelligents dans le but d'évaluer les performances en sécurité. Ce modèle a ainsi pu être simulé grâce à l'outil GRIF **(Gr**aphiques **I**nteractif pour la **F**iabilité).. Les résultats de simulation ont bien montré l'impact de l'utilisation des instruments intelligents dans une application sécuritaire sur les performances en sécurité. En effet, les valeurs des métriques (PFD et PFS) ont évolué avec l'introduction de fonctionnalités propres aux instruments intelligents illustrant ainsi les mécanismes introduits par ces fonctionnalités.

A travers un premier exemple d'un SIS, nous avons montré qu'un des apports des instruments intelligents est la transformation de défaillances dangereuses en défaillances sûres par le biais de la diminution de la probabilité des défaillances dangereuses et

l'augmentation de la probabilité des défaillances sûres par l'effet d'autodiagnostique d'un instrument intelligent

Le cas d'étude est un système mécatronique concerne la régulation de volume de deux réservoirs en redondance passive avec utilisation d'un seul réservoir à la fois.

Les principales méthodes abordées dans cette application lors d'une analyse de la sûreté de fonctionnement sont : arbre de défaillance, diagramme de fiabilité, réseau de Petri stochastique.

Il convient de déterminer l'approche qui sera la mieux adaptée à la modélisation du cas d'étude et à la prise en charge de l'aspect dynamique. L'outil logiciel de simulation utilisé est GRIF (**Gr**aphiques **I**nteractif pour la **F**iabilité). Les paramètres de la sûreté de fonctionnement traités sont alors : la fiabilité, la disponibilité et les deux indicateurs de sécurité PFD et PFS.

On constat :

- ✓ Les mesures de la disponibilité et de la fiabilité du système étudié sont des indicateurs de l'état de bon fonctionnement ou de dysfonctionnement.
- ✓ La diminution de la valeur de la probabilité de défaillance dangereuse (PFD) et l'augmentation de la valeur de la probabilité de défaillance sûre (PFS) confirme les avantages d'utilisation des instruments intelligents.
- ✓ La conversion de la probabilité de défaillances dangereuses (PFD) en probabilité de défaillances sûres (PFS) peut être exprimée par l'effet de la fonctionnalité d'autodiagnostic d'un instrument intelligent.
- ✓ Finalement, le travail mené a confirmé l'intérêt de l'approche RdPS qui est bien adaptée à la modélisation du comportement fonctionnel et dysfonctionnel du système instrument de sécurité et de système étudié dans le cas classique et avec intelligence par apport aux les deux autre méthodes diagramme de fiabilité et l'arbre de défaillance.

# BIBLIOGRAPHIE

# Bibliographie


[1] Mkhida A.,Thiriet J.M, Aubry J.F., (2008). « Déficience de la validation d'un capteur intelligent et incidence sur les performances d'une boucle de sécurité ».

[2] Mkhida A.,Thiriet J.M., Aubry J.F., (2007) « Modélisation formelle d'un instrument intelligent dans le cadre d'analyse de sureté de fonctionnement ».7ième édition du congrès international pluridisciplinaire Qualita – Tanger (Maroc).

[3] Mkhida A., (2008). « Contribution à l'évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité intégrant de l'Intelligence » Thèse de doctorat.

[4] Innal F., Haddad S., Chebila M., Bahmed L., (2014). «Optimisation des Architectures des Systèmes Instrumentés de Sécurité à l'aide des Algorithmes Génétiques ». Proceedings of Third International Conference on Industrial Engineering and Manufacturing ICIEM'14. Batna University,Algeria ,pp.603-609.

[5] Mkhida A., Thiriet J.M., Aubry J.F., (2008) « Impact de l'utilisation d'un réseau de communication sur les performances en sécurité d'un système instrumente de sécurité » 7e Conférence Internationale de Modélisation et Simulation, « Modélisation, Optimisation et Simulation des Systèmes : Communication, Coopération et Coordination». -MOSIM'08, page 5.

[6] Sallak M., Aubry J.F., (2008). « Conception optimale des systèmes instrumentes de sécurité en présence d'incertitudes ». 16$^{éme}$ Congrès de Maitrise des Risques et de Sureté de Fonctionnement-Avignon, communication 6B-2, page 2.

[7] Thuy N., Adjadi L-E A., Chaumette S., Bouchet S., V.de Dainous., (2008). « Evaluation des performances des Barrières Techniques de Sécurité ». Evaluation des Barrières Techniques de Sécurité, Rapport d'étude n° dra-08-95403-01561B (DCE DRA-73), - Ω.

[8] MECHRI W., (2011). « Evaluation de la performance des systèmes instruments de sécurité à paramètres imprécis ».Thèse de doctorat.

[9] Kharouati A., Debbache N., Menasria Y., (2014) « Utilisation des instruments intelligents pour les fonctions de sécurité d'un système ». III$^{éme}$ Conférence Internationale sur l'Ingénierie Industrielle et Manufacturière, ICIEM'14, Université de Batna, Algérie, 11-13,2014.

[10] Brissaud F., and Charpentier D., (2008). « Capteurs intelligents : nouvelles technologies et nouvelles problématiques pour la sûreté de fonctionnement ».16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement.

[11] Clarhaut J., (2009). « Prise en compte des séquences de défaillances pour la conception de systèmes d'automatisation Application au ferroutage ».Thèse de doctorat, 222 p.

[12] IEC 61508 (1998). Functional safety of Electrical/Electronic/Programmable Electronic (E/E/PE) safety related systems, International Electrotechnical Commission (IEC),

[13] IEC 61511. (2000). Functional safety. Safety Instrumented Systems for the process industry sector. International Electrotechnical Commission (IEC),

[14] Kharouati A., Debbache N.E., (2019). « Contribution of Intelligent Instruments in Improving the Dependability of a Mechatronic Systems ». Instrumentation Mesure Metrologie Vol. 18, No. 1, February,pp. 87-94 Journal homepage: http://iieta.org/Journals/i2m https://doi.org/10.18280/i2m.180114**.**

[15] Norme (2008). NF E 01 -010 – AFNOR.

[16] Isermann R., (2007). « Mechatronic systems - innovative products with embedded control ». Control Engineering Practice, 10:16.

[17] Isermann R., (2000). « Mechatronic systems : concepts and applications ». Transactions of the Institute of Measurement and Control, vol. 22, p. 29-55.

[18] Chalé H. G., Taofifenua O., Gaudré T., Topa A., Lévy N. & Boulanger J. L., (2011). « Reducing the Gap Between Formal and Informal Worlds in Automotive Safety Critical Systems». 21 st Annual INCOSE International Symposium. Denver, USA.

[19] Jallouli M., (2009). « Méthodologie de conception d'architectures de processeur sûres de fonctionnement pour les applications mécatroniques ». Thèse de doctorat, Université Paul Verlaine – Metz, France.

[20] Khalfaoui S., (2003). « Méthode de recherche des scénarios redoutés pour l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile », Thèse de doctorat de l'institut national polytechnique de Toulouse, Année 2003.

[21] Kharouati A., Debbache N.E., Menasria Y., (2012). « Etude de la sûreté de fonctionnement des systèmes instrumentés intelligents», 1er Journées Doctorales sur l'Automatique, les Télécommunications, l'Instrumentation et les Multimédia « JIDATIM'12 », Université Badji Mokhtar d'Annaba, Algérie, 16 et 17 Janvier

[22] Boucerredj L., Debbache N.E., (2011). « Évaluation de la sûreté de fonctionnement des systèmes mécatroniques en utilisant la notion de coupe minimale et la logique linéaire ». Conference International on Systems and Information Processing, Université 8 mai 45 de Guelma.

[23] Perez-Castaneda G-A., (2009). « Evaluation par simulation de la sûreté de fonctionnement de systèmes en contexte dynamique hybride ». Thèse de Doctorat. Institut National Polytechnique de Lorraine.

[24] Demri A., (2010). « Contribution à l'évaluation de la fiabilité d'un système mécatronique par modélisation fonctionnelle et dysfonctionnelle ». Thèse de Doctorat. Université d'Angers.

[25] Brissaud F., (2008). « Contributions à la modélisation et à l'évaluation de la sûreté de fonctionnement de systèmes de sécurité à fonctionnalités numériques». Thèse de doctorat. Institut national polytechnique de lorraine.

[26] Pagetti C., (2012). « Module de sûreté de fonctionnement ». 3ième TR - option SE, 10 décembre 2012.

[27] Batteux M., (2011). « Diagnosticabilité et diagnostic de systèmes technologiques pilotés». Thèse de doctorat, Université Paris-Sud11.

[28] Sallak M., (2007). «Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception : Application aux Systèmes Instrumentés de Sécurité». Thèse de doctorat. Doctorat de l'institut national polytechnique de lorraine

[29] Sylvie L., (2004). « Etudes de sûreté des installations électriques ». Cahier Technique Schneider Electric, n°184.

[30] Vesely W.E., Goldberg F.F., Roberts N.H., Haasl D.F., (1981). « Fault Tree Handbook ». U.S Nuclear Regulatory Commission Washington.

[31] Riera D., Clement E., (2012). « Modélisation dynamique en sûreté de fonctionnement : une avance pour l'analyse des systèmes complexes ». 18ème Congrès de Maîtrise des Risqué et Sûreté de Fonctionnement, 16 – 18 Octobre 2012. Tours.

[32] Watson H.A., (1961). « Launch Control Safety Study ». Section VII, Vol. 1, Bell Labs, Murray Hill, NJ.

[33] Ledoux J., Gaudoin O., (2007). « Modélisation aléatoire en fiabilité des logiciels ». Edition Hermes Science Publications.

[34] Villemeur A., (1988). « Sûreté de fonctionnement des systèmes industriels ». Edition Eyrolles.

[35] CEI 50 191. (1990). « Vocabulaire Electrotechnique International ». Sûreté de fonctionnement et qualité des services, Chapitre 191.

[36] Belhadaoui H., (2011). « Conception sûre des systèmes mécatroniques intelligents pour des applications critiques ». Thèse de Doctorat. Institut National Polytechnique de Lorraine.

[37] Laprie J.C., (2004). « Sûreté de fonctionnement informatique : concepts, défis, directions ». ACI Sécurité et Informatique, CNRS, LAAS, Toulouse, 15 – 17 novembre.

[38] NF EN 292 – 1, (1991). Sécurité de machines – Notions fondamentales, principes, généraux de conception – Partie 1: Terminologie de base – Méthodologie.

[39] Boucerredj L., (2015). «Sûreté de Fonctionnement : Recherche des Scénarios Critiques dans les Systèmes Mécatroniques». Thèse de doctorat, Université Badji Mokhtar Annaba, Algérie.

[40] Romain B., (2009). « Analyses de sûreté de fonctionnement multi-systèmes ». Thèse de doctorat, Université Sciences et Technologies - Bordeaux I.

[41] Boumelita D., (2012). « Etude de la sécurité d'un système d'alimentation en eau potable par réseau de Pétri hybride », JD'12, l'Automatique, les Télécommunications, l'Instrumentation et les Multimédia « JIDATIM'12 », Université Badji Mokhtar d'Annaba, Algérie.

[42] Guillerm R., (2011). « Intégration de la Sûreté de Fonctionnement dans les Processus d'Ingénierie Système ». Thèse de doctorat de l'université de Toulouse III – Paul Sabatier.

[43] ARP-4754, (1996). « Certification considerations for highly-integrated or complex aircraft systems ». Society of Automotive Engineers (SAE) standard, November 1996.

[44] DO-178B, (1992). « Software considerations in airborne systems and equipment certification ». RTCA et EUROCAE.

[45] DO-254, (2000). « Design assurance guidance for airborne electronic hardware ». RTCA et EUROCAE.

[46] ARP-4761, (1996). « Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment». Society of Automotive Engineers (SAE) standard.

[47] CEI-61508, (2010). « Functional safety of electrical/electronic/programmable electronic safety-related systems ». International Electrotechnical Commission standard.

[48] ISO-26262, (2008). « Véhicules routiers – sécurité fonctionnelle, version projet de comité ». International Organization of Standardization standard.

[49] Cabau E., (1999). « Introduction à la conception de la sûreté. Cahier technique Schneider », Electric n°144, 1999.

[50] Boumaiza A., Arbaoui F., Saidi ML., (2018). « Intelligent condition monitoring of variable speed wind energy conversion systems based on decentralized sliding mode observer» Advances in Modelling and Analysis C (73)2:37-44. : //doi.org/10.18280/ama_c.730202

[51] Mkhida A., Thiriet J.M., Aubry J F., (2014). « Integration of intelligent sensors in Safety Instrumented Systems (SIS) ». Process Safety and Environmental Protection (92): 142–149. http://dx.doi.org/10.1016/j.psep.2013.01.001.

[52] Shneeman R.D., Lee K.B., (2000) «Distributed Measurement and Control Based on the IEEE1451 Smart Transducer Interface Standards». IEEE Transactions on Instrumentation and Measurement, 49(3).

[53] Boucerredj L., Debbache N. E., (2014 c). « A novel algorithm to optimize the search of failure ». Joint International Symposium on "the Social impacts of Developments in Information, Manufacturing and Service Systems". CIE'44 & IMSS'14 Proceedings, Turkey.es 261 à 267.

[54] Djebabra M., (2006), « Etude de sûreté de fonctionnement d'un système électrique simple. Afrique Science ». ISSN 1813-548X. 2006, pp. 176 – 186.

[55] Bayart.M., Conrard B., Chovin.A., et Robert.M., CIAME (2005). « Capteurs et actionneurs intelligents» ,Techniques de l'ingénieur, S 7 520,

[56] Toulminet G.,(2002-2003) « Capteurs intelligents» , chapitre 6,

[57] Norbert N., (2004). « Du Signal à l'Information : le capteur intelligent » HAL Id: tel-00004468 https://tel.archives-ouvertes.fr/tel-00004468.

[58] Boukala.M.C., Ioualalen M., « Transformations sur les Réseaux de Petri Stochastiques (RdPS), Application à l'Evaluation des Performances » LSI, Département d'Informatique Faculté d' Electronique et d'Informatique U.S.T.H.B.

