Contribution à l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité intégrant de l'intelligence

Abdelhak Mkhida

Nancy-Université INPL

Institut National
Polytechnique de Lorraine

École doctorale IAEM Lorraine
Département de Formation Doctorale en Automatique

Contribution à l'évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité intégrant de l'Intelligence

THÈSE

Présentée et soutenue publiquement le 14 Novembre 2008

pour l'obtention du

Doctorat de l'institut National Polytechnique de Lorraine
Spécialité Automatique, Traitement du signal et Génie Informatique
par

ABDELHAK MKHIDA
Ingénieur ENIB

Composition du jury

Président :	M. ROBERT	Professeur à l'Université Henri Poincaré
Rapporteurs :	M. BAYART	Professeur à l'Université de Sciences et Techniques de Lille
	Y. VOISIN	Professeur à l'Université de Bourgogne
Examinateurs :	J-F. AUBRY	Professeur à l'INPL (Directeur de thèse)
	F. KRATZ	Professeur à l'ENSI de Bourges
	J-M. THIRIET	Professeur à l'Université Joseph Fourier de Grenoble (Co-directeur de thèse)

CRAN

Centre de Recherche en Automatique de Nancy
UMR 7039 – Nancy Université – CNRS
2, Avenue de la Forêt de Haye 54516 Vandoeuvre-Lès-Nancy
Tél. +33 (0) 83 59 59 59 Fax +33 (0) 3 83 59 56 44

Remerciements

Le travail présenté dans ce mémoire a été effectué au sein de l'équipe SACSS(Systèmes Automatisés Contraints par la Sûreté de fonctionnement et la Sécurité) du groupe thématique SURFDIAG (Sûreté de Fonctionnement et Diagnostic des systèmes) du Centre de Recherche en Automatique de Nancy (CRAN).

J'exprime mes profonds remerciements à mes deux directeurs de thèse, Jean-François Aubry et Jean-Marc Thiriet pour leur aide inestimable, leur patience et leurs encouragements tout au long de ce travail. Leurs compétences ont été un atout indéniable à la réussite de ces travaux et m'ont permis d'apprendre énormément durant ces années de collaboration.

Je suis très reconnaissant envers Madame Mireille Bayart, Professeur à l'Université des Sciences et Technologies de Lille, d'avoir accepté avec Monsieur Yvon Voisin, Professeur à l'université de Bourgogne, d'étudier mes travaux et d'en être les rapporteurs ainsi que pour l'intérêt et l'attention qu'ils ont accordés à cette étude.

J'exprime toute ma gratitude à Monsieur Michel Robert Professeur à l'université Henri Poincaré de Nancy et Monsieur Frederic Kratz Professeur à l'Ecole Nationale Supérieure d'Ingénieurs de Bourges d'avoir accepté d'examiner ce travail.

Je souhaiterais remercier également Monsieur Mohamed Bouidida, ainsi que Monsieur Youssef Benghabrit respectivement directeur et directeur adjoint de l'ENSAM de Meknès pour m'avoir permis de réaliser cette thèse dans de bonnes conditions.

Dans ces moments importants, je pense très fort à ma famille en commençant par mes excellents parents, ma formidable femme, mes deux joyaux Hajar et Aroua et au reste de ma famille : Mohamed, Naima, Rachid, Abdelali et Yassine ainsi que ma belle famille : Layachi, Omhani, Leila, Farah, Fatima Azzahra et Asmae. Je remercie aussi mes tantes et mes oncles. Je remercie tous mes proches et mes amis au Maroc, aux Pays bas, en France et partout ailleurs pour leur soutien, leur encouragements.

Je ne peux ne pas mentionner les gens qui m'ont soutenu, conseillé et aidé pendant toutes ses années : Mohammed Sallak, Hicham, Mohammed Habib, Rony, Gabriel, Olaf, Christophe et tout le reste du groupe SACSS.

Je remercie également tous ceux qui ont contribué de près ou de loin au parachèvement de ce travail de thèse, soit par leur savoir scientifique ou par leur amitié.

À mes parents, ma femme et mes deux filles pour leur soutien et leur amour
À ceux qui m'aiment et qui attendent avec impatience ma réussite
En espérant être à la hauteur de leurs attentes

Si tu ne peux pas faire front et foncer vers ton but sans te soucier des préjudices et des souffrances, pleure ton insignifiance et contente-toi d'une bébête de vie, terne et sans histoires.

A.Yassine

Acronymes

ALARP, (*As Low As Reasonably Practicable*), aussi bas que raisonnablement possible
AMDEC, Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
ANSI, (*American National Standards Institute*)
APD, Analyse préliminaire de dangers
API, Automates Programmables Industriels
APR, Analyse Préliminaire de Risques
ASIC, (*Application Specific Integrated Circuit*), circuits intégrés spécifiques à une application
BPCS, (*Base Process Control System*) système de commande de processus de base
CAN, (*Controller area Network*)
CD, couverture de diagnostic
CEI, Commission Electrotechnique Internationale
E/E/PE, systèmes électriques, électroniques et programmables E/E/EP
EUC, (*Equipment Under Control*),
FPL, (*FPL*, *Fixed program language*), langage de programme figé
GAME, (Globalement Au Moins Equivalent)
ISA, (*Instrumentation, Systems and Automation Society*)
ISO, (*International Standardardisation Organization*), Organisme international de normalisation
LVL, (*Limited Variability Language*), langage de variabilité limitée
MDT, (*Mean Down Time*), durée moyenne d'indisponibilité,
MTBF (*Mean Time Between Failures*), ou durée moyenne entre deux défaillances successives
MTTF (*Mean Time To Failure*), durée moyenne de bon fonctionnement avant la première défaillance
MTTR (*Mean Time To Repair*), Durée moyenne de réparation
NCS, (*Networked Control System*), Systèmes commandés par réseau,
NTR (*Nuisance Trip Rate*), taux d'arrêts intempestifs
PES, (*Programmable Electronic System*), système électronique programmable
PFD (*Probability of Failure on Demand*), probabilité de défaillance à la demande
PFD_{avg} (*Average Probability of Failure on Demand*), moyenne de la probabilité de défaillance à la demande
PFH, (*Probability of a dangerous Failure per Hour*), probabilité de défaillance dangereuse par heure
PFS, (*Probability of Failure to Safe*), probabilité de défaillances en sécurité,
PVST, (*Partial Valve Stroke Testing*): Test Partiel de la Course de Vanne
RdP, Réseaux de Petri
RRF, (*Risk Reduction Factor*), facteur de réduction de risque,

SADT, (Structured Analysis and Design Technique) ou Analyse Structurée et Technique de Conception
SAID, Systèmes d'Automatisation à Intelligence Distribuée
SAN (*Stochastic Activity Network*), Réseaux d'activités stochastiques
SIF, (*Safety Instrumented Function*), fonction instrumentée de sécurité
SIL, (*Safety Integrity Level*), niveaux d'intégrité de sécurité
SIS, Systèmes Instrumentés de Sécurité
SISID, (*Systèmes Instrumentés de Sécurité à Intelligence Distribuée*)
SFF, (*Safe Failure Fraction*), taux des défaillances en sécurité
SRS, (*Safety related systems*) systèmes relatifs à la sécurité
TEDS, (*Transducer Electronic Data Sheet*), fiche technique embarquée dans la mémoire du capteur spécifiée par la norme IEEE 1451
USOM, (*USer Operating Mode*)

Table des matières

Introduction

1. Problématique

Les établissements industriels ne se préoccupent plus uniquement des performances des systèmes en terme de qualité, de productivité et de rentabilité mais aussi en terme de sécurité. Des systèmes spécifiques appelés systèmes instrumentés de sécurités sont utilisés avec pour objectif de réduire les risques d'occurrence d'événements dangereux dans ces établissements en garantissant la protection des équipements, des personnes, de l'environnement et des biens. Ces risques traduisent à la fois la gravité du dommage et la fréquence d'occurrence de l'événement dangereux. Les échelles de gravité comportent plusieurs niveaux qui sont évalués en fonction des conséquences de l'événement dangereux sur les personnes, l'environnement et les biens.

L'installation en sécurité peut comporter plusieurs moyens pour atteindre une situation où tous les risques sont réduits à un risque tolérable. Des critères clairs et non ambigus doivent être définis en regard des niveaux de risque tolérable. Des mesures pour la mise en sécurité du procédé doivent être dédiées à chaque spécificité de protection. La conception du procédé, le choix des dispositifs et équipements de l'installation font partie de ces moyens. L'action sur les systèmes de commande de base des processus (BPCS), qui sont employés pour optimiser les conditions de conduite de procédé afin de maximiser la qualité et la production, peut aussi contribuer à réduire les risques. Ces actions restent parfois insuffisantes et il faut introduire d'autres systèmes de sécurité pour réduire encore le risque à un niveau acceptable. Les systèmes instrumentés de sécurités sont introduits pour pallier à ce besoin et répondre aux situations dangereuses lorsque le procédé se trouve dans des situations dangereuses.

Les systèmes instrumentés de sécurité sont utilisés pour exécuter des fonctions de sécurité, ils sont aussi appelés boucles de sécurité et ils comprennent tous les matériels, logiciels et équipements nécessaires pour obtenir la fonction de sécurité désirée. Ces systèmes peuvent atteindre un niveau d'intégrité de sécurité important en conformité avec les normes en vigueur (européenne, internationale…) telle que la norme CEI 61508 [CEI 00], la norme CEI 61511 [CEI 03] ou encore la norme ANSI/ISA S84.01-1996 [ISA 96] qui traitent de la sécurité fonctionnelle des systèmes relatifs à la sécurité. Ces systèmes (SIS) ont pour objectif de mettre le procédé en position de repli de sécurité lorsqu'il évolue vers une voie comportant un risque réel (explosion, feu, etc.), c'est-à-dire un état stable ne présentant pas de risque pour les personnes, l'environnement ou les biens.

La norme CEI 61508 est une norme multisectorielle traitant de l'ensemble de la problématique des systèmes électriques, électroniques et programmables E/E/EP tandis que la norme CEI 61511 est une déclinaison orientée vers les industries des procédés. Ces deux normes définissent les niveaux d'intégrité de sécurité (SIL, Safety Integrity Levels) et fixent le niveau

de réduction du risque que doit atteindre le SIS. Il existe 4 niveaux possibles, notés SIL1 à SIL4. Chacun d'eux dépend de la gravité et de la fréquence d'occurrence du risque. Il est évident que si un risque est très important, il nécessite des répliques très efficaces. Ces deux normes définissent un critère important pour caractériser les SIS : le PFD avg (Average Probability of Failure on Demand). La valeur du PFD avg représente la probabilité moyenne de défaillance du SIS lors de sa sollicitation ou encore l'indisponibilisé moyenne de la fonction de sécurité.

D'un autre côté, l'évolution importante des équipements d'automatisation favorisée par le formidable développement de l'informatique et de la microélectronique a contribué fortement à l'amélioration des instruments dans ces systèmes d'automatisation en les dotant d'une certaine intelligence. Ces instruments devenus intelligents intègrent de nouvelles fonctionnalités [BAY 93] et assurent conjointement avec les réseaux de communication la distribution des traitements et leur délocalisation au plus près du processus physique.

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 [NOB 04].

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 [CAM 01] 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 [GAR 02] 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. D'autre part, de par leur complexité, ces systèmes peuvent également être sources de défaillance.

Quant à l'évaluation de la sûreté de fonctionnement de ce type de systèmes, elle n'est pas triviale [JUM 03]. 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 à son environnement [KUM 96].

2. Objectifs

Le travail présenté dans cette thèse a pour objectif d'évaluer les performances en terme de sûreté de fonctionnement des systèmes instrumentés de sécurité 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 sur demande PFD et la probabilité de défaillances sûres PFS. Ces deux attributs sont importants pour la sécurité et leurs valeurs représentent respectivement une mesure du niveau de sécurité atteint (SIL) et la perte financière (arrêts fréquents de la production) causée par le système de sécurité en raison de déclenchements intempestifs. La valeur PFD est une exigence à satisfaire le niveau d'intégrité de sécurité de la norme CEI 61508. Pour la valeur PFS il n'existe pas actuellement

de prescriptions dans le monde de la sécurité internationale, bien que les utilisateurs de système de sécurité exigent un niveau aussi bas que possible de la valeur de la PFS. Dans nos travaux, nous parlerons indifféremment du SIL d'un SIS ou du SIL d'une fonction instrumentée de sécurité (SIF, Safety Instrumented Function). Nous prenons comme hypothèse que chaque SIS ne peut réaliser qu'une seule SIF.

La méthodologie que nous utilisons 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. La modélisation est traitée sous la forme d'une approche stochastique utilisant les SAN (*Stochastic Activity Network*). Les SAN sont un formalisme de modélisation puissant et sont une extension des réseaux de Petri stochastiques [MOV 84] [AZG 05]. Les SAN conservent toute la puissance de modélisation des réseaux de Petri stochastiques par l'emploi d'activités stochastiques. Un autre avantage des SAN est manifesté par le pouvoir d'accéder aux différents marquages de toutes les places à chaque instant moyennant des portes d'entrée et de sortie.