[59] Mechri W., BenOthman K., (2010). « Probabilistic fuzzy approach for the imprecise evaluation of safety instrumented systems ». International Review of Modeling and Simulation, 3(3) :388–400.

[60] Charpentier P., (2002). «Architecture d'automatisme en sécurité des machines : Etude des conditions de conception liées aux défaillances de mode commun». PhD thèses, Nancy Université, Institut Nationnal Polytechnique de Lorraine, France.

[61] Wang Y., West H.H., Mannan.M. S., (2004). «The impact of data uncertainty in determining safety integrity level ». Process Safety and Environmental Protection, 82:393397.

[62] Schonbeck.M., Rausand.M., Rouvroye J., (2010). «Human and organisational factors in the operational phase of safety instrumented systems : A new approach ». Safety Science, 48:310–318.

[63] Wolfgang V.P., Houtermans.M.J.M. (2005). « The effect of the diagnostic and periodic testing on the reliability of safety systems ». TUV Industrie Service GmbH, Automation, Software, Information Teschnology (ASI).

[64] ISA-TR84 (2002). ISA-TR84.00.02. Safety Instrumented Functions (SIF) - Safety Integrity Levels (SIL) Evaluation Techniques. The Instrumentation, Systems, and Automation Society, 67 Alexander Drive P.O. Box 12277 Research Triangle Park, North Carolina 27709.

[65] Lamy P., (2002). « Probabilité de défaillance dangereuse d'un système : explications et exemple de calcul ». Note Scientifique et Technique 225, Institut national de recherche et sécurité (INRS).

[66] Innal F., (2008). « Contribution à la modélisation des systèmes instrumentés de sécurité et à l'évaluation de leurs performances Analyse critique de la norme CEI 61508 ». PhD thesis, Université Bordeaux I, France.

[67] Barger P. (2003). «Evaluation et validation de la fiabilité et de la disponibilité des systèmes d'automatisation à intelligence distribuée en phase dynamique ». Thèse de doctorat de l'Université Henri Poincaré, Nancy 1.

[68] Mazouni M.H., (2008). « Pour une Meilleure Approche du Management des Risques : De la modélisation Ontologique du Processus Accidentel au Système Interactif d'aide à la Décision ». PhD thesis, Nancy Université, Institut Nationnal Polytechnique de Lorraine, France.

[69] IEC61513 (2001). Centrales nucléaires : Instrumentation et contrôle commande des systèmes importants pour la sureté, Prescriptions générales pour les systèmes. International Electrotechnical Commission (IEC).

[70] IEC62061 (2005). Sécurité des machines : Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurit´es. International Electrotechnical Commission (IEC).

[71] EN50126 (1999). Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS).

[72] EN50128 (2001). Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems.

[73] EN50129 (1998). Safety related electronic systems for signalling.

[74] Liu Y., Rausand M., (2011). « Reliability assessment of safety instrumented systems subject to different demand modes ». Journal of Loss Prevention in the Process Industries, 24:49–56.

[75] Signoret J-P., (2004). « High integrity protection system (hips) overcoming sil calculation difficulties». Technical report, TOTAL document, Pau.

[76] Bouguenna A., (2015). «Simulation matérielle d'un capteur intelligent. Technologie des Microsystèmes Electro-Mécaniques et Microfluidiques ». Mémoire de magister.

[77] YOUNES Y., (2012). « Minimisation d'énergie dans un réseau de capteurs". Mémoire de magister» . Université Mouloud Mammeri de Tizi-ouzou.

[78] Asch G., (1982). « Les capteurs en instrumentation industrielle», Dunod/Bordas, Pais,

[79] Gagniére.J et Macé.J-R (2015). « L'utilisation de capteurs intelligents chez AREVA: enjeux, perspectives et retour d'expériences». 17 International Congress of Metrology. 08007. DOI: 10.1051/Metrology / 2015 08 007. Owned by the authors published by EDP Sciences

[80]Robert.M., Riviere .J. M., Noizette .J. L., & F. Hermann,(1993). « Smart sensors in flexible manufacturing systems» , Sensors and Actuators A, vol. 37-38, pp. 239-246.

[81] Verdone, R., Dardari, D., Mazzini, G. & Conti, A., (2008). «Wireless Sensor and Actuator Networks», Technologies, Analysis and Design", Academic Press, Elsevier, London,

[82] Bayart. M et al., «Capteurs et Actionneurs Intelligents.GT 18-4 CIAME SEE, Doc. S 7520

[83] Mukhopadhyay.S. C., Palmerston North,( 2014) « Internet of Things Challenges and Opportunities, Smart Sensors, Measurement and Instrumentation, Volume 9, Springer International Publishing Switzerland

[84] Cecílio .J, Furtado.P, (2014). « Sensors in Industrial Time-Critical Environments", Computer Communications and Networks», Springer International Publishing Switzerland .

[85] Mukhopadhyay S.C., Jiang J-A., (2013). «Wireless Sensor Networks and Ecological Monitoring», Springer-Verlag Berlin Heidelberg,

[86] Nayak A., Stojmenovic I., (2010). «Wireless Sensor and Actuator Networks Algorithms and Protocols for Scalable Coordination and Data Communication», John Wiley & Sons Ltd.,

[87] Dargie W., et Poellabauer C., ( 2010) « Fundamentals of Wireless Sensor Networks Theory and Practice», Wiley series on Wireless Communications and Mobile Computing, first edition, John Wiley & Sons Ltd.,

[88] Sohraby K., et al., (2007) « Wireless Sensor Networks Technology, Protocols, and Applications», Wiley series on Wireless Communications and Mobile Computing, John Wiley & Sons Ltd.

[89] Mekid S., (2006). « Further Structural Intelligence for sensors Cluster Technology in Manufacturing» . Sensors. Vol 6. pp, 557-577.

[90] Meijer G. C. M., 1994. «Concepts and focus point for intelligent sensor systems», Sensors and Actuators A, vol. 41-42, pp. 183-191.

[91] Tian G., Y., Zhao Z.X., Baines R. W., (2000). « A fieldbus-based intelligent sensor» , Mechatronics, vol. 10, pp. 835-849.

[92] Calvez J.P., (1990). «Spécification et conception des systèmes - une méthodologie», Édition Masson, Paris

[93] Rumbaugh J., Blaha M., Premerlani W., Eddy F., (1991). « Object Oriented Modeling and Design», Prentice Hall International.

[94] Bouras A., (1997) « Contribution à la conception d'architectures réparties : modèles génériques et interopérabilité d'instruments intelligents», Thèse de Doctorat, Université des Sciences et Technologies de Lille.

[95] Albus J.S., (1991). «Outline for a theory of intelligence». IEEE Transactionson Systems. Man, and Cybernetics, Vol. 21, N°. 3,

[96] Tailland J., (2000) « Instruments intelligents : Modèle et outils de conception » thèse de doctorat. l'université de savoie.

[97] Bayart M., Chovin A., « module intelligent pour système automatisé à intelligence distribuée » Lail UPRESA CNRS 8021, CROUZET automatismes SA. france.

# ANNEXES

# Annexe A

# Modélisation par diagramme de fiabilité sous GRIF

## A.1 Les étapes de la modélisation par GRIF

Cette partie à pour objectif de présenter les étapes de modélisation et simulation de notre cas d'étude par l'outil «GRIF».

GRIF : est une plate-forme logicielle d'analyse des systèmes qui permet de déterminer les indicateurs fondamentaux de la sûreté de fonctionnement :

Fiabilité – Disponibilité – Performance – Sécurité

GRIF laisse le choix à l'utilisateur d'opter pour la technique de modélisation la plus adéquate à la résolution du système étudié : blocs diagrammes, arbres de défaillance, graphes de Markov, réseaux de Pétri. Des architectures déjà intégrées dans le logiciel facilitent cette modélisation. Développé au sein de Total, GRIF bénéficie de plus de 25 ans de Recherche et Développement. Cette plate-forme dispose ainsi de moteurs de calcul matures, très performants et aux capacités de modélisation propres à répondre aux besoins de l'ensemble des études fiabilistes.

### A.1.1 Fenêtre principale du module Bloc diagramme de fiabilité

La fenêtre principale est décomposée en plusieurs parties :

• **Barre de titre** : La barre de titre indique le nom du module et le nom du fichier en cours d'édition.

• **Barre de menu** : La barre de menu permet d'accéder à toutes les fonctions de l'application.

• **Barre d’icônes (raccourcis)** : La barre de raccourcis est une barre (horizontale) d’icônes permettant d’accéder plus rapidement aux fonctions usuelles.

• **Barre d’outils** : La barre d’outils (verticale) permet de sélectionner les éléments à utiliser pour la modélisation.

• **Zone de saisie** : Un maximum de place a été laissé à la zone de saisie graphique pour permettre de réaliser le modèle.

• **Arborescence** : L’arborescence est entre la zone de saisie et la barre d’outils. Elle permet de naviguer dans les pages et groupes du document.

• **Modèles** : La liste des modèles se situent en dessous de l’arborescence. Ils sont groupés en deux sous dossier suivant leur lieu d’enregistrement (Répertoire utilisateur ou d’installation).

• **Ensemble des tableaux** : Les tableaux de données sont regroupés dans des onglets à droite de la zone de saisie.

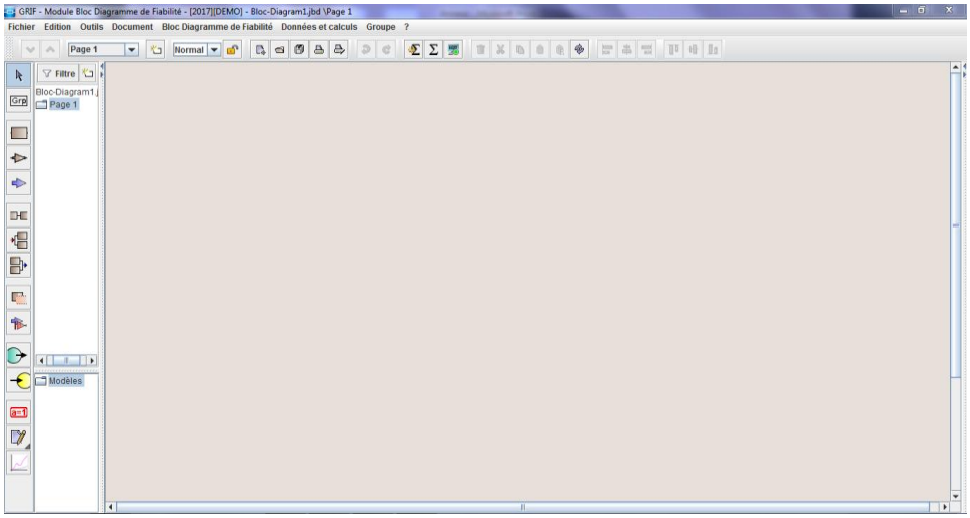



**Figure A.1** Fenêtre principale du module Bloc diagramme de fiabilité.

### *A.1.1.1Barre d'outils verticale*

Chaque modèle utilisé en sûreté de fonctionnement possède sa propre iconographie. L'ensemble de symboles graphiques relatifs aux diagrammes de fiabilité est représenté sur la barre d'icônes placée verticalement à gauche de la fenêtre de saisie. La barre d'outils verticale comporte les éléments suivants : bloc, connecteur, sortie, lien série, lien diviseur, lien k sur n, bloc identique, entrée, source, cible, outils champs dynamique, outils commentaire et outils.

| | |
|---|---|
|  | **Outils de sélection** Permet de sélectionner les objets graphiques dans la zone de saisie. |
|  | **Groupe** Permet d'ajouter un groupe (sous-page) au modèle. |
|  | **Bloc** représenté par un rectangle de couleur brune. |
|  | **Connecteur** représenté par une flèche de couleur brune. |
|  | **Sortie** représentée par une flèche de couleur bleue. |
|  | **Lien série** représenté par un arc non-orienté et permettant de connecter les différents éléments du modèle. |
|  | **Lien diviseur** représenté par une flèche de couleur rouge. |
|  | **Lien K sur N** représenté par une flèche de couleur bleue. |
|  | **Bloc identique** représentée par un bloc en pointillé de couleur rose. |
|  | **Entrée** représentée par une flèche de couleur rouge. |
|  | **Source** représentée par un cercle de couleur verte. |
|  | **Cible** représentée par un cercle de couleur jaune. |
|  | **Outils champs dynamique** Permet de créer des commentaires dynamiques affichant les données du modèle. |
|  | **Outils commentaire** Permet de créer des commentaires statiques. |
|  | **Outils courbe** Permet de tracer des courbes en sélectionnant des résultats de calculs dans la banque de résultats. |

**Tableau A.1** Barre d'outils verticale de diagramme de fiabilité.

### A.1.2Création d'un diagramme de fiabilité

#### *A.1.2.1 Saisie du diagramme*

##### *A.1.2.1.1 Saisie des blocs*

Pour saisir les différents **Blocs**, il suffit de sélectionner le symbole correspondant sur la barre d'outils verticale.

Ensuite à chaque clic gauche de la souris sur la surface de saisie graphique, un nouvel élément est créé. Chacun des blocs du modèle est caractérisé par trois paramètres:

- Un **numéro**: Situés au centre des blocs, ils sont incrémentés automatiquement. Ces numéros sont les vrais identifiants des blocs qui seront utilisés par le moteur de calcul. C'est pour cette raison que deux blocs ne peuvent pas avoir un numéro identique.
- Un **nom**: Un nom par défaut est attribué à chaque bloc ("Bi" pour le bloc numéro "i"). Comme chaque bloc représente, en général, un composant ou un sous-système bien précis, il est fortement conseillé de lui attribuer un nom plus mnémotechnique que celui donné par défaut afin de mieux se repérer dans le modèle et surtout dans le fichier résultat.
- Un **commentaire**: Ce champ permet d'ajouter du texte à un bloc afin de spécifier une particularité. Les commentaires ont pour but final de faciliter la compréhension générale du modèle.
- Une **loi**: C'est l'élément qui va servir à modéliser le comportement aléatoire du bloc c'est à dire celui qui va déterminer à chaque instant si l'état est à **VRAI** ou à **FAUX**. L'utilisateur a la possibilité de choisir parmi vingt trois lois qui doivent dans un deuxième temps être paramétrées (cf. ultérieurement la description détaillée des lois).
- ***Les connecteurs***
  - Fonction: élément pouvant "être la source" et/ou "être la cible" de plusieurs liens.
    1. S'il est la "source" de plusieurs liens, il est appelé connecteur **diviseur**.
    2. S'il est la "cible" de plusieurs liens, il est appelé connecteur **K sur N**.
  - Représentation graphique:
    1. les connecteurs "classiques" sont des triangles de couleur brune;
    2. les connecteurs **diviseurs** sont des triangles de couleur rouge;
    3. les connecteurs **K sur N** sont des triangles de couleur bleue.