Ce formalisme de modélisation est couplé à la technique de simulation (simulation de Monte Carlo) pour l'évaluation des performances. L'association des réseaux d'activités stochastiques à une méthode de simulation de Monte-Carlo constitue une approche alternative puissante pour évaluer la performance globale en sûreté de fonctionnement des systèmes présentant des aspects temporels et dynamiques [GHO 08]. Les SAN qui sont une extension des RdP ont le grand avantage de pouvoir modéliser et traiter non seulement des processus non-Markoviens, mais encore des processus concourants et interdépendants. Les SAN associés à cette simulation allient un grand pouvoir de modélisation et une souplesse d'utilisation pour les techniques de simulation de Monte-Carlo relativement insensibles aux dimensions du problème à traiter. Les SAN-MC satisfont au double critère précédent et ont donc été retenus dans le cadre de ce travail.

La modélisation de tous les dispositifs est conçue d'une manière hiérarchique, en partant des modèles de base du système. La composition est formée par la jonction des modèles de base qui constituent des structures génériques sous forme de bibliothèque de composants.

L'évaluation des performances en sécurité est assurée par la détermination des deux métriques PFD et PFS qui se rapportent aux deux modes de défaillances cités par la norme mais aussi du niveau d'intégrité de sécurité (SIL).

3. Organisation du rapport de thèse

Le premier chapitre présente le concept les 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 et de l'aspect sûreté de fonctionnement qui est très lié a leur développement. Nous discutons également de la validation [ROB 93] [CLA 00] [CLA95] dans les instruments intelligents qui assure par les données transmises via le réseau de communication une bonne qualité du SAID et participe à l'augmentation des performances de sa sûreté de fonctionnement. Nous

proposons aussi notre vision de l'intelligence dans les instruments par la proposition de gradation de cette notion à travers quatre niveaux allant de 0 à 3.

Le second chapitre est dédié aux systèmes instrumentés de sécurité (SIS). Un tour d'horizon est effectué décrivant les normes de sécurité relatives aux SIS. La norme CEI 61508 est la norme générique et dispose d'autres déclinaisons selon le secteur industriel. Cette norme formalise une démarche pour l'estimation du risque que présente le procédé et permet d'évaluer la diminution du risque que doit apporter le système instrumenté de sécurité. Cette norme est basée sur l'analyse du risque et son évaluation permettant d'obtenir une intégrité de sécurité qui se matérialise par des niveaux d'intégrité de sécurité (*Safety Integrity Level* : SIL). La dernière partie de ce chapitre traite des critiques formulées envers la norme CEI 61508, sa situation par rapport aux systèmes d'automatisation à intelligence distribuée (SAID) et des performances évaluables en terme de sécurité.

Dans le chapitre 3, 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 auxquels il y a eu incorporation d'instruments intelligents pour devenir des Systèmes Instrumentés de Sécurité à Intelligence Distribuée (SISID).

Dans le dernier chapitre, la modélisation et l'évaluation des performances relatives à la sûreté de fonctionnement sont traitées avec des structures qui disposent d'intelligence dans les instruments composant les SIS. Dans un premier temps, nous proposons à titre de référence l'étude d'un système sans intelligence. Puis, la méthodologie pour l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité à intelligence distribuée est mise en œuvre à travers la modélisation d'un système SIS sans redondance auquel nous introduisons des instruments intelligents et un réseau de communication. Une autre application concerne un exemple de procédé constitué d'un réservoir sous pression contenant un liquide inflammable volatil avec l'instrumentation associée [GOB 01]. Les systèmes de sécurité concernés sont ceux qui obéissent aux directives décrites au chapitre 2 concernant les systèmes instrumentés de sécurité. Ce sont donc des systèmes qui réagissent à des demandes d'activation de la fonction de sécurité suite à des situations dangereuses induites par le procédé de fabrication. Les taux de défaillance pour chaque composant sont supposés connu à priori, les évaluations vont concerner les interactions entre les différents composants du système. L'estimation du taux de défaillance global du système est assurée par la détermination des performances en sécurité et en se basant entre autres sur les taux de défaillances individuels des différents composants. Les métriques utilisées pour l'évaluation de la sûreté de fonctionnement des SISID se rapportent aux deux modes de défaillances cités par la norme : le mode de défaillance dangereux et le mode de défaillance en sécurité. Nous avons également introduit des indicateurs de performance reflétant l'impact de l'incorporation d'un niveau d'intelligence donné sur les performances globales en sécurité.

Chapitre 1 : Instrumentation Intelligente

Instrumentation intelligente

1. Introduction

Les dernières décennies ont vu le formidable développement de l'informatique et de l'informatique industrielle grâce aux progrès de la microélectronique. La réduction des coûts, l'augmentation des performances, de la rapidité, de l'intégration et des capacités de stockage ont conduit à une véritable révolution technologique.

Le milieu industriel a profité également de ce changement et l'échange de données informatisées est devenu une problématique classique dans les entreprises modernes. Il était donc incontournable que les techniques numériques migrent vers les composants les plus proches du processus, à savoir les capteurs et actionneurs qui intègrent aujourd'hui des micro-contrôleurs et des interfaces de communication.

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 réparti 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'interconnexion des instruments intelligents en réseau conduit aussi à des problèmes d'informatique répartie comme la synchronisation [TAI 00], le partage des ressources, la communication et des problèmes plus spécifiques à l'automaticien comme le respect des contraintes temporelles [ROB 93], la définition de scénarios de commande, la supervision, la fusion de données, le fonctionnement en mode dégradé, la planification des actions… [JOS 96].

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 [REV 05] [ROB 93]. 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 constituée uniquement d'instruments connectés entre eux.

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 resteraient séparés.

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 [ALB 91].

De nombreuses définitions sont donc proposées dans la littérature en mettant plutôt l'accent sur tels ou tels attributs. [LAU 04] propose que 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. [ALB 91] dresse des niveaux de l'intelligence en déclinant qu'au minimum, l'intelligence exige la capacité à explorer l'environnement, à prendre des décisions, et de contrôler l'action. Des niveaux plus élevés de l'intelligence peuvent inclure la capacité de reconnaître les objets et les événements, de représenter la connaissance dans un modèle, et de raisonner pour planifier l'avenir. Dans des formes avancées, l'intelligence fournit la capacité de percevoir et de comprendre, de choisir de façon judicieuse, et d'agir avec succès sous une grande variété de circonstances afin de survivre, de prospérer dans un environnement complexe et souvent hostile.

[STE 03] a introduit trois niveaux de l'intelligence, l'intelligence analytique, l'intelligence créative et l'intelligence pratique. L'intelligence analytique est l'aptitude à analyser et à évaluer des idées, à résoudre des problèmes et à prendre des décisions. Elle serait mesurée par les tests classiques. L'intelligence créative consiste à aller au-delà de ce qui est donné et à générer des idées nouvelles. Quant à l'intelligence pratique, c'est l'aptitude à trouver la meilleure adaptation possible entre soi et les demandes de l'environnement.

Un modèle qui est reconnu actuellement est celui de [CAR 93]. Dans ce modèle, on trouve un troisième niveau qui est représenté par l'intelligence générale. Au deuxième niveau on trouve huit facteurs de groupe (intelligence fluide, intelligence cristallisée, mémoire générale, perception visuelle, perception auditive, capacité de rappel, rapidité cognitive, vitesse de traitement). Le premier niveau est représenté par des facteurs de groupe mineurs correspondant à des aptitudes de faible étendue.

En effet, [CAR 93] a repris la notion d'intelligence générale transversale à toutes les opérations mentales impliquées sans opposition aux défenseurs d'une conception postulant une pluralité d'intelligences [MEY 06]. Les différentes formes d'intelligence ont été inspirées entre autres par R.B. Cattell (1941) qui avait mis en évidence deux facteurs particulièrement importants, il s'agit de l'intelligence fluide et de l'intelligence cristallisée. L'intelligence fluide est la compétence qui nous permet de résoudre des problèmes pour lesquels nous ne possédons pas de solutions apprises. En revanche, l'intelligence cristallisée est une compétence dérivée de l'exercice de l'intelligence fluide au cours de l'apprentissage.

Il existe donc plusieurs formes d'intelligence, classées sous forme de niveaux. Ces niveaux s'étalent du concept général de l'intelligence à des facteurs beaucoup plus spécifiques.

A partir des travaux en psychologie de l'intelligence précités auparavant, nous pouvons établir une classification des niveaux d'intelligence.

Un modèle hiérarchique qui s'apparente au modèle de [CAR 93] peut être proposé, dans lequel nous aurons trois niveaux d'intelligence, du niveau le plus général au niveau le plus proche des particularités de chaque situation. Ce modèle hiérarchique intègre à la fois l'intelligence générale ainsi que les autres formes spécifiques d'intelligence.

Le premier niveau concerne l'intelligence générale [CAR 93] [MEY 06], les performances à différentes tâches cognitives dépendent toutes d'un même facteur d'intelligence général. Les potentialités qui se rapportent à ce niveau relatent d'aptitudes très générales. Cette intelligence générale est sous-jacente à toutes les formes d'intelligence. Ce premier niveau s'apparente à notre sens à un système d'information classique représenté par la boucle Mesure-Décision-Action où la décision est prise en fonction d'une image de l'état du processus donnée par les capteurs. Lorsque cette image décrit convenablement l'état réel du processus, les décisions d'actions seront mieux adaptées.

Le deuxième niveau concerne des formes spécifiques d'intelligence décrites par huit facteurs de groupes dans [CAR 93]. Ces facteurs de groupes sont l'intelligence fluide, l'intelligence cristallisée, la mémoire générale et l'apprentissage, la perception visuelle, la perception auditive, la capacité de rappel, la rapidité cognitive et la vitesse de traitement. [ALB 91] a qualifié l'intelligence dans ce niveau par l'habilité à reconnaître les objets et les événements et planifier l'avenir. Nous pouvons attribuer ce niveau d'intelligence à un système dans lequel on observe une croissance et une évolution tant par l'accroissement en puissance de calcul et par l'accumulation de connaissances sur la façon de détecter, de décider et d'agir dans des situations complexes et difficiles. Les aspects spécifiques de l'intelligence décrits dans [CAR 93] peuvent être alors assimilés dans un point de vue système d'information à travers les correspondances suivantes : l'ensemble intelligence fluide, intelligence cristallisée et mémoire générale d'apprentissage correspond aux mémoires du système; la perception visuelle et auditive correspondent aux éléments de sensation du système et finalement l'ensemble constitué de la capacité de rappel, de la rapidité cognitive et de la vitesse de traitement correspond au traitement logique des informations supporté par un microcontrôleur.

Finalement, le troisième niveau d'après [ALB 91] se rapporte à une forme avancée d'intelligence qui fournit la capacité de percevoir et de comprendre, de choisir de façon judicieuse, et d'agir avec succès sous une grande variété de circonstances afin de prospérer dans un environnement complexe et souvent hostile. [STE 03] va dans le même sens en déclinant une l'intelligence pratique qu'il définit par l'aptitude à trouver la meilleure adaptation possible entre soi et les demandes de l'environnement. Nous constatons que l'appréhension de l'environnement est essentielle à ce niveau d'intelligence. En effet, il ne suffit plus au système d'information d'améliorer la qualité de l'image du processus à travers le traitement local au niveau de ses capteurs permettant l'amélioration de la qualité du signal élaboré (correction…) mais aussi être en mesure de permettre l'échange d'informations élaborées et la coopération entre différents nœuds du système pour permettre de prendre des décisions et d'agir sur le processus d'une façon convenable.

Dans la section suivante, nous allons nous intéresser à l'instrumentation intelligente par l'introduction du concept d'instrument intelligent.

3. Concept d'instrument intelligent

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.

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…

[NOB 04] définit un instrument intelligent par un instrument dont le but principal est la mesure ou la commande d'une variable d'un processus, c'est un instrument incluant de la flexibilité dans son utilisation avec des paramètres réglés par le fabricant ou l'opérateur. Le cycle de vie d'un instrument intelligent inclut la production de quelques progiciels générés par le fabricant et utilisés pour la configuration par l'opérateur.

3.1. Evolution des instruments intelligents

3.1.1. Les instruments intelligents jusqu'au milieu des années 1990

L'instrument intelligent était basé sur l'utilisation d'un élément de mesure traditionnel, mais a inclut des possibilités de traitements micro programmés pour améliorer l'exécution de l'élément de mesure. La sortie était analogique en 4-20 mA et peut être aussi numérique en ajoutant le protocole HART par exemple.

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 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. Les instruments intelligents après la fin des années 1990

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 [NOB 04].

3.2. Instrument “smart“ et instrument intelligent

L’évolution des instruments fait apparaître une progression de l’instrument analogique, à l’instrument numérique puis à l’instrument intelligent avec les limites suivantes :

- ✓ L’instrument analogique rudimentaire a pour rôle une simple conversion qui est une transmission d’une information analogique pour le capteur et une action sur le processus pour un actionneur.
- ✓ L’instrument numérique offre aussi la conversion du signal à travers une chaîne de traitements offrant la possibilité de numériser le signal en vue de son utilisation par une centrale d’acquisition.
- ✓ L’instrument "Smart" possède des fonctionnalités qui améliorent ses performances métrologiques, par des fonctions embarquées de mémorisation et de traitement de données.
- ✓ L’instrument intelligent est enrichi par une capacité à crédibiliser sa fonction associée à une implication plus importante dans la réalisation des fonctions du système auquel il appartient. Cette crédibilisation fait référence à une certaine capacité à valider la mesure produite pour le capteur ou rendre compte de la réalisation effective pour l’actionneur. L’instrument intelligent participe à la commande du système, à sa sécurité en offrant des possibilités d’alarme, à son exploitation en diffusant des informations relatives à sa maintenance. Il coopère via un système de communication, sélectionne les données à transmettre et éventuellement prend une décision.

Le dictionnaire de l’IEEE [DOR 93] tente d’élucider la distinction entre l’instrument "Smart" et l’instrument intelligent en stipulant que les systèmes intelligents, sont construits à partir de systèmes "Smart", avec un ensemble dédié d’actionneurs et de capteurs intégrés, et que les systèmes "Smart" contiennent une grande partie de capteurs distribués. En général, le terme de systèmes "Smart" implique généralement un constituant structurel dans lequel des fonctions numériques de détection, d'actionnement, de traitement du signal et de commande sont intégrées de façon tangible.

D’autres auteurs [FRA 00] [ZHA 04] étayent également que la définition de "Smart instruments" n'a pas été aussi largement acceptée et elle est soumise à un mauvais usage. [FRA 00] définit malgré cela un instrument "Smart" comme un instrument qui fournit des fonctions au-delà de celles qui sont nécessaires pour générer une représentation correcte des grandeurs détectées ou commandées. Cette fonction simplifie généralement l'intégration de l’instrument dans des applications dans un environnement de réseau ". Cette définition fournit un point de départ pour le contenu minimum d'un instrument "Smart" [FRA 00].

La distinction entre "Smart sensor "et "Intelligent sensor" est illustrée par la figure 1.1 :

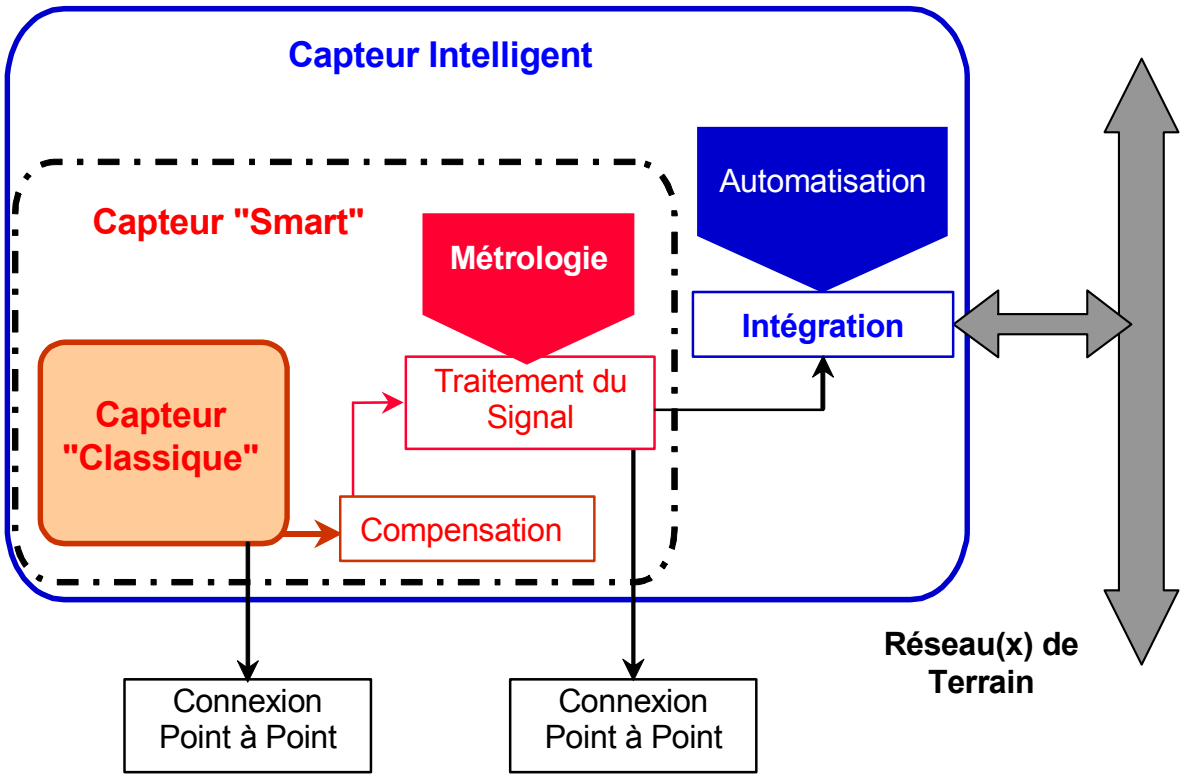


Figure 1.1 : Capteur "Smart" et Capteur Intelligent

Finalement notons que jusqu'à présent, aucun accord commun n'a été étendu à la définition d'un capteur intelligent avec l'absence d'une définition officielle de n'importe quelle organisation [ZHA 04] [MAS 98] [BOW 94].

Nous allons revenir à ces définitions sous forme de classification par niveaux à la fin de ce chapitre.

3.3. Architecture matérielle d'un instrument intelligent

3.3.1. Constituants de l'architecture matérielle

L'architecture matérielle support de l'intelligence des instruments (capteurs ou actionneurs) est réalisée autour d'un système à microprocesseur qui établit un dialogue permanent avec les différents constituants à travers un bus interne. Elle dépend de l'application et de l'environnement de communication et peut être associée, par exemple, à des robots ou à des automates programmables. Elle se compose des sous-ensembles suivants :

- ✓ Des moyens de communication avec les opérateurs et/ou le système d'automatisation ; ces moyens permettent l'échange des informations utilisées par les opérateurs ou les autres équipements de la structure distribuée,
- ✓ Des moyens de traitement numérique (unité de calcul associée à des mémoires) qui permettent le traitement des informations et la distribution du système,
- ✓ Un transducteur pour le capteur ou un organe d'actionnement pour l'actionneur.

[MEK06] propose une architecture matérielle comprenant les éléments suivants:

- ✓ un élément de sensation qui lie le monde extérieur à un système de capteur par la génération d'un signal électrique (par exemple la tension, le courant) avec la réponse aux propriétés physiques de l'environnement telles que la température, la pression, l'intensité lumineuse, le son, la vibration, etc.
- ✓ un élément d'interface pour le conditionnement du signal et la conversion de donnée. Le signal obtenu en sortie du capteur est modifié et converti en donnée numérique avant d'être transféré à l'élément de traitement.
- ✓ un élément de traitement qui inclut un microcontrôleur avec une mémoire associée et un logiciel; c'est la composante principale de l'architecture où le signal entrant est traité.
- ✓ un élément de communication, lequel pourvoit une communication bidirectionnelle entre l'élément de traitement et les utilisateurs.
- ✓ une source d'alimentation.

L'architecture matérielle d'un instrument intelligent s'apparente à celle d'une machine informatique classique. Ainsi pour un utilisateur externe, un instrument peut être considéré comme une entité proposant des services qui manipulent des variables et font appel à un ensemble de ressources [TAI 00].

La figure 1.2 présente un modèle standard d'architecture matérielle pour les instruments intelligents [BEA 93] [BAY 94]. Cette structure est devenue standard grâce à la norme IEEE1451 [SHN00] qui la reprend. Cette norme a pour but de fournir un cadre cohérent et ouvert permettant la mise en relation d'appareillages de faible capacité mémoire et dont les possibilités se réduisent à opérer des prises de mesures en un point donné.

La philosophie générale du développement de ce standard repose sur la création d'une volonté d'uniformiser les interfaces des appareils, et ce en ajoutant des capacités à celles déjà existantes, tout en conservant le coût de la transition possible à tous les vendeurs de l'industrie.

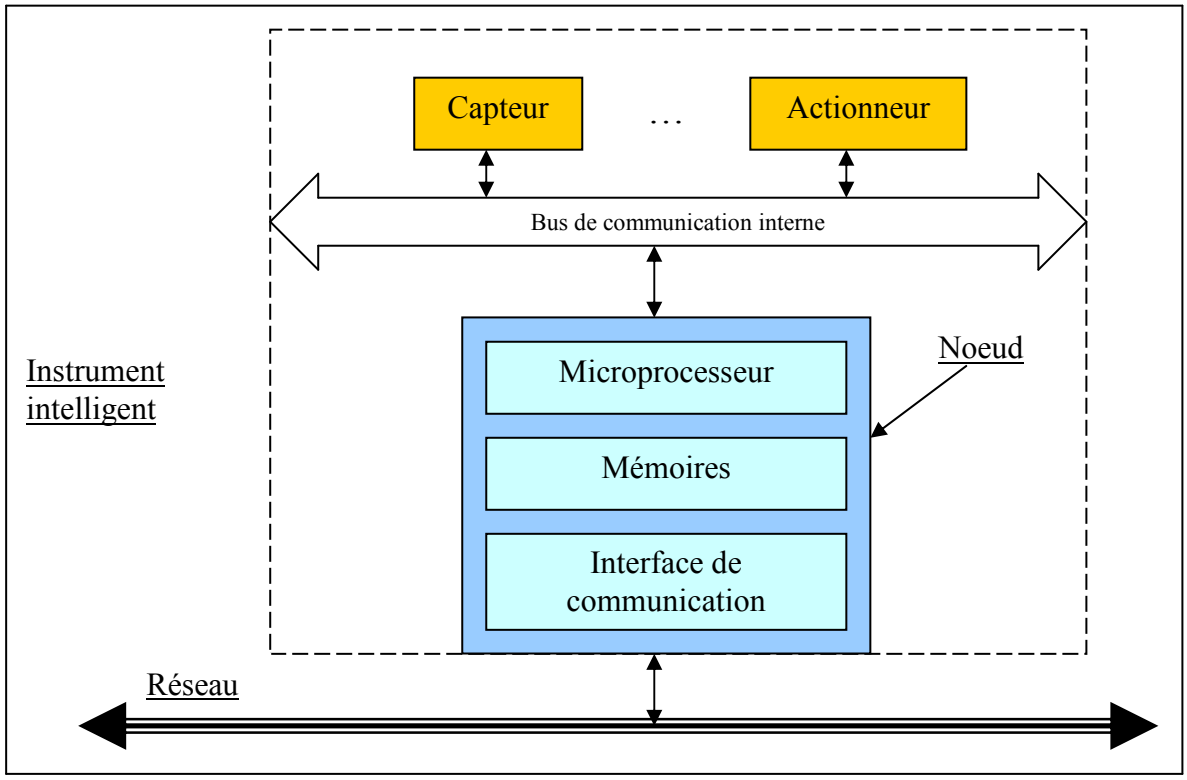


Figure 1.2 : Architecture matérielle d'instruments intelligents

Le standard envisagé propose également l'indépendance vis-à-vis de la couche réseau mise en œuvre ainsi que l'indépendance vis-à-vis du type de microprocesseur embarqué sur le système. La famille 1451P consiste en la proposition et le développement de quatre standards :

- ✓ IEEE 1451.1, Network Capable Application Processor (NCAP);
- ✓ IEEE 1451.2, Transducer to Microprocessor and Transducer Electronic Data Sheet (TEDS) Format;
- ✓ IEEE 1451.3, Digital Communication and Transducer Electronic Data Sheet (TEDS) Format for Distributed Multidrop Systems;
- ✓ IEEE 1451.4, Mixed Mode Communication Protocols and TEDS Formats.

Un instrument intelligent est donc constitué de capteurs ou d'actionneurs reliés à un nœud par l'intermédiaire d'un bus interne. Cet instrument peut être composé uniquement de capteurs, uniquement d'actionneurs ou des deux. Il peut aussi être composé d'un seul capteur et d'un seul actionneur.

Un noeud est un ensemble de composants dont les principaux sont :

- ✓ Le microprocesseur : qui permet de faire les calculs,
- ✓ Les mémoires (ROM ou EPROM, RAM),
- ✓ L'interface de communication : qui permet de gérer la réception ou l'émission de données sur le réseau.

Une telle architecture matérielle est capable d'intégrer les différentes fonctionnalités qui peuvent appartenir aux instruments intelligents.