Remarque importante: En fonction des liens qui sont reliés au connecteur, ce dernier est converti automatiquement en **diviseur** ou en **K sur N**.

Dans l'exemple ci-dessous, un connecteur **diviseur** a été tracé entre les blocs **B1** et **B3** et un connecteur **K sur N** a été tracé entre **B2** et **B4**.

- Identification: chaque connecteur est défini par

1. un numéro: C'est le "vrai" identifiant (celui qui sera utilisé par le moteur de calcul). Les numéros sont incrémentés automatiquement. Deux connecteurs ne peuvent pas avoir un numéro identique.
2. un nom: Il permet simplement à l'utilisateur de donner au connecteur une appellation lui permettant de mieux se repérer au sein du modèle.

3. un nombre **K** (seulement pour les connecteurs **K sur N**): Ici, **N** est le nombre de connections en entrée du connecteur. Si au moins **K** d'entre elles sont à VRAI, alors la valeur booléenne transmise par la sortie du connecteur est VRAI sinon c'est FAUX.

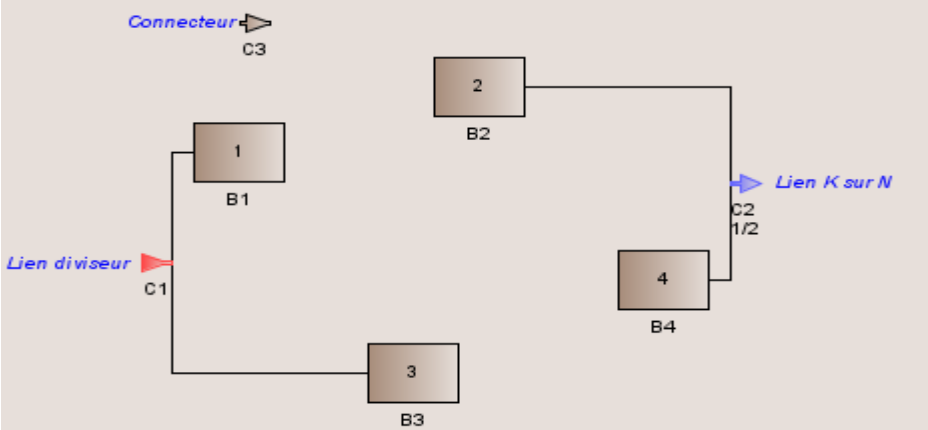



**Figure A.2** Les connecteurs sur GRIF.

## A.2 Bloc diagramme de fiabilité de notre cas d'étude

La figure ci-dessous représente le diagramme de fiabilité qui modélise le comportement du système de régulation de volume de deux réservoirs à redondance passive. Le but était donc de construire un diagramme permettant d'évaluer la disponibilité du système.

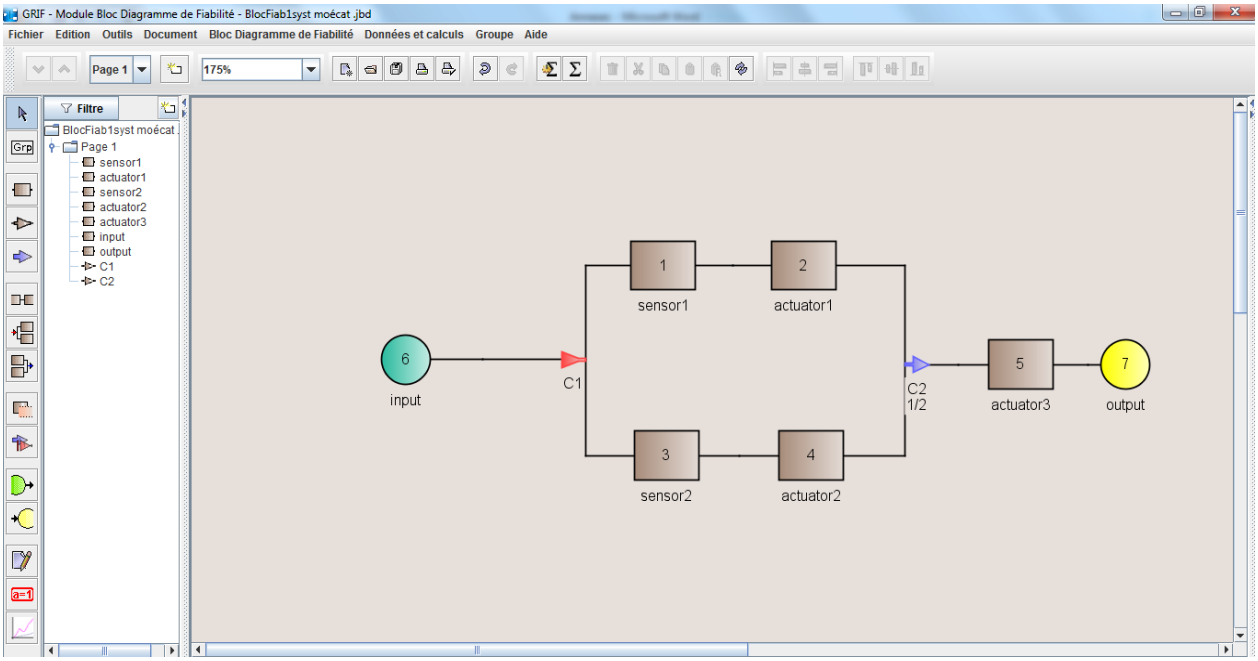



**Figure A.3** Diagramme de fiabilité de notre cas d'étude sur GRIF.

### A.2.1 Calcul de la fiabilité du système

Les calculs s'effectuent en deux étapes:

• le paramétrage des calculs;

• la lecture des résultats dans la banque de résultat.

La fenêtre de paramétrage des calculs est accessible de deux manières différentes : soit par le menu **Données et calculs - configuration et lancement du calcul**.

La fenêtre de paramétrage qui est ainsi ouverte est appelée **Lancement des calculs**.

La fenêtre de paramétrage se décompose en cinq onglets comme la figure ce dessous démontre.

- **Paramétrage des calculs de probabilités** : permet de définir les calculs à effectuer.
- **Indisponibilité** : qui selon les normes notée Q(t), U(t) ou PFD(t)
- **Disponibilité** : A(t) = 1 - U(t)
- **Intensité Inconditionnelle de Défaillance** : qui selon les normes notée W(t), UFI(t) ou PFH(t). C'est la probabilité que le système tombe en panne entre t et t+dt, sachant qu'à t=0 le système n'est pas défaillant.
- **Intensité Conditionnelle de Défaillance (Lambda eq)** : qui selon les normes notée CFI(t). C'est la probabilité que le système tombe en panne entre t et t+dt, sachant que le système n'est pas défaillant à t et qu'à t=0 il n'était pas défaillant non plus.
- **Défiabilité** : F(t) = 1 - R(t)
- **Fiabilité** : R(t) = R(t)=$e^{-\lambda(t)}$

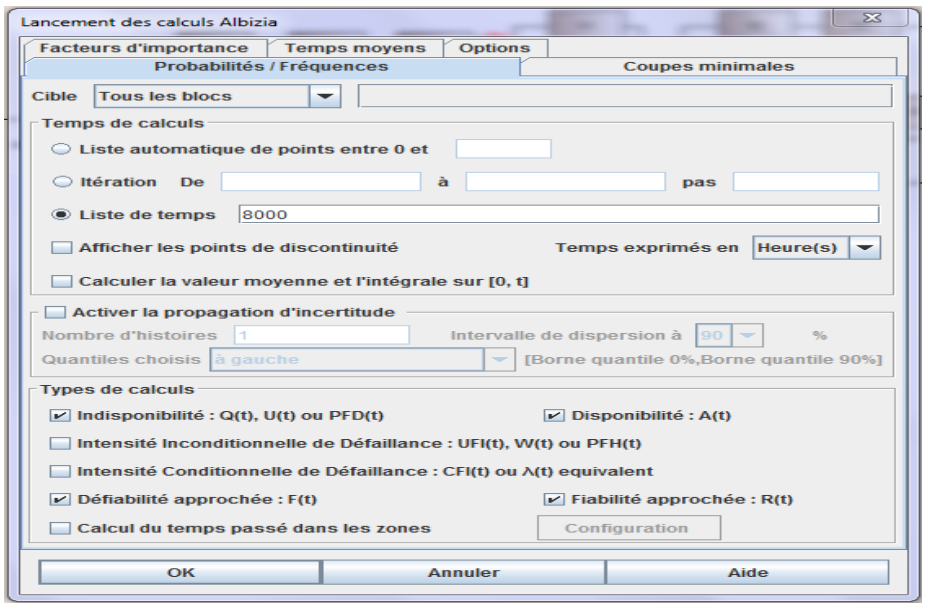



**Figure A.4** Fenêtre des calculs.

Le calcul de la fiabilité R(t) de notre système s'effectuer à l'aide du lancement d'un calcul avec des itérations de 0 à 8000 avec un pas de 100 dans la fenêtre de paramétrage des calculs de probabilités (Probabilités / Fréquences) qui été bien expliqué dans la figure B.5.

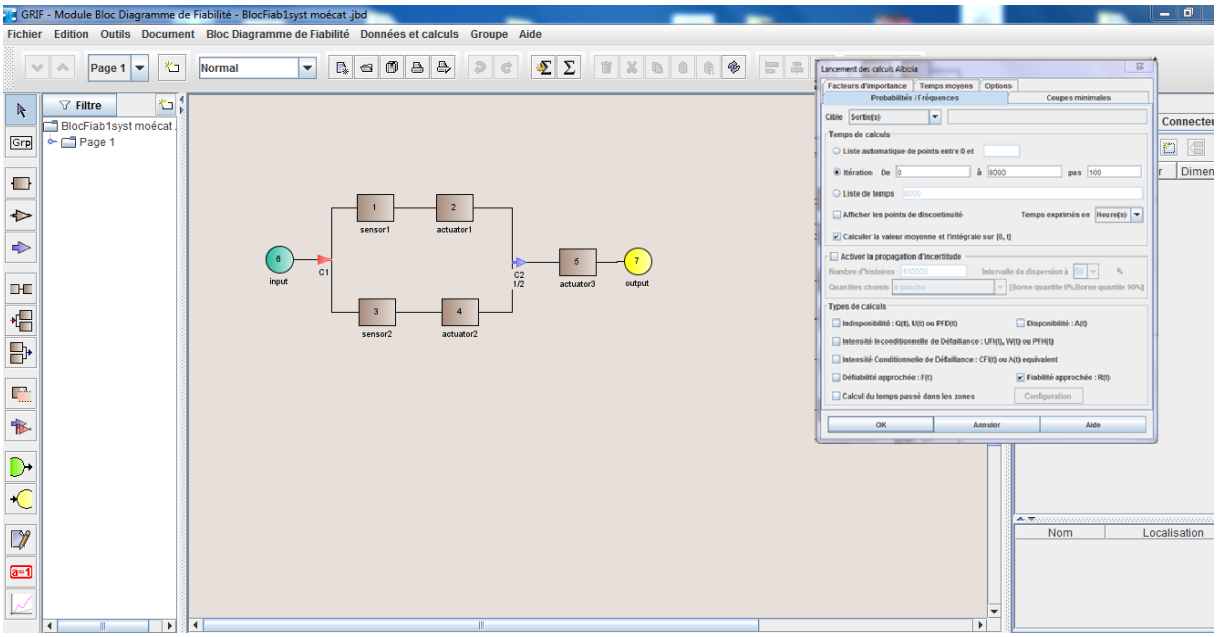



**Figure A.5** Calcul de la fiabilité du système.

### A.2.2 Résultat de la simulation pour la fiabilité

Les résultats sont présentés sous la forme d'une fenêtre composée de 5 onglets:

- Probabilités
- Facteurs d'importance
- Coupes
- Temps moyens
- Résultats
- Info

Afin de mieux étudier le modèle et les résultats, il est possible de tracer des courbes. Pour cela, il suffit de faire un clic gauche sur l'icône correspondante de la barre des tâches verticale. Puis la courbe de la fiabilité montrer dans la figure B.6 suivante donc sera affiché.

Icône **Graphique**: 

La courbe de la fiabilité décroit selon une exponentielle montrée par la figure B.6 :

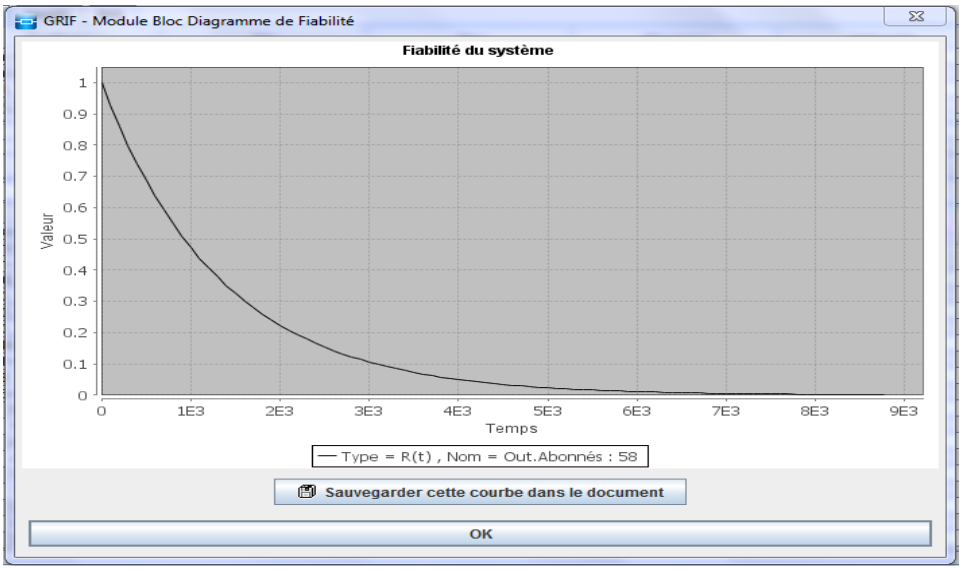



**Figure A.6** Courbe de la fiabilité du système.

### A.2.3 calcul de la disponibilité du système

Le principe de calcul de la disponibilité du système s'exécuter de la même façon que la fiabilité, sauf on a choisi le type de probabilité de calcul et cocher l'icône : Disponibilité A(t).

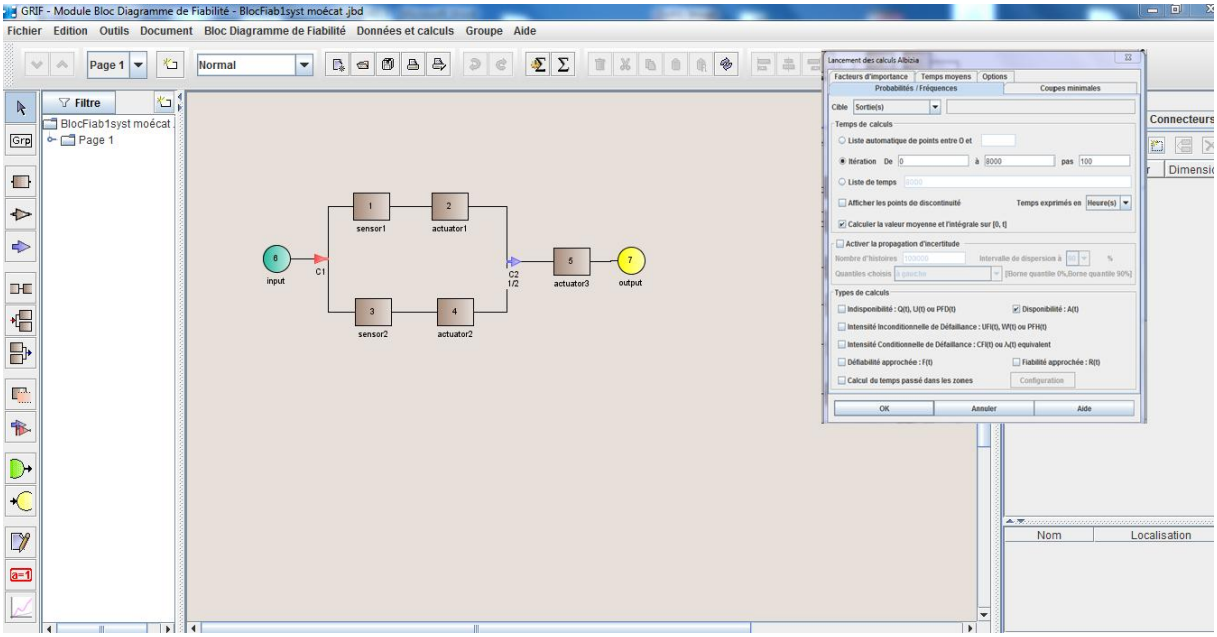



**Figure A.7** Calcul de la disponibilité du système.

### A.2.4 Résultat de la simulation pour la disponibilité

La figure B.8 représente la variation de la disponibilité du système à travers le temps. Cette disponibilité décroissante dans le temps vers une valeur fixe est appelée disponibilité asymptotique.

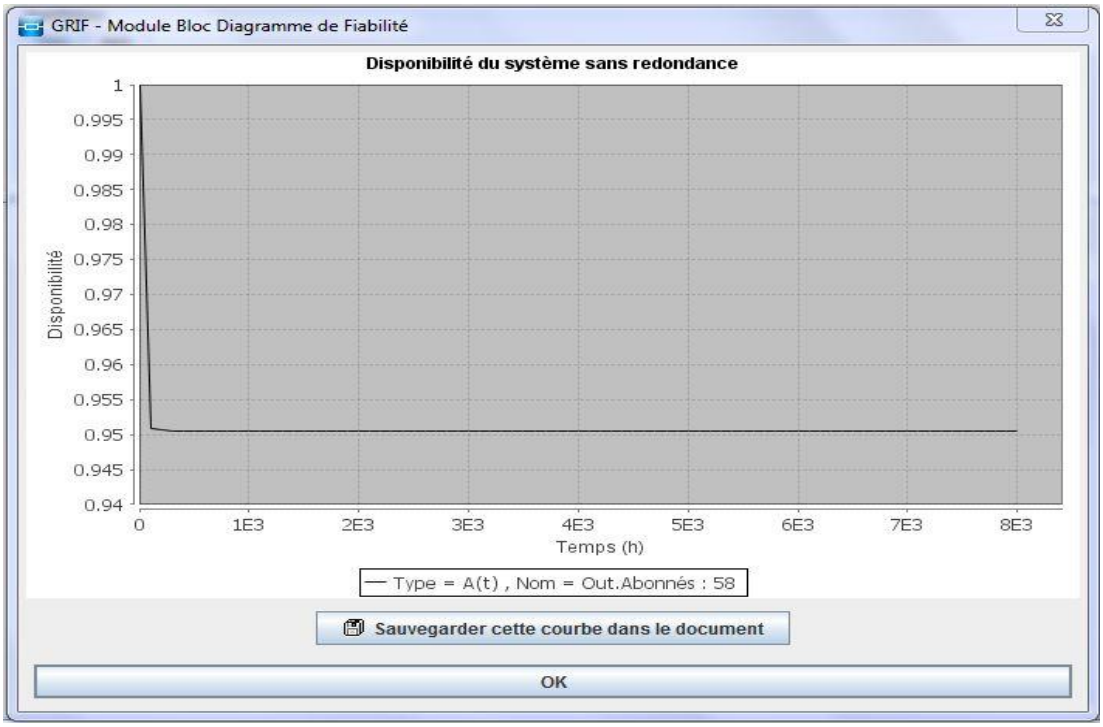



**Figure A.8** Courbe de la disponibilité du système.

# Annexe B

# Modélisation par L’arbre de défaillance sous GRIF

## B.1 Présentation de l’interface

Tree permet de modéliser un système sous la forme d'un arbre de défaillances, une modélisation simple et transverse à tous les domaines (aéronautique, automobile, ferroviaire, pétrolier ...) de par sa logique booléenne. Le module Tree s'appuie sur ALBIZIA, le moteur de calcul par BDD (Binary Decision Diagram) développé par TOTAL. Le point fort d'ALBIZIA est qu'il est capable d'effectuer des calculs analytiques exacts et de fournir rapidement un très grand nombre d'informations sur le système étudié.

### *B.1.1 Fenêtre principale du module arbre de défaillance*

La fenêtre principale est décomposée en plusieurs parties

• **Barre de titre** : La barre de titre indique le nom du module et le nom du fichier en cours d'édition.
• **Barre de menu** : La barre de menu permet d'accéder à toutes les fonctions de l'application.
• **Barre d'icônes (raccourcis)** : La barre de raccourcis est une barre (horizontale) d'icônes permettant d'accéder plus rapidement aux fonctions usuelles.
• **Barre d'outils** : La barre d'outils (verticale) permet de sélectionner les éléments à utiliser pour la modélisation.
• **Zone de saisie** : Un maximum de place a été laissé à la zone de saisie graphique pour permettre de réaliser le modèle.

• **Arborescence** : L'arborescence est entre la zone de saisie et la barre d'outils. Elle permet de naviguer dans les pages et groupes du document.

• **Modèles** : La liste des modèles se situent en dessous de l'arborescence. Ils sont groupés en deux sous dossier suivant leur lieu d'enregistrement (Répertoire utilisateur ou d'installation).

• **Ensemble des tableaux** : Les tableaux de données sont regroupés dans des onglets à droite de la zone de saisie.

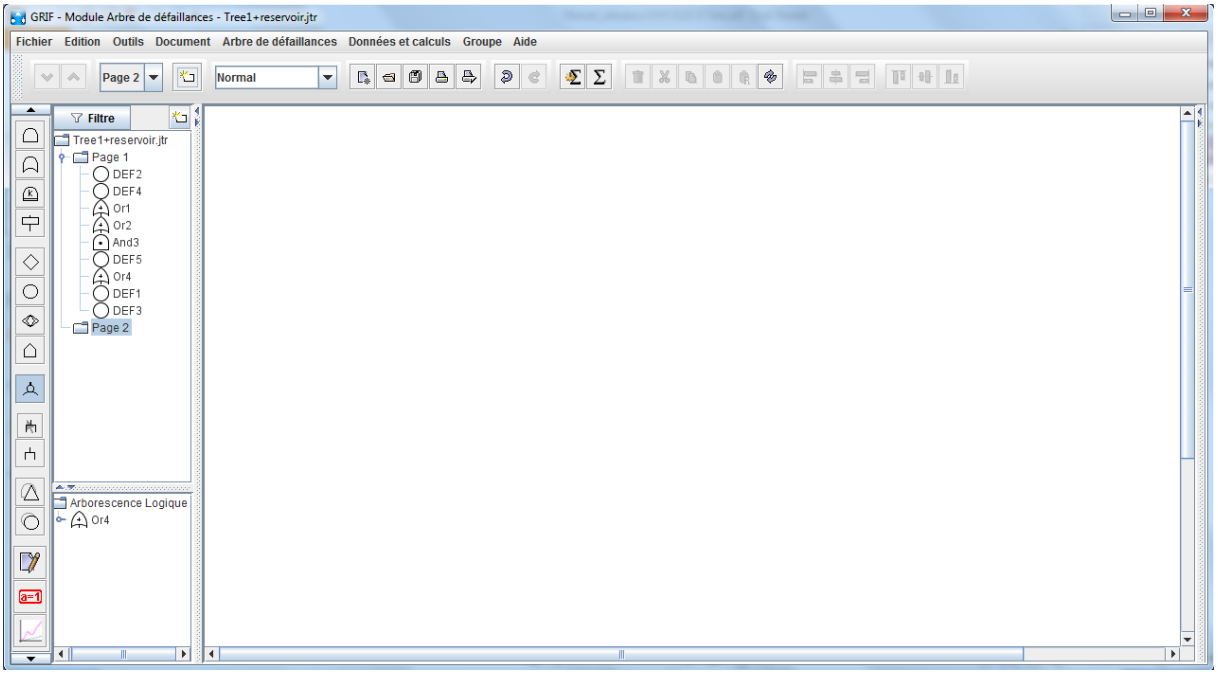



**Figure B.1** Fenêtre principale du module arbre de défaillances

### *B.1.1.1 Barre d'outils verticale*

Chaque modèle utilisé en sûreté de fonctionnement possède sa propre iconographie. L'ensemble de symboles graphiques relatifs aux arbres de défaillances est représenté sur la barre d'icônes placée verticalement à gauche de la fenêtre de saisie.

| | |
|---|---|
|  | **Outils de sélection** Permet de sélectionner les objets graphiques dans la zone de saisie. |
|  | **Groupe** Permet d'ajouter un groupe (sous-page) au modèle. |
|  | **Porte "ET"** L'événement de sortie apparaît si tous les événements d'entrées apparaissent. |
|  | **Porte "OU"** L'événement de sortie apparaît si au moins un des événements d'entrées apparaît. |
|  | **Porte "K sur N"** L'événement de sortie apparaît si au moins k événements d'entrées apparaissent (k < n). |
|  | **Porte "NOR"** L'événement de sortie apparaît si aucun des événements d'entrées n'est apparu. |
|  | **Porte "NAND"** L'événement de sortie apparaît si au moins un des événements d'entrées n'apparait pas. |
|  | **Porte "XOR"** L'événement de sortie apparaît si un seul événement d'entrée apparaît. |
|  | **Porte "Si/Alors/Sinon"** L'événement de sortie vaut la valeur de l'évènement 'alors' si l'évènement 'si' apparaît et vaut la valeur de l'évènement 'sinon' autrement. |
|  | **Porte "Négation"** L'événement de sortie apparaît si l'événement d'entrée n'apparaît pas. L'état logique de la sortie est l'inverse de celui d'entrée. |
|  | **Porte "Commentaire"** Permet d'insérer un commentaire au sein du modèle. |
|  | **Evénement de base** Événement du plus bas niveau pour lequel la probabilité d'apparition ou d'information de fiabilité est disponible. |
|  | **Evénement élémentaire** Le développement de cet événement est terminé. Il correspond à la défaillance d'un système ou d'un équipement qui pourrait être détaillé mais pour lequel on une utilise une loi équivalente. |
|  | **Evénement à développer** Le développement de cet événement n'est pas terminé par manque temporaire d'information. Cet évènement devra être développé ultérieurement. |
|  | **Evénement "Maison"** Événement qui doit se produire avec certitude lors de la production ou de la maintenance. On peut aussi le définir comme un événement non-probabilisé, que l'on doit choisir de mettre à 1 ou à 0 avant tout traitement de l'arbre. Ce type d'événement permet d'avoir plusieurs variantes d'un arbre sur un seul dessin, en modifiant la logique de l'arbre selon la valeur choisie par l'utilisateur. |
|  | **Lien (un seul)** pour créer une connexion (et uneseule) entre une entrée (porte) et une sortie (porte ou événement). |
|  | **Liens (plusieurs)** pour créer des connexions entre les entrées (portes) et les sorties (portes et événements). |
|  | **Renvoi identique** Permet de creer un raccourci vers une autre porte. |
|  | **Evénement répété** Permet de creer un raccourci vers un autre évènement. |
|  | **Outil champs dynamique** Permet de créer des commentaires dynamiques affichant les données du modèle |
|  | **Outil commentaire** Permet de créer des commentaires statiques. |

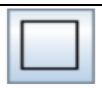
| | |
|---|---|
|  | **Outil ligne** Permet de créer des lignes ou flèches de tous styles. |
|  | **Outil rectangle** Permet de créer des zones rectangulaires de couleurs différentes. Ces zones peuvent être ancrées à la page. |
|  | **Outil polygone** Permet de créer des zones en forme de polygone fermé. Ces zones peuvent être ancrées à la page. |
|  | **Outil cercle** Permet de créer des zones circulaires de couleurs différentes. Ces zones peuvent être ancrées à la page. |
|  | **Outil ellipse** Permet de créer des zones de forme elliptique. Ces zones peuvent être ancrées à la page. |
|  | **Outil courbe** Permet de tracer des courbes en sélectionnant des résultats de calculs dans la banque de résultats. |

**Tableau B.1** Barre d'outils verticale de l'arbre de défaillance.

## B.1.2 Création d'un arbre de défaillance

### *B.1.2.1 Saisie de l'arbre*

#### *B.1.2.1.1 Saisie des portes*

Pour saisir les différentes **Portes**, il suffit de sélectionner le symbole correspondant sur la barre d'outils verticale. Ensuite à chaque clic gauche de la souris sur la surface de saisie graphique, un nouvel élément est créé. Chacune des portes du modèle est caractérisée par cinq paramètres:

- ✓ Un **numéro** : le numéro et le type sont les vrais identifiants des portes (ceux qui seront utilisés par le moteur de calcul). C'est pour cette raison que lorsque l'utilisateur souhaite changer le numéro de certaines portes il doit faire attention au fait que deux portes ne peuvent pas avoir un numéro identique. Ils sont incrémentés automatiquement au fur et à mesure de la création de nouveaux éléments.