3.3.2. Aperçu sur la norme IEEE 1451

La norme IEEE 1451 [IEE 04] a pour objectif de définir une interface standardisée pour les réseaux de capteurs. Celle-ci offre la possibilité de configurer automatiquement les capteurs en y intégrant une interface spécifique et une fonction d'auto-reconnaissance. Cette norme spécifie le format d'une fiche technique embarquée dans la mémoire du capteur sous forme du fichier TEDS (pour Tranducer Electronic Data Sheett). Ce fichier est une sorte d'identificateur de capteur. Cette fiche possède, entre autre, l'identité du capteur, ses caractéristiques (sensibilité,...) ainsi que la possibilité pour l'utilisateur d'ajouter des données personnelles (localisation du capteur,...) [LEE 00]. Ce concept est déjà mis en œuvre dans les capteurs de process (type Hart et bus de terrain) mais le terme TEDS est plutôt réservé aux capteurs de mesure mécanique.

Le fichier TEDS comprend trois zones distinctes, l'une spécifie l'identité du capteur (son fabricant, son numéro de série, etc…), la deuxième comporte ses principales caractéristiques techniques (avec notamment sa gamme de mesure, sa sensibilité, sa date d'étalonnage, etc…), et la dernière est réservée à l'utilisateur.

Cette norme standardise les caractéristiques des capteurs intelligents à savoir la définition des interfaces pour qu'ils puissent se connecter à des réseaux divers. Parmi ces fonctions, nous pouvons citer : la facilité d'installation, l'auto-identification, l'auto-diagnostic, la fiabilité, le temps d'éveil pour la coordination avec d'autres noeuds, quelques fonctions logicielles, le traitement du signal, des protocoles de contrôles standards et des interfaces réseaux. De plus, cette norme vise à rapprocher l'intelligence du point de la mesure et à minimiser les coûts d'intégration ou de maintenance dans des réseaux distribués [LEW 04]. La norme propose également l'indépendance vis-à-vis de la couche réseau mise en œuvre ainsi que l'indépendance vis-à-vis du type de microprocesseur embarqué sur le système.

Cette norme n'est pas encore achevée, c'est une solution provisoire et une étape vers des capteurs intelligents raccordés sur un réseau universel.

3.4. Architecture fonctionnelle

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 [ROB 93] a proposé les fonctionnalités de configuration, de communication, de mesure, de calcul et de validation. De même, Meijer [MEI 94] inclut trois fonctionnalités; compensation, calcul et communication. Tandis que Tian [TIA00] suggérait que ce qui s'appelle un capteur intelligent devrait avoir les fonctions de compensation, validation, fusion de données (data-fusion) et communication. Pour Revillard [REV 05] un instrument intelligent est capable d'intégrer des fonctionnalités comme la communication, l'auto-configuration, l'auto-contrôle. Mekid [MEK 06] 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'auto-calibration.

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.

La fonction de la fusion de données est de s'assurer que seule l'information la plus appropriée soit transmise entre les capteurs.

Les fonctionnalités génériques des capteurs intelligents se résument comme suit : l'acquisition (mesure et conditionnement), la configuration (paramétrage et réglage), la validation (traitement et prise de décision) et la communication.

Si la fonction mesure est l'une des fonctions primordiales d'un capteur intelligent, car elle permet d'alimenter par les données qu'elle fournit toutes les autres fonctionnalités, il en est autrement pour l'actionneur intelligent.

En ce qui concerne l'actionneur intelligent, on peut réutiliser la même architecture fonctionnelle et remplacer la fonctionnalité mesure par une autre que l'on nommera actionnement et qui aura pour but d'exécuter la commande reçue par l'actionneur. On dit que ce type d'actionneur intelligent fonctionne en boucle ouverte. On dit que celui-ci fonctionne en boucle ouverte s'il ne dispose pas de fonction "mesure" et qu'il fonctionne en boucle fermée s'il possède un système d'information comprenant au minimum cette fonction, dont le rôle est de délivrer les informations nécessaires à l'élaboration de la commande. Ainsi un actionneur, outre ses fonctionnalités propres, intègre celles du capteur et il dispose de possibilités de gestion locale des informations.

Une illustration des fonctionnalités d'un capteur intelligent est montrée dans la figure 1.3 [ROB 93] :

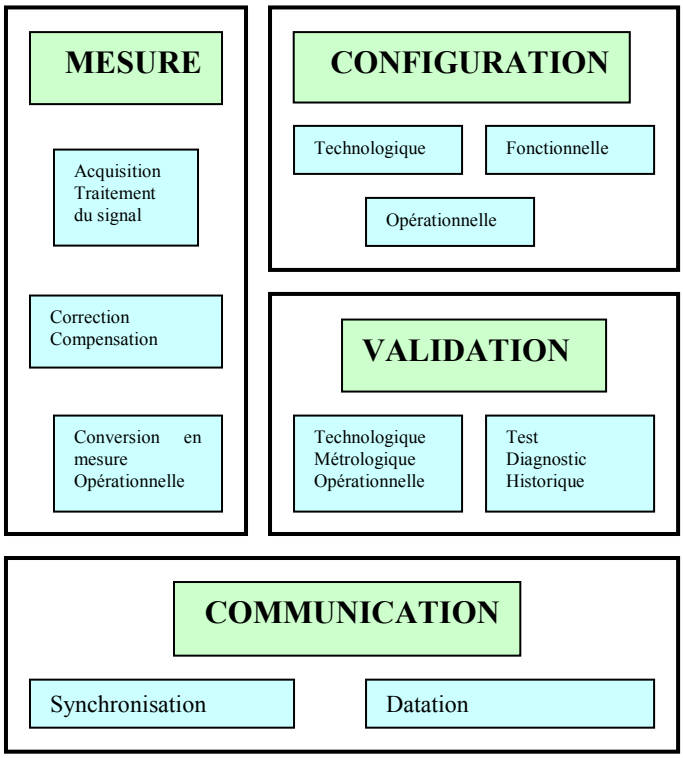


Figure 1.3 : Fonctionnalités d'un capteur intelligent [ROB 93]

La structure fonctionnelle d'un actionneur intelligent comprend les fonctions *actionner*, *traiter*, *mesurer*, *communiquer* bénéficiant de l'amélioration de leurs performances que permet d'intégrer une capacité locale de traitement de l'information [STA 94]. La fonction *traiter* comprend les activités *surveiller*, *élaborer* des informations, *gérer* la base de données. Ce traitement d'information là où elles sont produites permet de fournir une base de données locale validée pour l'ensemble des utilisateurs.

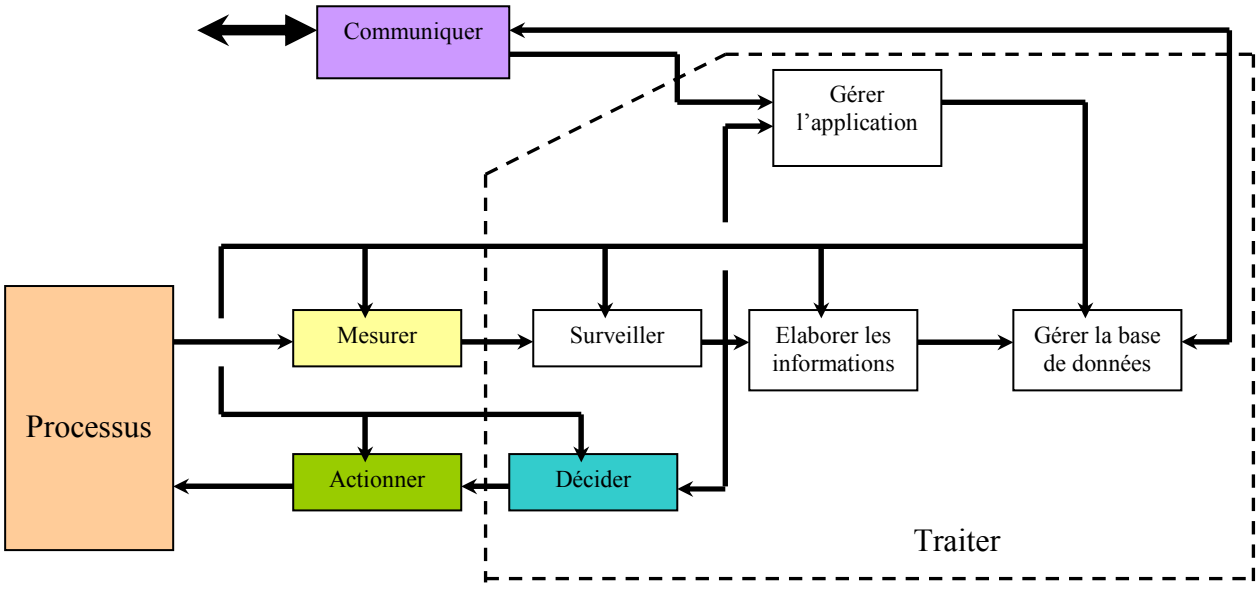


Figure 1.4 : Architecture fonctionnelle générique d'un actionneur intelligent [STA 94]

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 1.5 illustre une proposition de fonctionnalités d'un instrument intelligent générique.

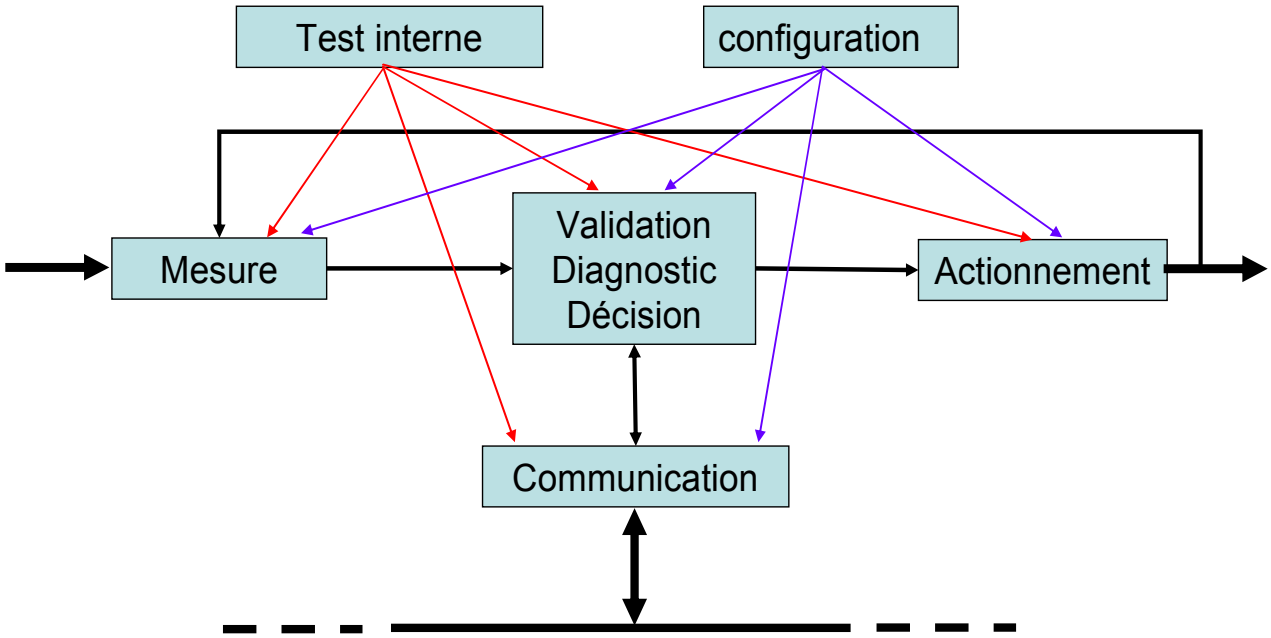


Figure 1.5 : Architecture fonctionnelle d'instruments intelligents

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.

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 noeud 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.

4. 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.

Le modèle interne [GEH 94] 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.

Le modèle externe [RUM 91] 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.

Nous abordons quelques modèles génériques d'instruments intelligents.

4.1. Modèles internes

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 [CAL 90].

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) [RUM 91]. 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).

4.2. Modèle USOM (modèle externe)

En ce qui concerne le modèle externe, l'approche USOM (USer Operating Mode) est la plus répandue [BOU 97]. 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.