- ✓ Un **nom** : C'est un paramètre qui est défini automatiquement et qui ne peut pas être modifié par l'utilisateur. Le nom de chaque porte est composé de son "type" suivit de son "numéro" (ex.: "And1" ou "KofN3").

✓ Un **entier "K sur N"** : Ce champ n'est accessible que dans le cas des portes de type **K sur N**. Il permet à l'utilisateur de choisir la valeur de **K** (par défaut **K** vaut 1).

✓ Un **commentaire** : Ce champ permet d'ajouter du texte à l'intérieur de la porte. Cette fonction a pour but de faciliter la lecture du modèle (en spécifiant la particularité de ces éléments).

✓ Un **type** : Une fois qu'une porte a été créée, il est possible de modifier son type parmi les cinq types disponibles au niveau de la liste déroulante.

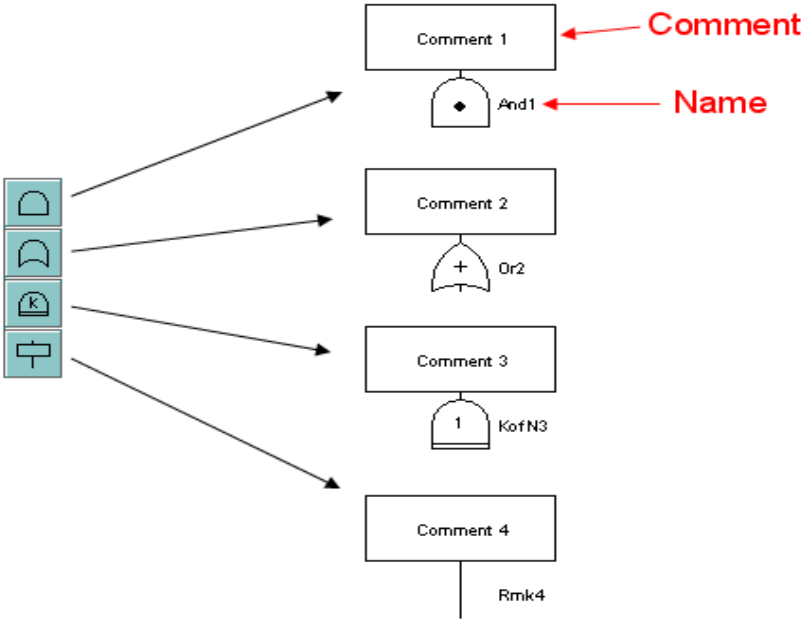



**Figure B.2** Saisie des portes

### *B.1.2.1.2 Saisie des événements*

Pour saisir les **Evénements** du modèle, il suffit de sélectionner le symbole correspondant sur la barre d'outils verticale. Ensuite à chaque clic gauche de la souris sur la surface de saisie graphique, un nouvel élément est créé. Chacun des événements du modèle est caractérisé par différents paramètres regroupés en 3 onglets:

1. **Général** avec les informations suivantes:

• Un **numéro** : le numéro et le type sont les vrais identifiants des événements (ceux qui seront utilisés par le moteur de calcul). C'est pour cette raison que lorsque l'utilisateur souhaite changer le numéro de certains événements il doit faire attention au fait que deux événements ne peuvent pas avoir un numéro identique. Ils sont incrémentés automatiquement au fur et à mesure de la création de nouveaux éléments.

• Un **nom** : Le nom par défaut qui est attribué aux événements est **Evti** pour le ième élément créé. Il est conseillé à l'utilisateur de remplacer ce nom par quelque chose de plus mnémotechnique afin de faciliter la lecture du modèle.

• Un **commentaire** : Ce champ permet d'ajouter du texte à l'intérieur de l'événement. Cette fonction a pour but de faciliter la lecture du modèle (en spécifiant la particularité de ces éléments).

• Une **loi** : C'est l'élément qui va servir à modéliser l'aspect aléatoire de l'événement. L'utilisateur a la possibilité de choisir parmi vingt trois lois qui doivent dans un deuxième temps être paramétrées (cf. ultérieurement la description détaillée des loi).

• Un **type** : Une fois qu'un événement a été créé, il est possible de modifier son type parmi les quatre types disponibles au niveau de la liste déroulante.

2. un onglet **Attributs**

3. un onglet **Avancé** pour spécifier le comportement de l'évènement.

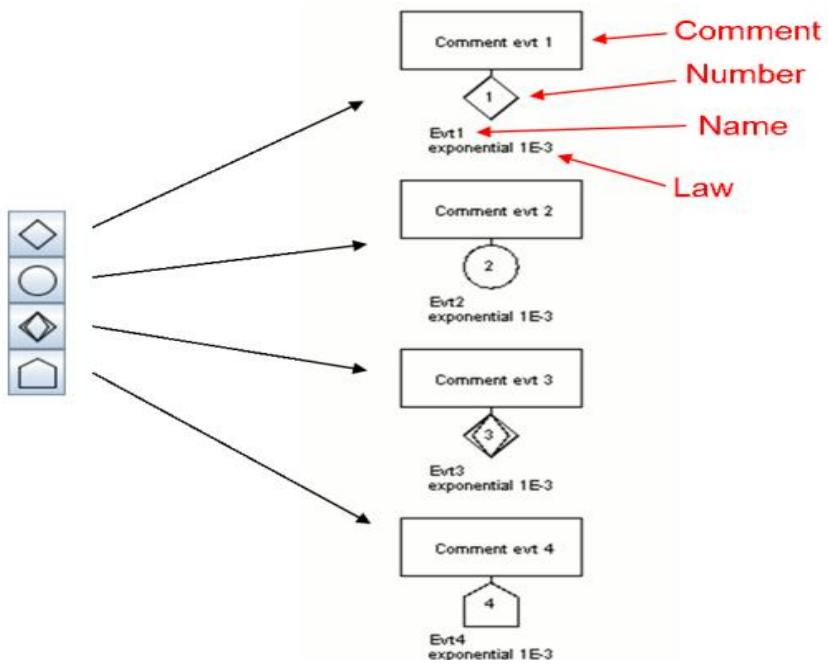



**Figure B.3** Saisie des événements

### *B.1.2.1.3 Saisie des liens*

Une fois les portes et les événements créés, il faut les connecter entre eux afin d'établir la logique de l'arbre. Il existe deux types de connexions possibles: les connexions "porte -> porte" et les connexions "porte -> événement".

Pour réaliser une connexion, il suffit de:

- Cliquer sur l'icône correspondante de la barre d'outils verticale
- . Sélectionner la porte de départ en faisant un clic gauche sur la zone spécifique (point pour les portes "ET", croix pour les portes "OU"...) et laisser le bouton enfoncé.
- Faire glisser la souris jusqu'à l'élément qui doit être connecté.
- Relâcher la souris.

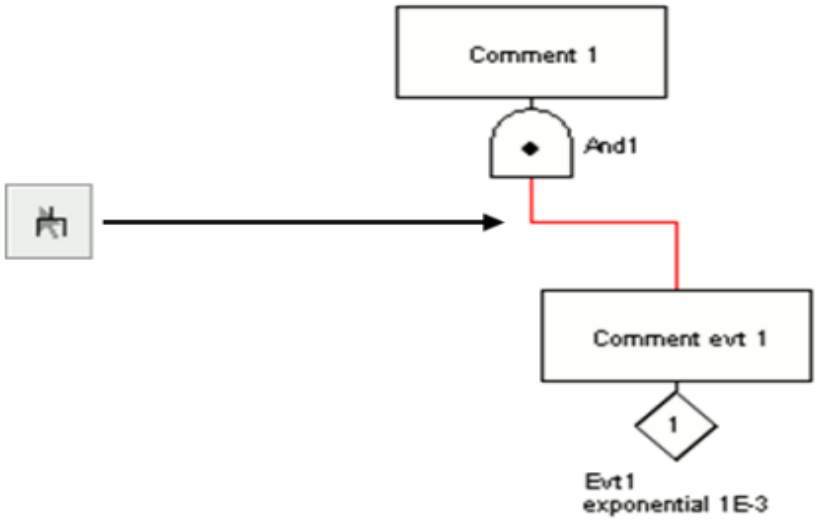



**Figure B.4** Saisie des liens.

## B.2 Arbre de défaillance de notre cas d'étude

La figure B.5 illustre l'arbre de défaillances classique relatif aux états de fonctionnement du système mécatronique étudie concerne la régulation de volume de deux réservoirs en redondance passive avec utilisation d'un seul réservoir à la fois sous GRIF (**Gr**aphiques **I**nteractif pour la **F**iabilité).

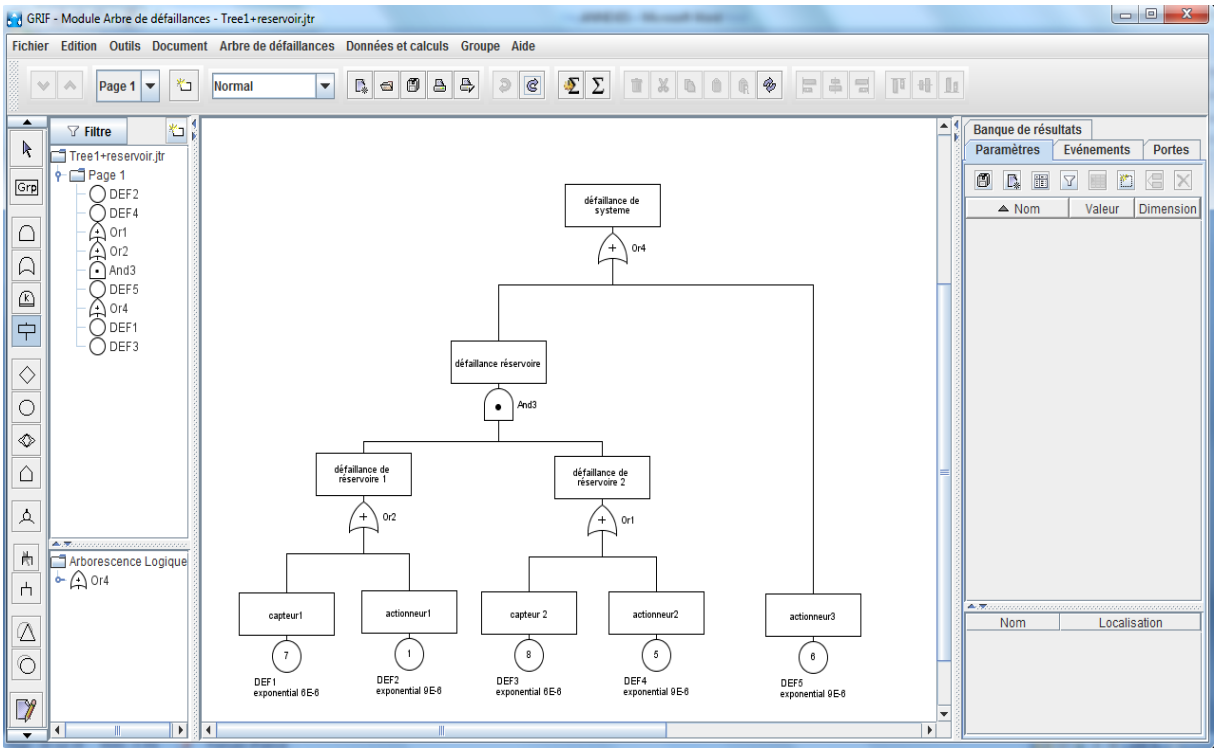



**Figure B.5** Arbre de défaillances du système à deux réservoirs (cas d'étude).

### B.2.1 Calcul de la fiabilité du système

Les calculs s'effectuent en deux étapes:

• le paramétrage des calculs;

• la lecture des résultats dans la banque de résultat.

La fenêtre de paramétrage des calculs est accessible de deux manières différentes : soit par le menu **Données et calculs - configuration et lancement du calcul**.

La fenêtre de paramétrage qui est ainsi ouverte est appelée **Lancement des calculs**.

La fenêtre de paramétrage se décompose en cinq onglets comme la figure ce dessous démontre.