4.2.1. Services d'un instrument intelligent

Les services sont définis d'un point de vue externe, ils sont le résultat de l'exécution d'un traitement (ou l'ensemble de traitements), auquel on peut associer une interprétation en termes fonctionnels. La description d'un service consiste à décrire le résultat produit par son exécution. Un service est une entité qui consomme des variables et en produit d'autres conformément à la figure suivante :

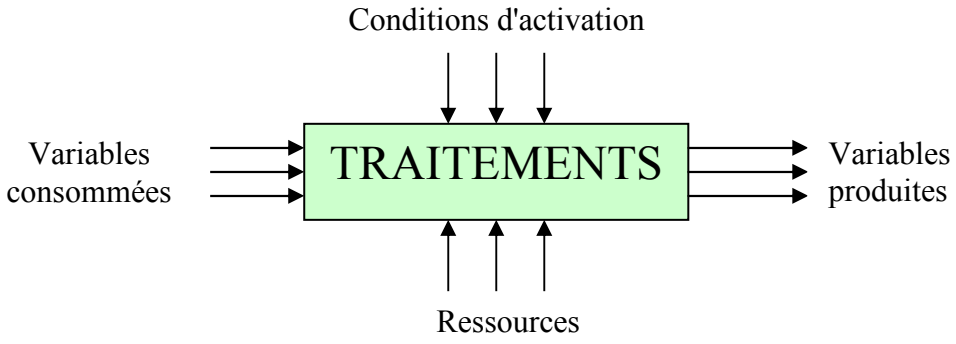


Figure 1.6 : Représentation d'un service

L'exécution d'un service est déclenchée par l'avènement d'une condition d'activation et nécessite la disponibilité d'un certain nombre de ressources. Le service peut s'exécuter de manière nominale dans le cas où l'ensemble de ressources qu'il utilise est validé.

La défaillance de certaines ressources n'implique pas forcément l'indisponibilité du service qui les utilise. Des traitements de remplacement peuvent être prévus. L'ensemble de ces traitements définit les versions possibles de ce service.

4.2.2. Organisation des services en modes d'utilisation

Un mode d'utilisation comprend au moins un service et chaque service appartient à au moins un mode d'utilisation. Ainsi l'ensemble des modes d'utilisation est un recouvrement de l'ensemble des services.

A un instant donné, l'instrument se trouve dans un mode d'utilisation donné. Seuls les services appartenant à ce mode pourront être exécutés.

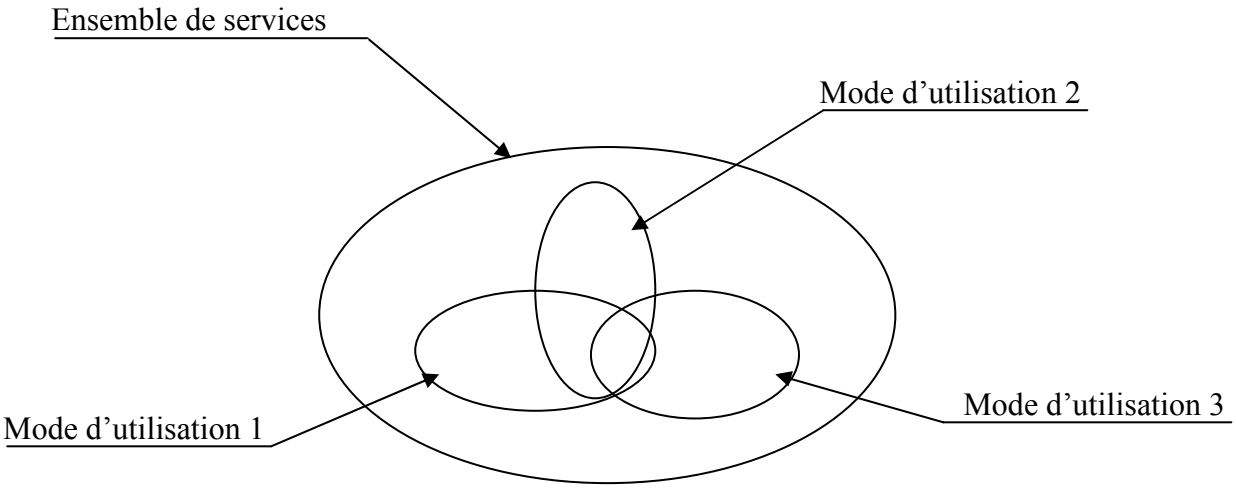


Figure 1.7 : Modes d'utilisation et services

4.3. Approche client serveur

Le choix d'un modèle générique doit permettre l'expression d'une architecture fonctionnelle générale adaptée aux applications de contrôle-commande.

Tailland [TAI 00] considère que les deux modèles internes et externes sont nécessaires et complémentaires. Il voit la couche interne d'un instrument intelligent comme un enchaînement de services appelés services internes. Ces services internes sont des entités fonctionnelles élémentaires qui ne sont pas accessibles directement par l'utilisateur. En fait, ce modèle utilise une approche client/serveur qui positionne la couche interne comme serveur de la couche externe. Pour la couche externe, le modèle USOM est utilisé. Donc, l'utilisateur voit l'instrument intelligent comme un ensemble de services (les services externes).

Révillard [REV 05] élabore un modèle d'instrument intelligent qui se base sur le modèle client/serveur en reprenant des études menées dans [TAI 00]. Ce modèle d'instruments intelligents traite la relation de type client/serveur qui permet d'exprimer les fonctionnalités offertes par un instrument à son utilisateur (personne physique ou autre instrument intelligent). Il traite aussi la relation client/serveur qui s'établit au sein même de l'instrument intelligent. Cette relation se manifeste par la réalisation de service externe par l'instrument intelligent. La conception des instruments intelligents utilise une méthode de conception centrée architecture avec un logiciel qui gère le comportement des instruments intelligents.

La figure 1.8 est le résultat des études menées dans [BEN 01]. Elle représente le modèle d'instrument intelligent qui se base sur le modèle client/serveur de [CAL 90].

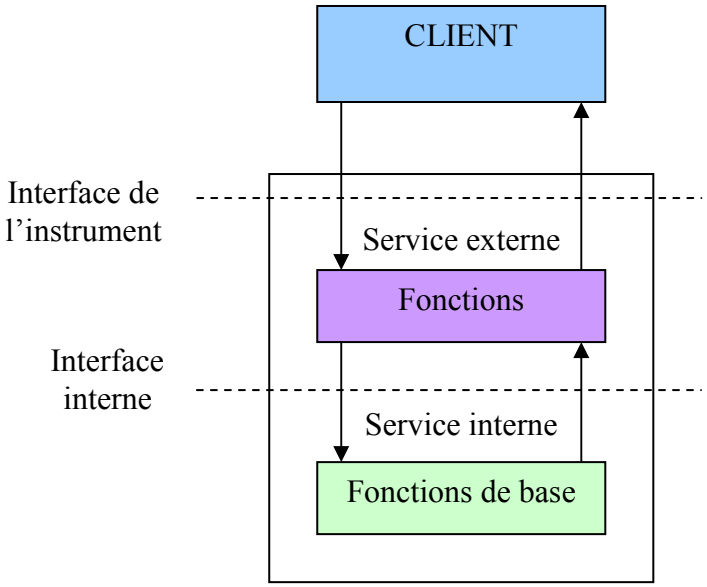


Figure 1.8 : Modèle client/serveur

Après avoir dressé le concept d'instrument intelligent, nous allons dans ce qui celui s'intéresser au système d'automatisation à intelligence distribuée qui intègre ce type d'instruments.

5. Systèmes d'automatisation à intelligence distribuée

5.1. Introduction

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. 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.

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 4-20 mA 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 dotés 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).

.

5.2. Evolution des SAP vers les SAID

Un système automatisé accomplit des fonctions en minimisant les interventions humaines. L'accomplissement de ces fonctions est équivalent à la délivrance de services qui ont pour objectifs en particulier l'augmentation de la productivité, l'amélioration de la qualité, l'augmentation de la sécurité ainsi que de faciliter la tâche des opérateurs.

Un système automatisé se compose d'un certain ensemble d'entités en interaction qui sont l'homme, le processus à automatiser, le système d'automatisation. Ces entités sont organisées pour satisfaire un besoin et le choix de l'organisation est fait en fonction du procédé.

Un Système Automatisé de Production (SAP) désigne l'ensemble des installations destinées à augmenter la valeur ajoutée de produits conformément aux objectifs de productivité, de qualité, de fiabilité, etc. Il regroupe l'ensemble des moyens matériels et logiciels conduisant à la fabrication d'un produit.

Le SAP regroupe ainsi les éléments constituants la partie automatisme, communication et conduite de l'installation. Il assure l'acquisition des informations fournies par les capteurs, en fait le traitement et élabore la commande des actionneurs.

Une autre approche du SAP consiste à le décomposer en deux parties bien distinctes, une partie commande (ou système d'information) où sont effectuées les tâches de coordination et une partie opérative qui est constituée en partie du processus physique [GRE 91]. Capteurs, actionneurs et machines-outils dans les processus manufacturiers constituent la partie opérative du processus.

Le SAP assure aussi la communication par l'échange d'information avec son environnement. Il comprend également une interface avec les opérateurs permettant la conduite ainsi que la gestion technique. Le SAP est en effet en relation directe avec le système de décision de l'entreprise.

On distingue trois types d'architectures différentes pour structurer les systèmes automatisés de production :

L'architecture fonctionnelle d'un système d'automatisation est un modèle abstrait formalisé de la structure et du comportement externe des activités du système d'automatisation. C'est une description de la solution envisagée pour répondre aux exigences du cahier des charges. L'architecture fonctionnelle est un résultat de l'étape de spécification.

L'architecture matérielle d'un système automatisé est constituée d'un ensemble de machines dotées de systèmes d'exploitation, d'un ensemble de moyens de communication connectant ces machines.

L'architecture opérationnelle désignera le résultat d'une projection de l'architecture fonctionnelle sur une architecture matérielle. L'architecture opérationnelle validée et optimisée est le résultat de l'étape de conception. Il s'agit de la "meilleure" architecture opérationnelle au sens d'un ou plusieurs critères. Elle est validée dans le sens où elle est conforme au cahier des charges, c'est-à-dire qu'elle respecte toutes les contraintes énoncées [TAI 00].

Le terme SAID provient donc de SAP (Système Automatisé de Production) auquel ID (Intelligence Distribuée) a été ajoutée dans les années quatre-vingt-dix avec l'apparition des unités de traitement numérique et des réseaux de communication [THI 04]. Le terme P de production a ensuite été enlevé pour tendre à plus de généricité.

Les SAID sont des systèmes constitués de composants intelligents répartis autour d'un réseau de communication tel qu'un réseau de terrain. Dans le cas où la boucle de commande est fermée par un canal de communication, ces systèmes sont appelés des systèmes commandés en réseau ("Networked Control Systems" ou NCS) [WAL 99].

D'après le dictionnaire de l'IEEE [DOR 93], le SAID est une structure de contrôle interactif intégrant des caractéristiques cognitives qui peuvent inclure des techniques d'intelligence artificielle et certaines constructions fondées sur la connaissance pour émuler le comportement d'apprentissage avec une capacité globale de la performance. Le rôle du SAID est de pouvoir fournir une approche systématique pour traiter les nombreuses contraintes qui sont impliquées dans la commande.

Les SAID se sont développés avec l'augmentation croissante du nombre d'informations nécessaires au contrôle des processus industriels qui a conduit au développement d'unités de traitement de plus en plus performantes, capables de traiter rapidement un grand nombre d'informations. Ces systèmes permettent aussi une grande flexibilité en terme de vitesse de commande, de sécurité, de conformité de la fabrication, de fiabilité [LAF 97]. Ils contribuent à assurer d'importants services comme le traitement et la communication [DAI 03].

La première évolution est apparue avec l'introduction des bus de terrain, ils ont permis de déporter les entrées/sorties numériques et analogiques et de réduire les coûts et temps de câblage. L'ensemble des informations est traité par l'unité centrale.

La répartition de l'unité centrale et le rapprochement des traitements au niveau des instruments de terrain ont fait évoluer le concept de systèmes d'automatisation vers celui de SAID [BAY 05] [HER 97]. Les traitements locaux peuvent être implantés directement dans les composants d'automatisme intelligents (capteurs et actionneurs intelligents) ou dans des petites unités de traitements (micro-automate) gérant un sous-ensemble de composants intelligents.

Le micro-automate communicant sera utilisé comme un module de traitement déporté pour traiter une partie de l'application [CHO 96].

La figure 1.9 montre 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.

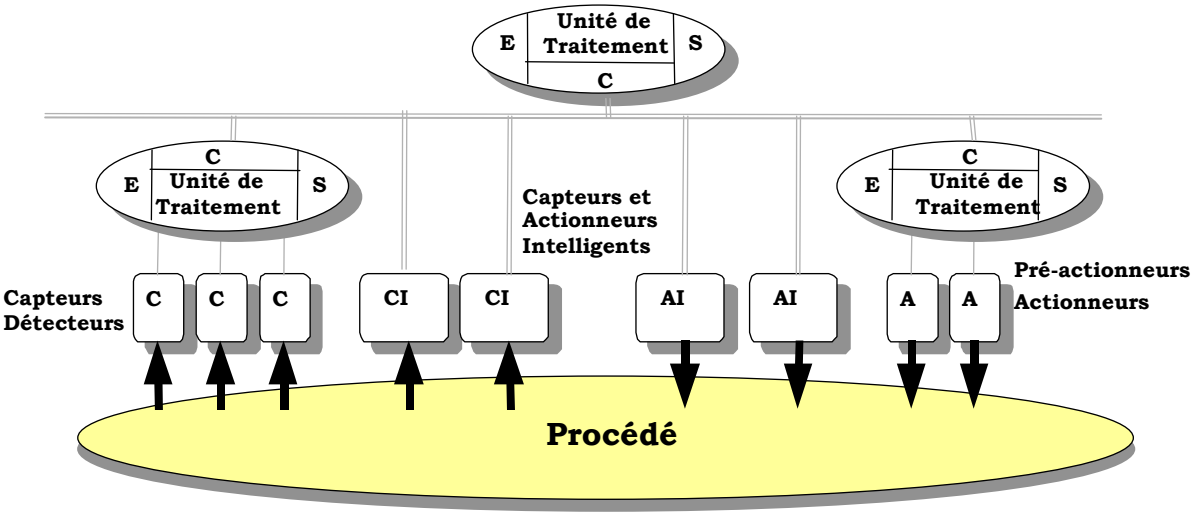


Figure 1.9 : Automatisme décentralisé

De nos jours, les architectures distribuées sont la base de beaucoup de systèmes industriels [CAM 99]. 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 [LEE 01]. 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.

5.3. 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 [RIE 02], 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 [BAR 03]. 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 pour un actionneur subissant une usure.

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 l'analyse et la conception de ces systèmes [ZHA 01]. 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.

Néanmoins, ces systèmes associant des réseaux de communication offrent des améliorations 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.

5.4. Les SAID sont ils considérés comme des systèmes complexes ?

La complexité d'un système tient compte de leurs comportements, leur taille, de la diversité des informations mises en jeu ainsi que des phénomènes régissant le fonctionnement de ces systèmes [BEN 04].

Les systèmes complexes posent des problèmes nouveaux et importants d'analyse et de modélisation et parfois il n'est pas possible de passer de l'étape de l'analyse à l'étape de l'exécution des traitements sans le passage par des étapes intermédiaires permettant la réduction du problème.

La modélisation de systèmes complexes conduit à l'obtention de modèles non-linéaires dont la dynamique est influencée à la fois par des événements discrets et des dynamiques continues.

Le cas des SAID s'apparente bien au cas des systèmes complexes dont la complexité est aussi liée à l'étude de la sûreté de fonctionnement.

Dans [NIC 90], il est rappelé que la défaillance d'une simple pièce, le non-respect d'une partie de la procédure, une erreur de diagnostic peuvent en certaines circonstances compromettre gravement le fonctionnement d'une installation.

5.5. SAID et sûreté de fonctionnement

La distribution des traitements dans les SAID apporte à priori plus d'efficacité au niveau de la sûreté de fonctionnement de ces systèmes par rapport aux systèmes classiques à architecture centralisée [LAP 95] [VIL 88]. En effet, la défaillance d'une unité de commande n'entraîne pas nécessairement l'arrêt de l'installation dans la mesure où une distribution des tâches vers les autres unités est réalisée.

L'intelligence dans les capteurs et actionneurs contribue à crédibiliser les informations produites ou les actions effectuées visant des objectifs de sûreté de fonctionnement. L'utilisation des réseaux de terrain permettant la diffusion des informations vers tous les équipements et la délocalisation des traitements au plus près du processus permettent une réactivité à l'occurrence d'incidents ce qui contribue à l'amélioration de la fiabilité. La maintenabilité est grandement facilitée par les possibilités d'interrogation à distance sur l'état des composants.

Un autre attribut de la sûreté de fonctionnement concerne la crédibilité englobant les aspects intégrité et sûreté [CEI 91] et correspondant à l'assurance fournie par le dispositif de sa capacité à reconnaître et à signaler son état. La crédibilité est améliorée par l'ensemble des moyens de validation des instruments intelligents.

Finalement, 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 [CAM 01] dans les applications où la sécurité est critique mais elle peut introduire de nouveaux modes de défaillance affectant la sécurité [GAR 02]. Ainsi, les capacités de communication offrent des possibilités d'autodiagnostic et une mise en place d'arc réflexe permettant l'amélioration de la sécurité. D'autre part, de par leur complexité, ces systèmes peuvent également être sources de défaillance.

Il est nécessaire alors d'étudier et d'améliorer la sûreté de fonctionnement des systèmes qui pourraient impliquer certains risques pour le processus de commande ou aux utilisateurs [CAM 97].

Quant à l'évaluation de la sûreté de fonctionnement des SAID, elle n'est pas triviale [JUM 03] [BAR 02]. Quelques problèmes à résoudre concernent l'évaluation des algorithmes et programmes, l'utilisation du réseau de communication (délai …), l'évaluation globale de la sûreté de fonctionnement en tenant compte des caractéristiques des composants et de la topologie du système distribué. Cette évaluation concerne deux approches : l'approche statique (aspect structurel) [CON 99] et l'approche dynamique (aspect fonctionnel et dysfonctionnel) [BAR 03].

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 à son environnement. Un modèle générique des différentes causes directes d'un accident est présenté dans [KUM 96] (cf. figure 1.10).

Des études ont été réalisées pour l'évaluation de la sûreté de fonctionnement des SAID en phase dynamique en estimant le taux d'usure en fonction de la configuration dynamique du système [MKH 05] [BAR 03]. Ceci a permis d'obtenir une comparaison quantitative des comportements dynamiques du système.

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 [BEN 04]:

- ✓ 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.

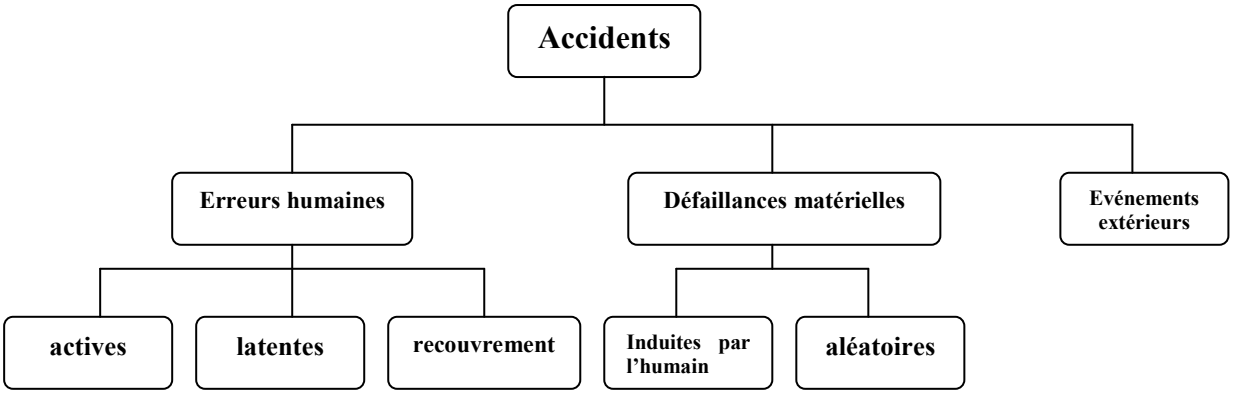


Figure 1.10 : Causes d'un accident selon [KUM 96]

6. Validation dans les instruments intelligents

Un instrument intelligent doit fournir des informations réputées valides. La notion d'informations valides oblige la prise en compte de l'univers de la validation au sens le plus large. Il y a toujours une limite au delà de laquelle la validation devient impossible. Cette limite peut être soit : économique, technologique, ou liée à la méthode d'élaboration de la mesure …

La fonctionnalité validation d'un instrument intelligent se doit de couvrir : la totalité de la technologie alors mise en œuvre, l'ensemble de l'espace fonctionnel de l'instrument, et enfin le domaine opérationnel spécifique à l'exploitant propriétaire de l'instance matérielle de l'instrument.

La validation des données est une notion très importante dans la mesure que les systèmes sensibles aux défauts sont pris en compte. Lorsque des capteurs intelligents sont inclus dans de tels systèmes, des données sont fournies et elles vont qualifier l'estimation produite avec une certaine confiance associée.

6.1. Hiérarchie nécessaire à l'élaboration de la mesure

L'élaboration de la mesure opérationnelle fournie au consommateur doit être structurée selon une certaine hiérarchie [ROB 93].

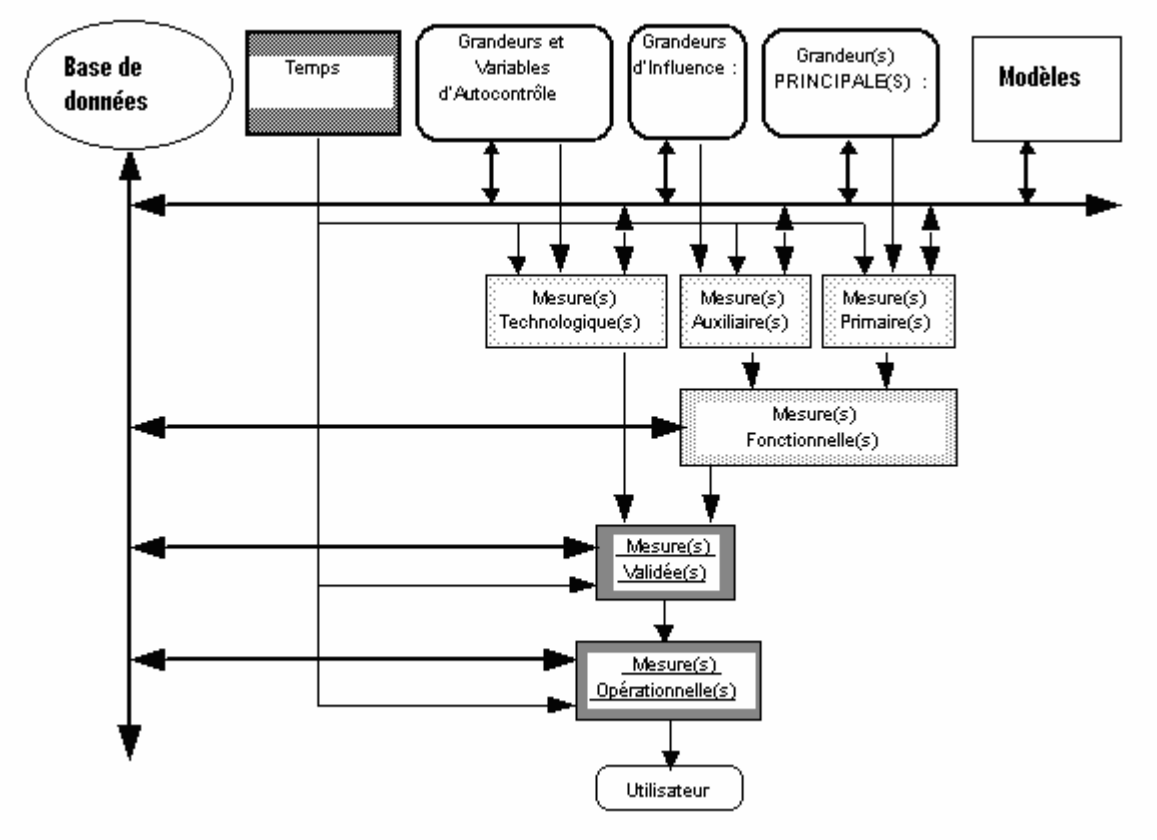


Figure 1.11 : Hiérarchie d'élaboration de la mesure opérationnelle [ROB 93]

La figure 1.11 décrit la hiérarchie nécessaire à l'élaboration de la mesure opérationnelle qui est une mesure validée directement exploitable par l'utilisateur.

La mesure opérationnelle est issue de mesures primaires (grandeurs principales), celles-ci sont éventuellement corrigées par les mesures secondaires (grandeurs d'influence) et elles sont validées par référence à des modèles.

La fonctionnalité validation d'un instrument intelligent couvre la technologie mise en œuvre, les mesures fonctionnelles incluant les mesures auxiliaires et le domaine opérationnel spécifique au consommateur.