- **Paramétrage des calculs de probabilités** : permet de définir les calculs à effectuer.
- **Indisponibilité** : qui selon les normes notée Q(t), U(t) ou PFD(t)
- **Disponibilité** : A(t) = 1 - U(t)
- **Intensité Inconditionnelle de Défaillance** : qui selon les normes notée W(t), UFI(t) ou PFH(t). C'est la probabilité que le système tombe en panne entre t et t+dt, sachant qu'à t=0 le système n'est pas défaillant.
- **Intensité Conditionnelle de Défaillance (Lambda eq)** : qui selon les normes notée CFI(t). C'est la probabilité que le système tombe en panne entre t et t+dt,

sachant que le système n'est pas défaillant à t et qu'à t=0 il n'était pas défaillant non plus.

- **Défiabilité** : F(t) = 1 - R(t)
- **Fiabilité** : R(t) = R(t)=$e^{-\lambda(t)}$

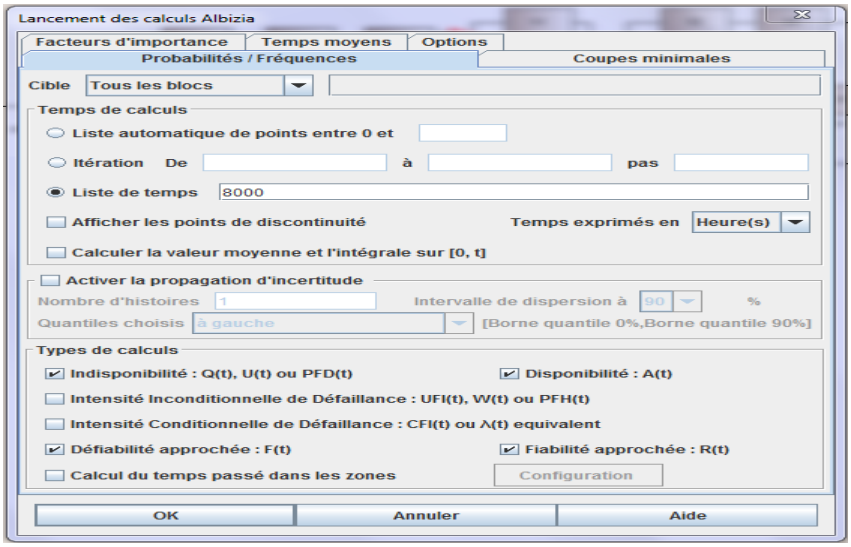



**Figure B.6** Fenêtre des calculs.

Le calcul de la fiabilité R(t) de notre système s'effectuer à l'aide du lancement d'un calcul avec des itérations de 0 à 10000 avec un pas de 100 dans la fenêtre de paramétrage des calculs de probabilités (Probabilités / Fréquences) qui été bien expliqué dans la figure B.7

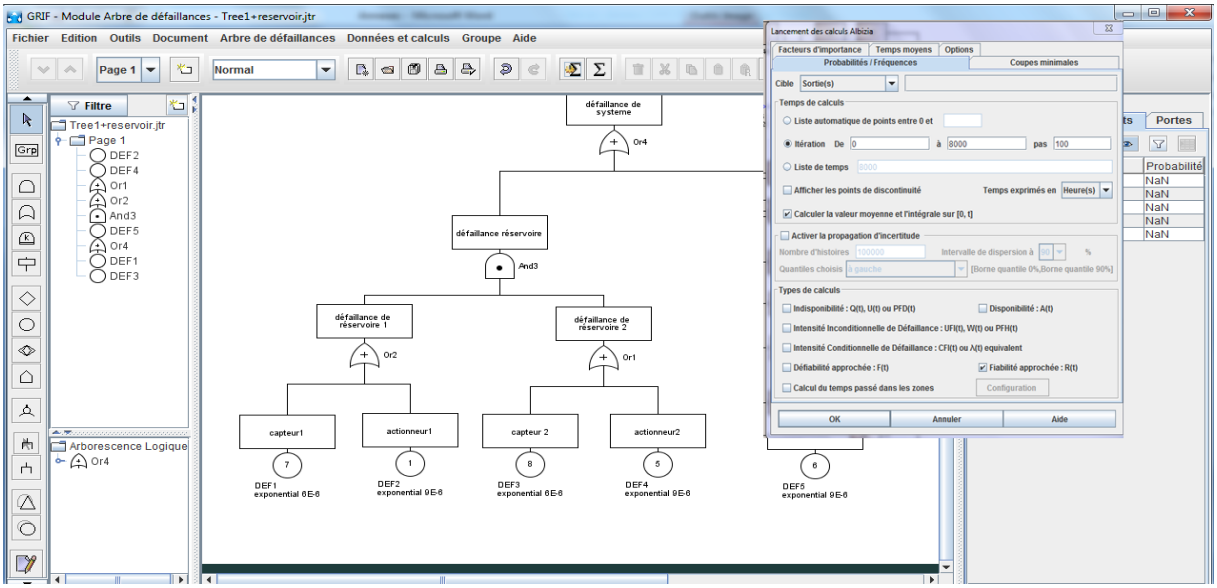



**Figure B.7** Calcul de la fiabilité du système.

### B.2.2 Résultat de la simulation pour la fiabilité

Les résultats sont présentés sous la forme d'une fenêtre composée de 5 onglets:

• Probabilités

• Facteurs d'importance

• Coupes

• Temps moyens

• Résultats

• Info

Afin de mieux étudier le modèle et les résultats, il est possible de tracer des courbes. Pour cela, il suffit de faire un clic gauche sur l'icône correspondante de la barre des tâches verticale. Puis la courbe de la fiabilité montrer dans la figure B.6 suivante donc sera affiché.

Icône **Graphique**: 

La courbe de la fiabilité décroit selon une exponentielle montrée par la figure B.8 :

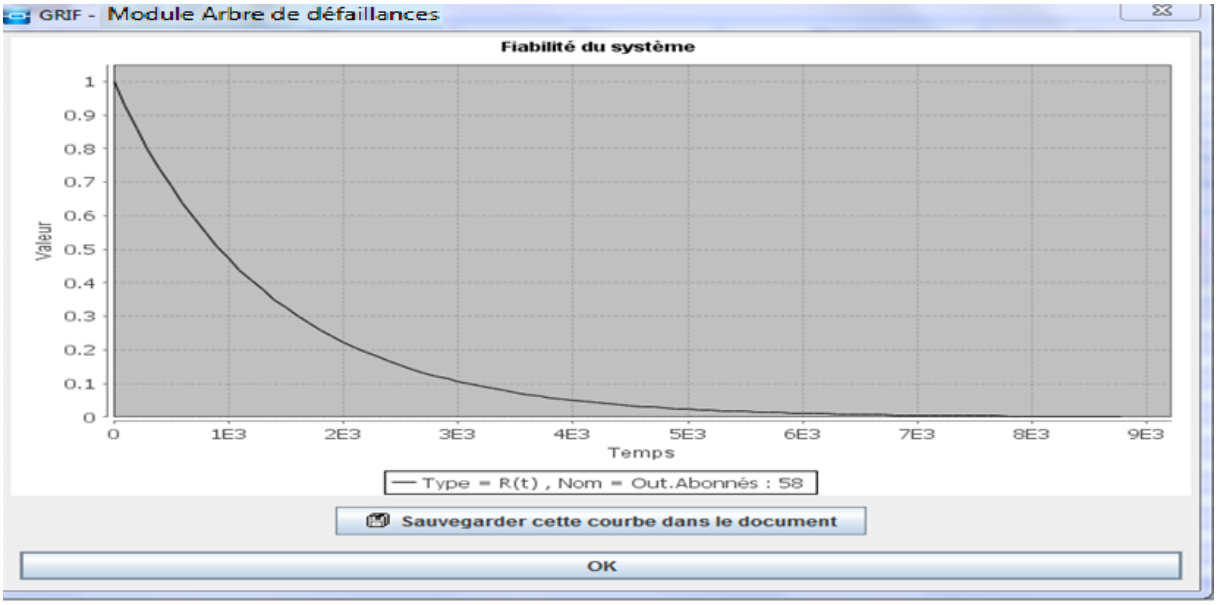



**Figure B.8** Courbe de la fiabilité du système.

### B.2.3 Le calcul de la disponibilité du système

Le principe de calcul de la disponibilité du système s'exécuter de la même façon que la fiabilité, sauf on a choisi le type de probabilité de calcul et cocher l'icône : Disponibilité A(t).

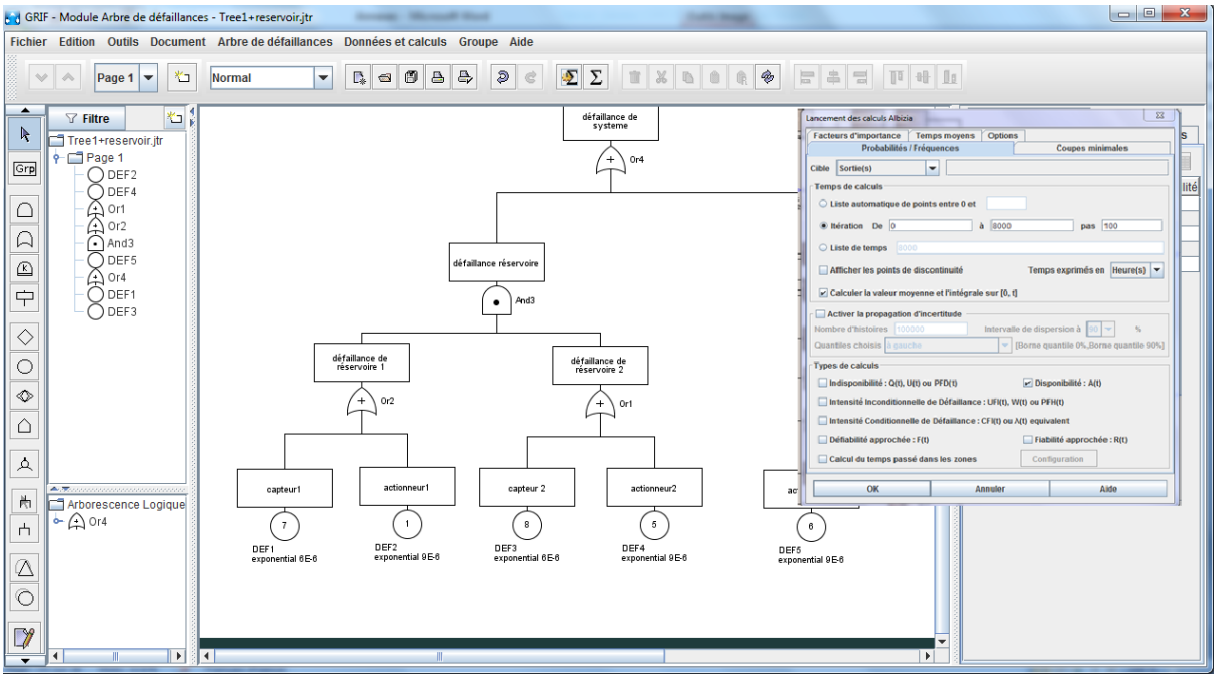



**Figure B.9** Calcul de la disponibilité du système.

### B.2.4 Résultat de la simulation pour la disponibilité

La figure B.8 représente la variation de la disponibilité du système à travers le temps. Cette disponibilité décroissante dans le temps vers une valeur fixe est appelée disponibilité asymptotique. La disponibilité asymptotique tend vers la valeur de 91,33%.

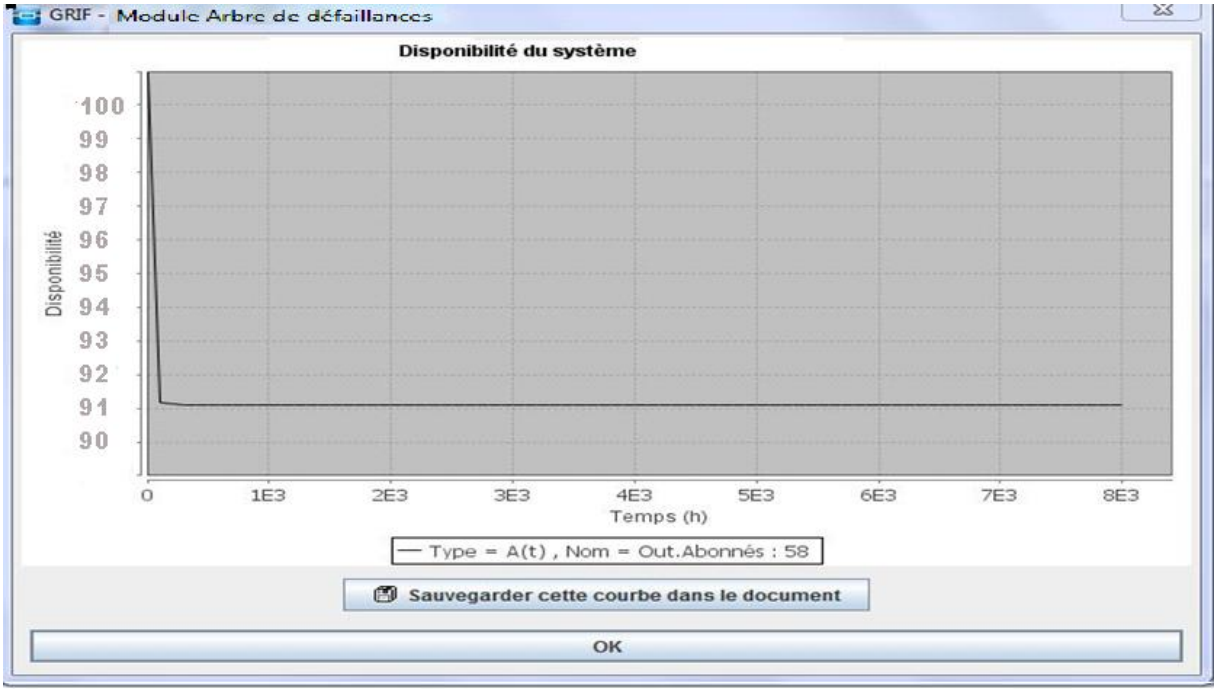



**Figure B.10** Courbe de la disponibilité du système.

# Annexe C

# Modélisation par réseau de Petri sous GRIF

## C.1. Présentation de l'interface

### C.1.1. Fenêtre principale du module Réseaux de Petri à prédicats

La fenêtre principale est décomposée en plusieurs parties :

• **Barre de titre** : La barre de titre indique le nom du module et le nom du fichier en cours d'édition.