Nous pouvons donc caractériser les trois formes principales de validation :

- ✓ La validation technologique : Elle consiste à s'assurer que le matériel n'est pas défaillant. Elle concerne le bon fonctionnement de l'instrument intelligent en termes de technologie comme par exemple la mesure de la tension de l'alimentation, de la température de l'électronique... Outre la défaillance, la détection d'erreur de conception/installation telle que le corps d'épreuve implanté ne correspond pas à la configuration de l'instrument, fait partie de la validation technologique. Ainsi la mesure fonctionnelle est validée par la prise en compte de mesures technologiques qui se rapportent particulièrement à la technologie de l'instrument [ROB 93]. Il faut noter que cette validation technologique ne garantit pas que l'estimation produite par le capteur est correcte, mais seulement que les conditions d'exploitation n'étaient pas contre des exactitudes éventuelles [STA 05].
- ✓ La validation fonctionnelle : Elle consiste à s'assurer que les informations sont valables d'un point de vue fonctionnel. Elle concerne toutes les formes de vérification de la cohérence des données ; ce peut être l'emploi de modèle (variation dans l'étendue de mesure) ou la comparaison de différentes mesures successives afin d'en détecter les erreurs éventuelles. La cohérence de la mesure par rapport à des modèles permet d'enrichir la validation. Les méthodes utilisées concernent le diagnostic à base de modèle et elles sont développées pour diverses applications et revêtent différentes formes suivant la nature des applications envisagées. Pour détecter les éléments défectueux d'un système, un certain degré de redondance est requis. La redondance désigne le fait de disposer d'une même information de plusieurs manières. Cette redondance est utilisée pour effectuer des tests de cohérence entre les variables mesurées elles-mêmes ou entre les variables mesurées et le modèle du système.
- ✓ La validation opérationnelle : Elle concerne essentiellement le recoupement d'informations entre les différents équipements du système et elle s'opère par l'intermédiaire d'un dialogue avec d'autres éléments du système; ainsi l'envoi d'un ordre à un actionneur doit être suivi d'un effet ressenti par certains capteurs et inversement, l'évolution d'une grandeur physique doit correspondre à l'effet de commandes transmises à un ou plusieurs actionneurs. Par ailleurs, outre la détection de défaillance, la validation opérationnelle doit contrôler que les paramètres entre instruments définis lors de la conception/installation sont cohérents (même unité de travail, période d'échantillonnage compatible…). La validation de la mesure opérationnelle s'opère aussi par l'intermédiaire d'un dialogue avec d'autres éléments distribués du système global assurant ainsi une sorte de redondance matérielle.

6.2. Caractéristiques de la validation

6.2.1. Validation au niveau du capteur

La fonctionnalité validation est indissociable de la fonctionnalité mesure et elle a pour rôle de décerner une confiance sur cette mesure. Nous allons nous intéresser dans ce paragraphe à voir comment on peut assurer une validation de type fonctionnel notamment avec des techniques éprouvées de diagnostic.

La détection de défauts basée sur l'utilisation de modèles (diagnostic) consiste en la génération de résidus par la reconstruction de la sortie et sa comparaison avec la sortie mesurée et ensuite l'étape de la validation consiste en la prise de décision vis-à-vis de ce modèle qui ne donne qu'une approximation du comportement réel.

La cohérence entre les signaux mesurés du système et ceux du modèle est reflétée par des caractéristiques statistiques d'un signal indicateur de défauts appelé résidu. Celui-ci est généré par un système qui filtre les entrées et les sorties de l'instrument [NYB 97]. En pratique, on génère des résidus ayant une moyenne nulle en fonctionnement normal et différents de zéro en fonctionnement défaillant.

Pour [CLA 00], la nouvelle fonction exigée d'un instrument intelligent est la génération en ligne de l'incertitude. C'est un nombre dans les mêmes unités que les données mesurées et qui représente l'erreur associée à la mesure. Cette incertitude sur la mesure possède deux composantes : les effets aléatoires dus aux bruits et les erreurs systématiques. Les expériences répétées peuvent réduire le premier mais pas le second.

Un modèle de défaut est donc une représentation formelle de la connaissance des défauts et de leurs façons d'influencer le système. Plus spécifiquement, le terme défaut signifie que le comportement d'un composant a dévié de son comportement normal. Pour autant, il ne signifie pas que l'instrument a cessé de fonctionner.

Un défaut dans le détecteur de température tel qu'un circuit ouvert est détectable par les autotests internes. Sans correction, le défaut est propagé par une équation de compensation pour produire un grand offset. Une fois le défaut marqué, l'approche correcte est d'utiliser la dernière bonne valeur du mesurande. L'incertitude relative correspond à la température enregistrée dans l'historique du capteur. La nouvelle valeur est peut être imprécise mais conviendra pour assurer la fonction.

Un autre algorithme possible consiste à prendre la moyenne des valeurs stockées dans un historique et se trouvant entre deux limites. La bonne valeur appartient à l'intervalle entre ces deux limites et la valeur moyenne de la température est celle qu'on utilise pour la compensation.

[ISE 92] propose un principe qui permet de calculer la nouvelle valeur des paramètres qui minimise l'écart entre les grandeurs mesurées et les grandeurs calculées avec les paramètres estimés.

Le résultat est ainsi comparé aux paramètres du modèle de référence obtenus dans le cas sans défauts et l'erreur d'estimation est alors utilisée comme résidu.

$$r(k) = \Theta_{nom} - \hat{\Theta}(k)$$

où Θ_{nom} est le vecteur des valeurs nominales des paramètres et $\hat{\Theta}(k)$ le vecteur de paramètres estimé à l'instant k.

Le vecteur de paramètres estimé $\hat{\Theta}(k)$ peut être calculé par deux façons : hors ligne ou en ligne. Dans le premier cas $\hat{\Theta}(k)$ est obtenu analytiquement à partir des mesures à chaque instant. Dans ce cas, l'algorithme de l'estimateur au sens des moindres carrés traite simultanément les N mesures recueillies sur le système. Dans le deuxième cas l'algorithme récursif traite les mesures successivement. C'est-à-dire que l'estimation future dépend de l'estimation présente.

Le choix d'un horizon glissant comportant N mesures s'avère plus efficace pour les raisons suivantes [BAI 07]:

- ✓ les données correspondant aux mesures peuvent être trop nombreuses pour être stockées en mémoire. On souhaite alors les utiliser simultanément et ne mémoriser

qu'une quantité limitée d'information, indépendante du nombre de mesures plutôt que d'avoir à gérer une importante base de données ;

- ✓ on peut vouloir utiliser les résultats pour prendre des décisions immédiates à partir des mesures réalisées, sans devoir attendre de disposer de toutes les données. Dans le contexte de la sûreté de fonctionnement, on souhaite suivre l'évolution des paramètres du système pour s'assurer que son comportement reste normal.

Ainsi, les tests vont porter sur le gradient (vitesse de variation) du signal plutôt que sur la valeur absolue du signal. La détection du défaut se fera si l'amplitude du signal n'est pas comprise dans un intervalle admissible.

La validation peut être représentée par l'intersection de trois cercles dans la figure 1.12 qui la montre comme résultat de combinaisons de technologies.

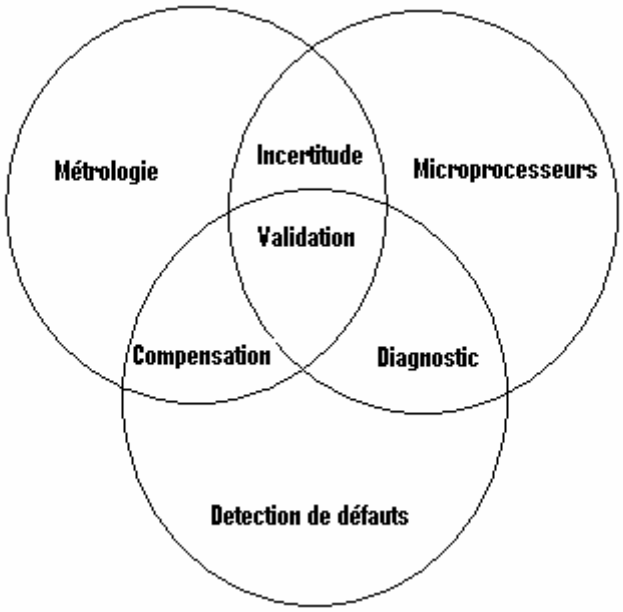


Figure 1.12 : La validation par combinaisons de technologies [CLA 00]

Nous constatons que la validation est au cœur d'un processus combinant plusieurs technologies. L'utilisation de microprocesseurs offre plusieurs flexibilités garantissant l'implantation de différents algorithmes de détection de défauts assurant ainsi du diagnostic au sein des instruments dont les informations sont compensées. La détection de défauts basée sur l'utilisation de modèles (diagnostic) consiste en la génération d'incertitudes par la reconstruction de la sortie et sa comparaison avec la sortie mesurée et ensuite l'étape de la validation consiste en la prise de décision vis-à-vis de ce modèle pour formuler une approximation du comportement réel.

6.2.2. Validation au niveau de l'actionneur

Un actionneur permet à une variable de processus (débit, position ou force) d'être manœuvrée selon la demande d'un signal de commande u. Cet actionneur est considéré abusivement linéaire, réagissant instantanément et possédant un rendement illimité. En pratique, les actionneurs sont non linéaires, ils ont une dynamique lente et leur action est limitée. En outre, ils se détériorent dans le temps, ce qui dégrade la performance de la boucle [CLA 95].

Un exemple d'actionneurs subissant des non linéarités (collage, hystérésis) est celui des vannes de commande de débit très répandues.

L'actionneur intelligent mesure et compense ses caractéristiques indésirables, détecte et corrige des conditions de fautes et rend compte de son comportement. Les changements de la dynamique ainsi que les limites de saturation courantes peuvent être prises en considération dans un actionneur intelligent.

Un actionneur idéal reçoit une demande u_d et la transforme en commande u_a. La relation qui existent entre u_d et u_a est linéaire entre deux limites de saturation u_{min} et u_{max}. Il est commode de prendre u_{min} = 0 et u_{max} = 100% (par exemple, fermeture entière d'une vanne et son ouverture entière).

Supposons que l'actionneur est saturé. Il retourne le signal correspondant au signal réel de l'actionneur ainsi que le signal correspondant aux variables relatives au processus. Puisque u_d est contrôlée et u_a est mesurée, il est possible d'avoir une image précise de la non linéarité de l'actionneur avec l'algorithme de compensation. Le point clé est qu'il est alors possible d'inverser la non linéarité de sorte que par l'intermédiaire d'une table consultable n'importe quelle valeur u_a exigée sera sélectionnée par la valeur de u_d appropriée.

Par conséquent en employant la rétroaction interne ou en appliquant une non-linéarité inverse l'actionneur nominal approche l'idéal.

La validation dans un actionneur utilise tous les moyens à disposition pour évaluer et compenser les non linéarités internes.

[TOM 01] stipule qu'une mise en œuvre réussie de validation de l'actionneur doit être donc être capable d'observer ses propres caractéristiques et soit continuellement capable d'adapter la compensation.

Le cas des actionneurs est similaire au cas des capteurs dans l'utilisation de la méthode de génération de résidus. La reconstruction à base d'observateurs et filtres peut être utilisée, il s'agit d'un processus simulant le fonctionnement du système à partir d'un modèle mathématique où la sortie est corrigée par l'erreur d'estimation de la sortie [BAI 07]. En règle générale, les approches à base d'observateurs consistent à comparer des fonctions des sorties estimées avec les mêmes fonctions de sorties mesurées.

7. Classification de l'intelligence dans les instruments

Comme guise de synthèse, notons que la définition de l'intelligence est sujette à débat. La référence à laquelle nous pouvons donc nous y attacher est l'intelligence humaine. Nous avons dressé un bilan de l'intelligence dans l'instrumentation par la caractérisation de différents niveaux relatifs aux différentes fonctionnalités implantées dans les instruments puisqu'il existe donc plusieurs formes d'intelligence, classées sous forme de niveaux qui s'étalent du concept général de l'intelligence à des facteurs beaucoup plus spécifiques.

Nous avons caractérisé les systèmes instrumentés en quatre niveaux : le système rudimentaire, encore très répandu, le système numérique, le système basé sur un instrument dit smart et enfin le système (exploitant un processeur dédié) basé sur un instrument intelligent.

7.1. Niveau 0

Malgré les avancées technologiques dans le domaine de l'instrumentation et de la microélectronique, beaucoup de systèmes sont encore constitués rudimentairement d'un capteur (transducteur et conditionneur) qui transmet simplement une information analogique et d'un actionneur qui agit sur un processus avec un dispositif associé constituant l'ensemble de l'électronique. Selon le modèle fonctionnel générique proposé en figure 1.6, le niveau requiert les fonctionnalités mesure et actionnement.

7.2. Niveau 1

Différentes évolutions sont apparues avec une intégration plus ou moins grande via des circuits associés au capteur. Ainsi le conditionnement du signal a été mis en œuvre. L'association d'un dispositif de communication adapté a permis l'exploitation à distance des informations fournies par l'instrument. L'association d'un processeur a proximité de l'instrument a permis la numérisation du signal. A ce niveau là, on dispose d'un instrument numérique communiquant. La sûreté de fonctionnement ne va se trouver améliorée du fait de la complexité accrue par l'emploi de composants numériques intégrant du logiciel et introduisant de nouveaux modes de défaillances. Les améliorations obtenues avec ce type d'instruments s'expriment en termes de critères métrologiques (meilleure précision…) et de facilité d'utilisation. Ce niveau requiert les fonctionnalités mesure, actionnement, configuration et quelques fonctionnalités non décrites et qui se rapportent à l'amélioration de la métrologie de l'instrument.