• **Barre de menu** : La barre de menu permet d'accéder à toutes les fonctions de l'application.

• **Barre d'icônes (raccourcis)** : La barre de raccourcis est une barre (horizontale) d'icônes permettant d'accéder plus rapidement aux fonctions usuelles.

• **Barre d'outils** : La barre d'outils (verticale) permet de sélectionner les éléments à utiliser pour la modélisation.

• **Zone de saisie** : Un maximum de place a été laissé à la zone de saisie graphique pour permettre de réaliser le modèle.

• **Arborescence** : L'arborescence est entre la zone de saisie et la barre d'outils. Elle permet de naviguer dans les pages et groupes du document.

• **Modèles** : La liste des modèles se situent en dessous de l'arborescence. Ils sont groupés en deux sous dossier suivant leur lieu d'enregistrement (Répertoire utilisateur ou d'installation).

• **Ensemble des tableaux** : Les tableaux de données sont regroupés dans des onglets à droite de la zone de saisie.

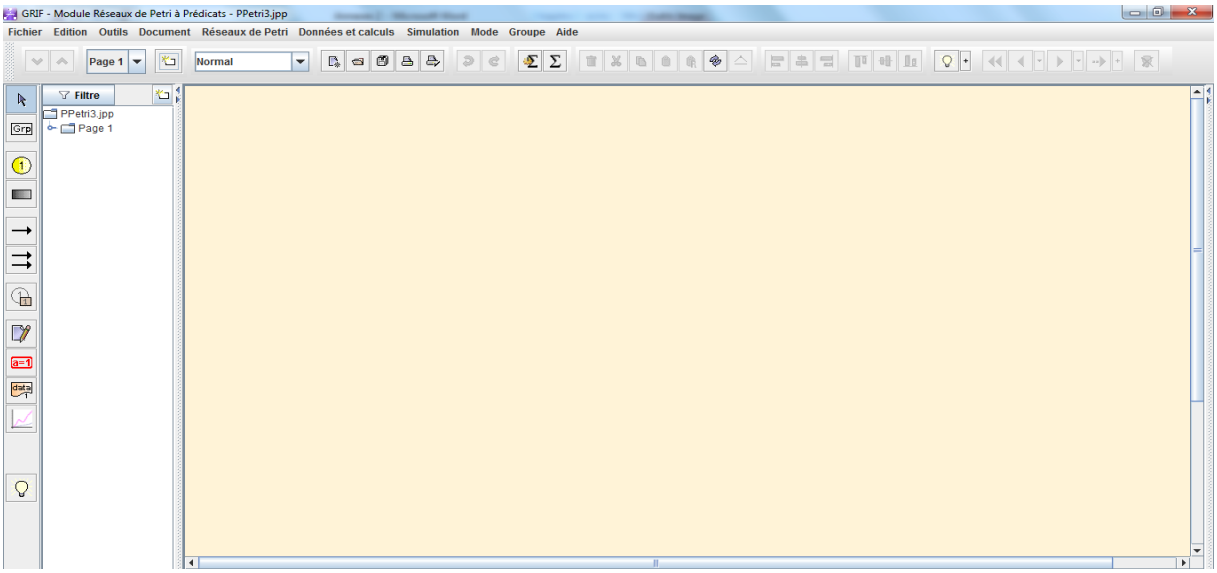



**Figure C.1** Fenêtre principale du module de réseau de Petri.

### *C.1.1.1 Barre d'outils verticale*

Chaque modèle utilisé en sûreté de fonctionnement possède sa propre iconographie. L'ensemble de symboles graphiques relatifs aux réseaux de Petri est représenté sur la barre d'icônes placée verticalement à gauche de la fenêtre de saisie. La barre d'outils verticale comporte les éléments suivants :

| | |
|---|---|
|  | **Outils de sélection** Permet de sélectionner les objets graphiques dans la zone de saisie. |
|  | **Groupe** Permet d'ajouter un groupe (sous-page) au modèle. |
|  | **Places** représentées par des cercles. |
|  | **Transitions** représentées par des rectangles. |
|  | **Arcs amont et aval** représentés par des flèches. |
|  | **Arcs amont et aval** représentés par des flèches. |
|  | **Place répétée (ou Renvoi)** pour réaliser des liaisons entre plusieurs parties du même modèle (sur des pages ou dans des groupes différents). |
|  | **Commentaire** pour ajouter du texte directement sur le graphique. |
|  | **Affichage dynamique** pour afficher une valeur d'un élément du modèle. |
|  | **Variables locales** pour créer des variables liées uniquement à une partie du modèle. |
|  | **Courbe** pour tracer des courbes représentant des calculs sur le modèle. |
|  | **Simulation** permet de passer en mode simulation. |

**Tableau C.1** Barre d'outils verticale de réseau de Petri.

### C.1.2 Création d'un réseau de Petri

#### *C.1.2.1 Saisie du réseau*

##### *C.1.2.1.1 Saisie des places*

Pour saisir les différentes **Places**, il suffit de sélectionner le symbole correspondant sur la barre des symboles. Ensuite à chaque clic de la souris sur la surface de saisie graphique, un nouvel élément est créé. Chacune des places du modèle est caractérisée par trois paramètres:

- Un **numéro** : Situés au centre des places, ils sont incrémentés automatiquement. Ces numéros sont les vrais identifiants des places qui seront utilisés par le moteur

de calcul. C'est pour cette raison que deux places ne peuvent pas avoir un numéro identique.

- Un **label** : Un label par défaut est attribué à chaque place ("Pli" pour la place numéro "i"). Comme chaque place a, en général, un sens bien précis pour l'utilisateur, il est fortement conseillé de lui attribuer un label plus mnémotechnique que celui donné par défaut. Cela permet de mieux se repérer dans le modèle et dans le fichier résultats.
- Un nombre de **jetons** : Il est égal à zéro par défaut pour chacune des places créées. Dans un réseau de Petri la présence (ou non) d'un jeton dans une place correspond, en général, à la présence (ou non) d'un état particulier pour un des composants du système modélisé par le réseau de Petri. L'ensemble des jetons présents à un instant donné ("marquage" du réseau de Petri) correspond de ce fait à l'état global du système étudié. L'évolution de ce "marquage" constitue de l'aspect dynamique du système.

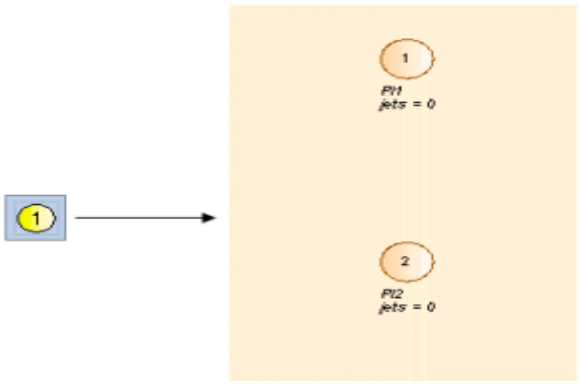



**Figure C.2** Saisie des places

### *C.1.2.1.2 Saisie des transitions*

Pour saisir les différentes **Transitions**, il suffit de sélectionner le symbole correspondant sur la barre des symboles. Ensuite à chaque clic de la souris sur la surface de saisie graphique, un nouvel élément est créé.

Dans un réseau de Petri, les **Transitions** modélisent les événements qui peuvent se produire à un moment donné sur le système étudié (défaillances, tests, maintenance...). Les "Tir" des transitions modifient le marquage des places auxquelles elles sont reliées par les arcs (amonts et avals). C'est ce qui permet de simuler le comportement dynamique du système.

A sa création, chaque transition est pourvue d'un nom par défaut ("Tri" pour la transition saisie en i ème position). Contrairement aux places, le numéro des transitions n'a aucune importance car il n'est pas utilisé dans le fichier de données généré pour les moteurs de calcul. Il est donc très fortement conseillé (plus que pour les places) de leur attribuer un label mnémotechnique.

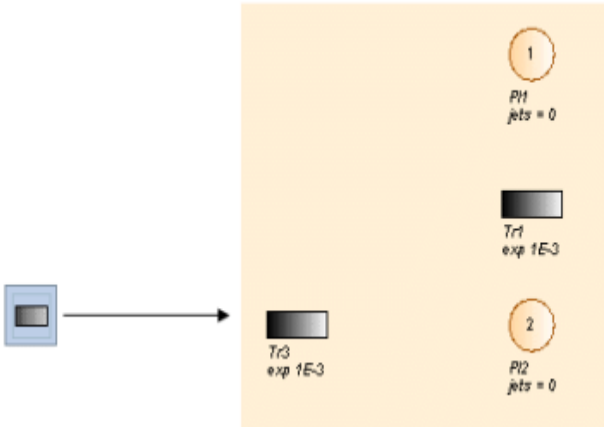



**Figure C.3** Saisie des transitions.

### *C.1.2.1.3. Saisie des arcs amonts et avals*

La fonction des "arcs amonts" est de décrire une partie des conditions de validation des transitions (l'autre partie étant gérée par les "gardes". En effet, ils définissent le marquage nécessaire des places amont pour permettre le tir de la transition.

La fonction des "arcs avals" est de décrire ce qui se passe au niveau des transferts de jetons lorsque le "tir" de la transition a lieu.

Pour saisir les arcs amont ou aval il suffit de :

1. sélectionner l'une des deux icônes correspondantes sur la barre des symboles:

•la "flèche unique" qui ne permet de saisir qu'un seul arc à la fois ou

• la "flèche double" qui permet de saisir autant d'arcs que l'on veut.

2. sélectionner une "place" (respectivement une "transition") de départ en cliquant dessus avec le bouton gauche.

3. Faire glisser la souris (sans lâcher le bouton) jusqu'à la **Transition** (respectivement la **Place**) d'arrivée où on relâche le bouton.

C'est l'ordre "place" => "transition" ou "transition" => "place" qui détermine le type ("amont" ou "aval") de l'arc saisi.

Sur la figure C.4 ci-dessous on peut voir le résultat obtenu. Des arcs amont ont été tirés entre la places 1 et la transition Tr1, puis entre la place 2 et la transition Tr2, et des arcs avals ont

été tirés entre la transition TR1 et la place 2, puis entre la transition Tr2 et la place 3, etc... On notera que contrairement aux "Réseaux de Fiabilité" il n'existe pas d'arc bidirectionnel pour les "Réseaux de Petri". Cependant il arrive souvent qu'un arc amont et un arc aval doivent être tirés entre la même place et la même transition. Dans ce cas ils peuvent être superposés et donner l'illusion d'un arc bidirectionnel mais il s'agit bien de deux arcs séparés.

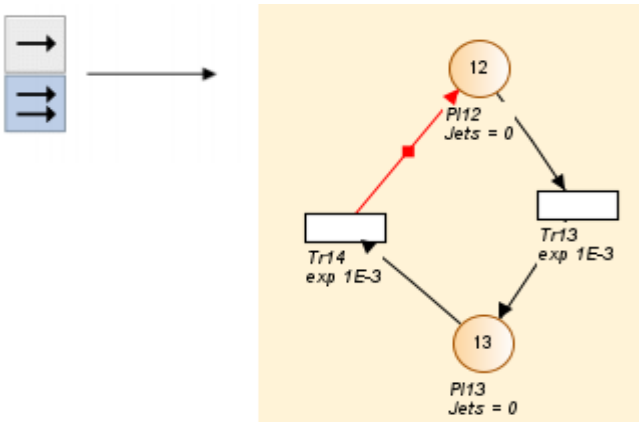



**Figure C.4** Saisie des arcs amonts et avals.

## C.2 Réseau de Petri de notre cas d'étude

On choisi Le modèle du capteur intelligent est décrit par le schéma de la figure C.5.

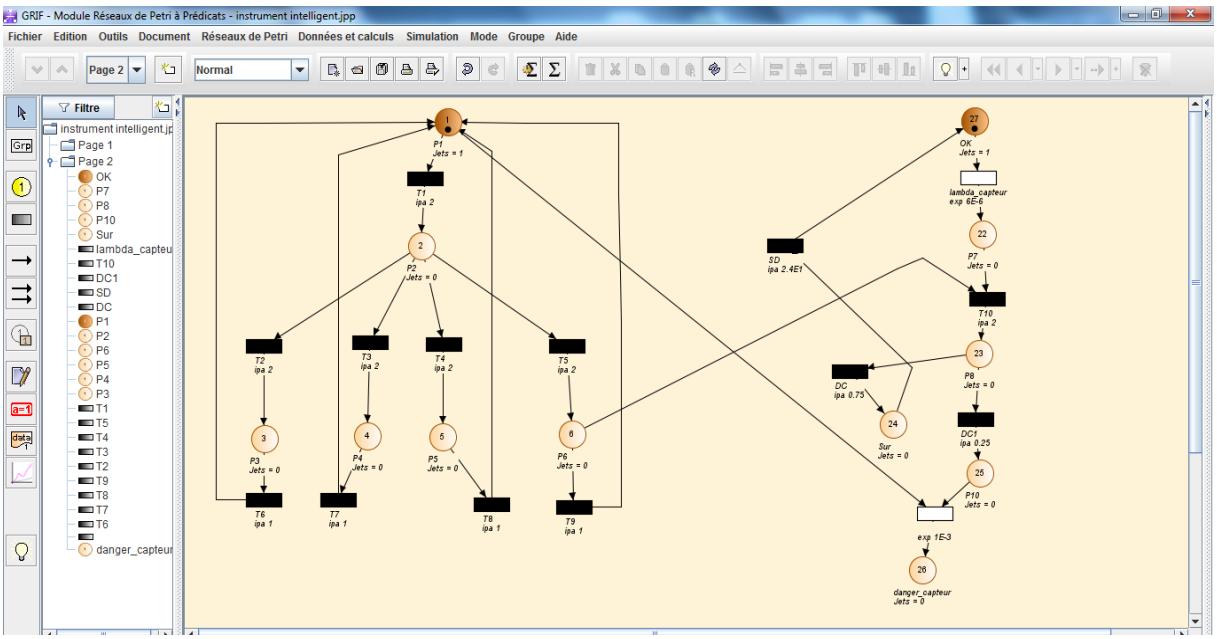



**Figure C.5** modèle de réseau Petri du capteur intelligent sur GRIF.

### C.2.1 Calcul de la fiabilité du système

Les calculs s'effectuent en deux étapes:

• le paramétrage des calculs;

• la lecture des résultats dans la banque de résultat.

La fenêtre de paramétrage des calculs est accessible de deux manières différentes : soit par le menu **Données et calculs - configuration et lancement du calcul**.

La fenêtre de paramétrage qui est ainsi ouverte est appelée **Lancement des calculs**.

La fenêtre de paramétrage se décompose en cinq onglets comme la figure ce dessous démontre.

- **Paramétrage des calculs de probabilités** : permet de définir les calculs à effectuer.
- **Indisponibilité** : qui selon les normes notée Q(t), U(t) ou PFD(t)
- **Disponibilité** : A(t) = 1 - U(t)
- **Intensité Inconditionnelle de Défaillance** : qui selon les normes notée W(t), UFI(t) ou PFH(t). C'est la probabilité que le système tombe en panne entre t et t+dt, sachant qu'à t=0 le système n'est pas défaillant.
- **Intensité Conditionnelle de Défaillance (Lambda eq)** : qui selon les normes notée CFI(t). C'est la probabilité que le système tombe en panne entre t et t+dt, sachant que le système n'est pas défaillant à t et qu'à t=0 il n'était pas défaillant non plus.
- **Défiabilité** : F(t) = 1 - R(t)

**Fiabilité** : R(t) = R(t)=$e^{-\lambda(t)}$

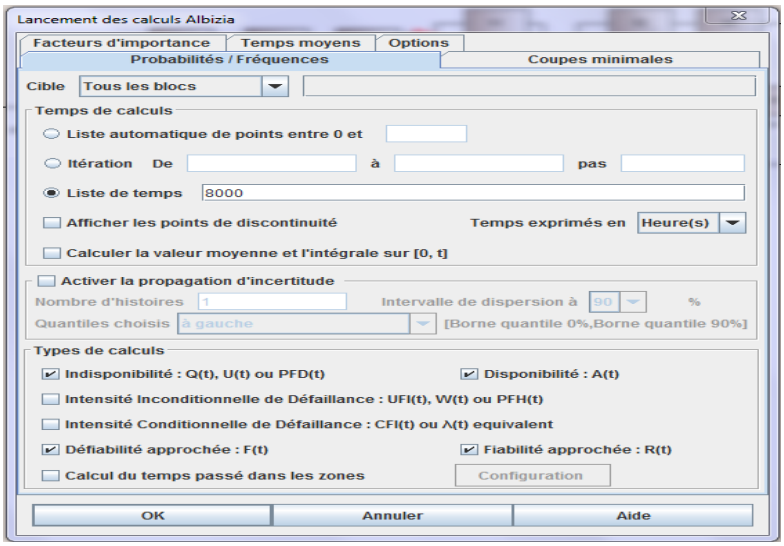



**Figure C.6** Fenêtre des calculs.

Le calcul de la fiabilité R(t) de notre système s'effectuer à l'aide du lancement d'un calcul avec des itérations de 0 à 10000 avec un pas de 100 dans la fenêtre de paramétrage des calculs de probabilités (Probabilités / Fréquences) qui été bien expliqué dans la figure C.7

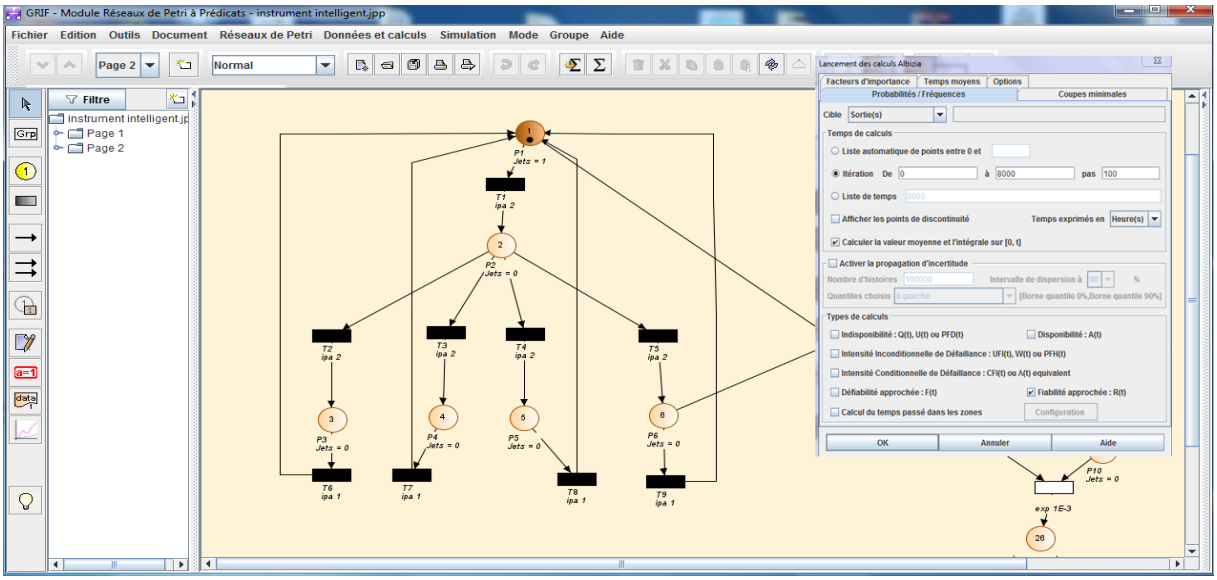



**Figure C.7** Calcul de la fiabilité du système.

### C.2.2 Résultat de la simulation pour la fiabilité

Les résultats sont présentés sous la forme d'une fenêtre composée de 5 onglets:

- Probabilités
- Facteurs d'importance
- Coupes
- Temps moyens
- Résultats
- Info

Afin de mieux étudier le modèle et les résultats, il est possible de tracer des courbes. Pour cela, il suffit de faire un clic gauche sur l'icône correspondante de la barre des tâches verticale. Puis la courbe de la fiabilité montrer dans la figure B.6 suivante donc sera affiché.

Icône **Graphique**: 

La courbe de la fiabilité décroit selon une exponentielle montrée par la figure C.8 :

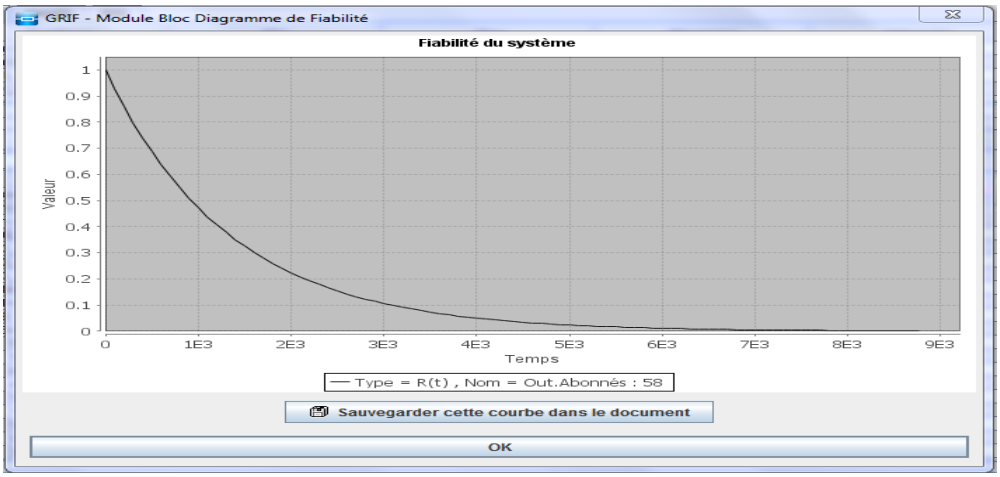



**Figure C.8** Courbe de la fiabilité du système.

### C.2.3 Le calcul de la disponibilité du système

Le principe de calcul de la disponibilité du système s'exécuter de la même façon que la fiabilité, sauf on a choisi le type de probabilité de calcul et cocher l'icône : Disponibilité A(t).

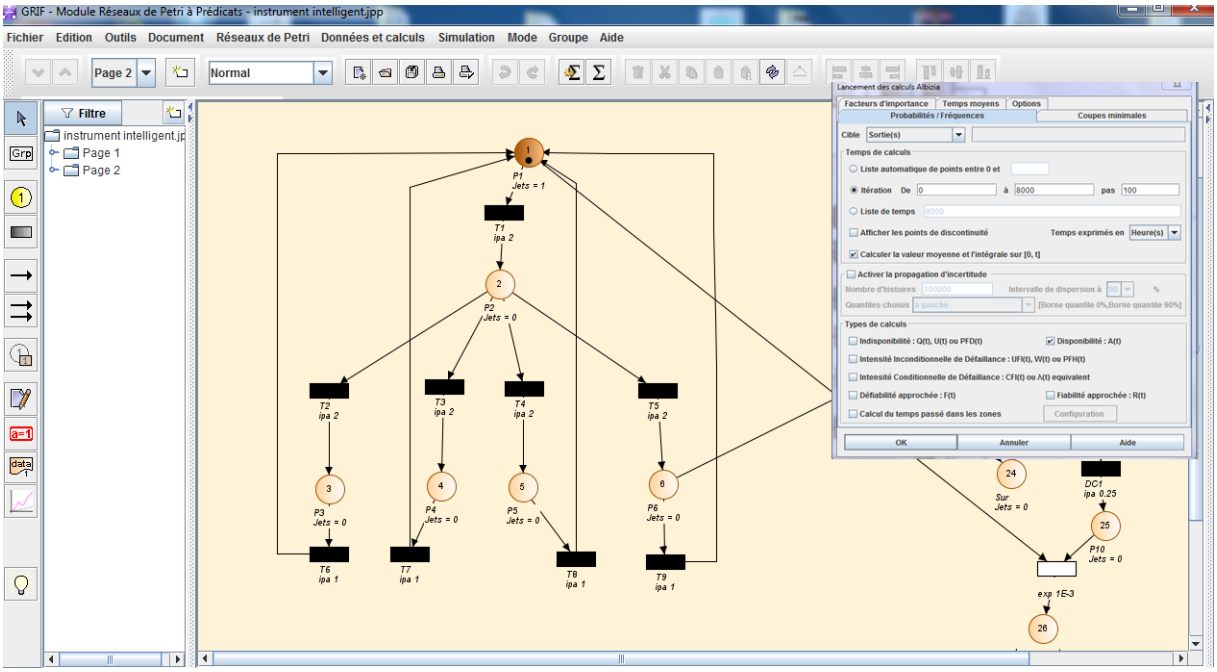



**Figure C.9** Calcul de la disponibilité du système.

### C.2.4 Résultat de la simulation pour la disponibilité

La figure B.10 représente la variation de la disponibilité du système à travers le temps. Cette disponibilité décroissante dans le temps vers une valeur fixe est appelée disponibilité asymptotique. Pour la modélisation par bloc diagramme de fiabilité sans redondance, la disponibilité asymptotique tend vers la valeur de 91,33%.

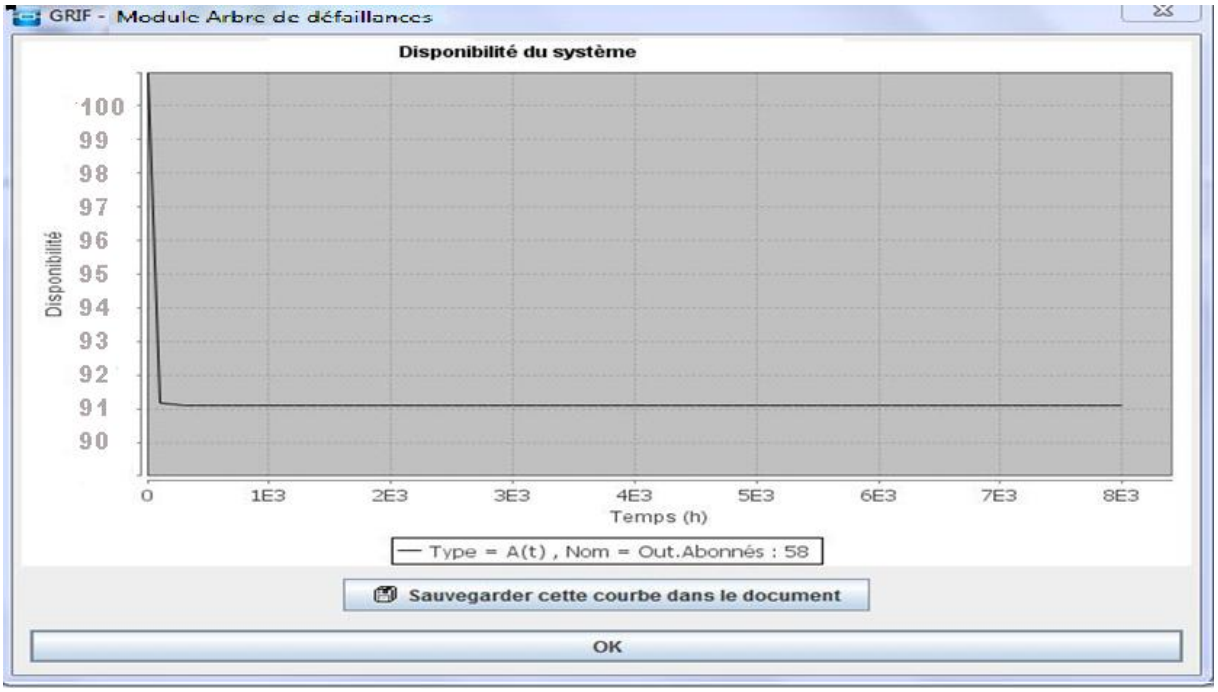



**Figure C.10** Courbe de la disponibilité du système.