7.3. Niveau 2

La notion d'instrument "smart", c'est à dire de système qui dispose d'une certaine capacité de calcul assurée par un circuit programmable du type microcontrôleur ou microprocesseur lui permettant de prendre en compte certaines dérives et grandeurs d'influence et donc de générer un signal corrigé que le système d'acquisition pourra alors acquérir via une interface de communication intégrée. L'existence d'un élément de calcul programmable et d'un bloc mémoire associé va permettre l'implémentation de nombreuses fonctionnalités au sein de l'instrument telles que l'existence d'autotests intégrés et autodiagnostics locaux susceptibles de déterminer automatiquement l'élément défaillant. D'autres fonctionnalités sont disponibles dans le système "smart" et se rapportent essentiellement à la configuration à distance (type et numéro d'identification de l'instrument, sa date de mise en service et ses dates prévisibles de maintenance programmée, ses caractéristiques métrologiques et de fonctionnement…). L'association de la validation à l'autodiagnostic et la décision vont permettre d'appréhender l'environnement de l'instrument localement et de pouvoir assurer la continuité du service en présence de défauts. Ce niveau requiert l'ensemble des fonctionnalités décrites dans le modèle fonctionnel générique mais leur exploitation est restreinte et n'est pas complète.

7.4. Niveau 3

L'intérêt de l'utilisation d'un instrument intelligent est la crédibilité des informations et la sûreté de fonctionnement. En effet, une information erronée peut conduire à la prise d'une mauvaise décision et mener à la défaillance du système. L'instrument doit délivrer une information validée pour permettre l'amélioration de la sûreté de fonctionnement du système. Les moyens mis en œuvre pour l'amélioration de la crédibilité et de la sûreté de

fonctionnement se rapportent aux apports de la fonctionnalité validation sous toutes ses formes. En effet, le placement de l'instrument intelligent dans un contexte système permet l'échange d'informations élaborées et la coopération entre différents nœuds du système pour permettre de prendre des décisions et d'agir sur le processus. L'instrument fait alors partie d'une architecture distribuée favorisant la communication des informations entre différents instruments. Ici à ce niveau, l'ensemble des fonctionnalités relatives au modèle générique sont implantées et exploitées permettant ainsi de tirer le maximum de profits de l'intelligence dans les instruments.

8. Conclusion

L'évolution technologique des instruments intelligents et des réseaux de communication ont permis le développement des systèmes d'automatisation à intelligence distribuée. La délocalisation du traitement au plus près des instruments constituant ces systèmes et les possibilités accrues d'échange d'information permettent de distribuer le contrôle commande.

Les instruments intelligents sont des équipements qui contiennent un certain nombre de fonctionnalités leurs permettant de communiquer, de faire des calculs, d'élaborer une mesure, de la valider en fonction d'éléments disponibles localement ou à distance, de prendre des décisions. L'instrument intelligent, en plus des fonctionnalités qui améliorent ses performances métrologiques, possède une capacité à crédibiliser sa fonction (validant la mesure produite pour le capteur ou rendant compte de la réalisation effective de l'action de l'actionneur).

L'intelligence dans les instruments intelligents porte une sémantique équivoque, un instrument intelligent est souvent considéré intelligent dès qu'il intègre un traitement numérique. La définition de l'intelligence dans un instrument intelligent n'est pas universelle. La définition de l'intelligence est donc très vaste. Nous pourrons définir l'intelligence comme la capacité d'un système à agir de façon appropriée dans un environnement donné afin de réaliser un ou plusieurs objectifs.

L'évolution du concept d'instrument intelligent est illustrée par le schéma de la figure 1.13 [GEO 05]. En effet, le traitement des informations était localisé à un niveau supérieur de la pyramide CIM qui est un niveau supérieur de décision et où la visibilité est globale. Après, il y a eu une évolution vers la distribution du traitement au niveau des automatismes pour remédier notamment aux coûts élevés des câblages et de l'installation et à la fiabilité du système altérée par la gestion de plusieurs boucles au moyen d'un calculateur central. Le dernier pas de l'évolution des systèmes d'automatisation est celui de l'incorporation d'instruments intelligents au niveau le plus bas de la pyramide CIM, c'est-à-dire le niveau terrain. Les traitements sont localisés au plus près du processus physique et toute défaillance locale d'une boucle n'est pas répercutée aux autres niveaux du système.

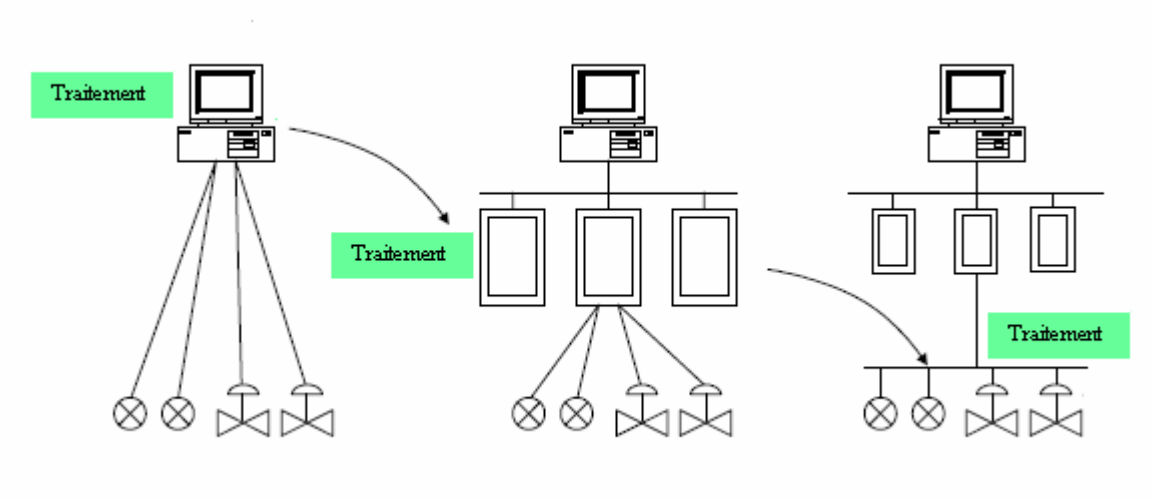


Figure 1.13 : Evolution des systèmes d'automatisation

Un des problèmes liés au développement des SAID relativement à la communication est le choix du réseau de terrain avec lequel ces constituants seront compatibles. Une fois que ce choix a été effectué, il faut mettre en place une architecture adaptée permettant l'intégration de ces fonctions. La notion d'interopérabilité entre les instruments de différents constructeurs constitue un sérieux problème et doit être considérée dès la conception. On peut noter l'exemple des systèmes classiques utilisant le standard 4-20 mA comme un exemple de norme respectant le principe d'interopérabilité puisqu'ils définissent non seulement un système de transmission mais également un formalisme de représentation des informations.

[TAO 05] propose une solution pour remédier au problème de l'interopérabilité avec la nouvelle génération de capteurs intelligents IP connectés par le protocole TCP/IP à Internet où les échanges d'informations peuvent être élaborés.

La validation dans les instruments intelligents (capteurs ou actionneurs) assure par les données transmises via le réseau de communication une bonne qualité du SAID et participe à l'augmentation des performances de sa sûreté de fonctionnement. Des données défectueuses peuvent provoquer des comportements inattendus ou la défaillance du système et donc, l'instrument intelligent doit être en mesure d'évaluer la validité de la collecte des données pour éviter tous effets désastreux de la propagation de données erronées. La validation devient plus importante lorsque les données provenant de divers instruments sont envoyés au système [CLA 00], [TIA 00]. Les objectifs de cette validation sont d'améliorer la sécurité lors de l'utilisation des instruments intelligents dans les boucles de sécurité.

Enfin, il nous est apparu nécessaire d'attribuer des niveaux d'intelligence aux instruments en fonction des fonctionnalités implantées. Il y a des degrés ou niveaux de l'intelligence, et ceux-ci sont déterminés par: la puissance de calcul du système, la sophistication des algorithmes que le système utilise pour le traitement des données, par la gestion des modèles, la génération de comportement et la coopération entre différents interlocuteurs du système.

Chapitre 2 : Systèmes Instrumentés de Sécurité

Les Systèmes Instrumentés de Sécurité

1. Introduction

Diverses sécurités sont mises en œuvre lorsque les systèmes automatisés présentent des risques pour l'homme, l'environnement ou les biens. Ces types de sécurités utilisent des moyens contribuant soit à la prévention soit à la protection pour limiter les conséquences d'un dysfonctionnement. Les systèmes instrumentés de sécurité (SIS) sont souvent utilisés comme moyens de protection pour réaliser des fonctions instrumentées de sécurité (SIF). Pour concevoir ces systèmes, deux normes sont utilisées : l'ANSI/ISA S84.01-1996 [ISA 96] et la CEI 61511 [CEI 03] qui est une déclinaison de la norme générique CEI 61508 [CEI 00].

Les systèmes instrumentés de sécurité sont utilisés pour exécuter des fonctions de sécurité dans les industries de production par processus (ou de transformation). Ce sont des moyens de sécurité chargés de surveiller que le procédé ne franchit pas certaines limites (au-delà desquelles il pourrait devenir dangereux) et d'actionner les organes de sécurité lorsqu'un tel danger se présente.

La première partie de ce chapitre porte sur la norme CEI 61508 qui est une norme générique et couvre plusieurs aspects tels que le cycle de vie, l'allocation de l'intégrité de sécurité en fonction d'un objectif, le choix de l'architecture matérielle ...

Pour être plus facilement mise en oeuvre, des normes filles sectorielles ont été imaginées : c'est le cas notamment de la norme CEI 61511, spécialement pensée pour mettre en oeuvre les systèmes instrumentés de sécurité, ou de la norme CEI 62061 qui est dédiée au secteur machine.

Les normes ANSI/ISA S84.01-1996 [ISA 96] et CEI 61511 [CEI 03] établissent les prescriptions relatives à la spécification, la conception, l'installation, l'exploitation et la maintenance du SIS, afin d'avoir toute confiance dans sa capacité à amener le procédé dans un état sûr. Les étapes de base pour se conformer à ces normes sont :

- ✓ Etablir une cible de sécurité (risque acceptable) du procédé et évaluer le risque existant.
- ✓ Identifier les fonctions de sécurité requises et les affecter aux niveaux de protection.
- ✓ Déterminer si la fonction instrumentée de sécurité est requise.

- ✓ Implémenter la fonction instrumentée de sécurité dans un SIS et déterminer le SIL du SIS.
- ✓ Vérifier que le SIS permet d'atteindre la cible de sécurité exigée au départ.

Toute la difficulté est d'estimer le risque que présente le procédé et d'évaluer la diminution du risque que doit apporter le système instrumenté de sécurité. La norme formalise une démarche :

- ✓ d'analyse de risque qui identifie ce qui doit être fait pour éviter les événements dangereux associés au procédé et
- ✓ d'évaluation de risque permettant l'obtention de l'intégrité de la sécurité exigée du système pour que le risque devienne acceptable.

Cette intégrité de sécurité se matérialise par des niveaux SIL (*Safety Integrity Level*). Ces niveaux SILs sont d'autant plus importants lorsque la réduction du risque est importante et ils doivent concerner la boucle complète du SIS. Donner un niveau de SIL pour un instrument n'a en soi pas de sens.

La dernière partie montre les limites de la norme CEI 61508 et sa situation par rapport aux systèmes d'automatisation à intelligence distribuée (SAID). En effet, certains industriels soulignent l'extrême complexité qui rend cette norme difficilement applicable et son manque de précision laissant trop de place à l'interprétation. Des chercheurs aussi avancent quelques réticences en estimant que la mise en œuvre pratique de cette norme est difficile et sujette à caution dans la mesure où les résultats obtenus dépendent de la manière dont elle est appliquée [INN 06]. De plus, la norme reste muette à propos des systèmes d'automatisation distribuée et n'aborde pas les problèmes de communication entre les différents instruments des dispositifs de sécurité ainsi que l'intelligence propre de ces instruments. Nous terminons le chapitre par une description des performances évaluables en terme de sécurité.

2. Concept de la sécurité

Les établissements industriels déploient beaucoup d'efforts pour éviter des accidents. Mais malgré cela, de nombreux accidents industriels se produisent dans le monde (SEVESO en Italie (1976), AZF à Toulouse (2001),…) causant plusieurs victimes et dégâts sur les biens et l'environnement. L'ampleur et la fréquence de ces accidents ont suscité de nombreux efforts sur des études de sécurité afin de mieux maîtriser les risques.

Dans les études de sécurité, l'étude de dangers doit mener à l'identification de sources ou situations pouvant nuire aux personnes, aux biens et à l'environnement. Cette étude de dangers doit aboutir à un ensemble de mesures de maîtrise de risques mises en œuvre à l'intérieur de l'installation à un niveau jugé acceptable par l'exploitant de l'installation.

2.1. Notion de danger

La norme CEI 61508 [CEI 00] définit le danger comme une nuisance potentielle pouvant porter atteinte aux biens (détérioration ou destruction), à l'environnement, ou aux personnes. Les dangers peuvent avoir une incidence directe sur les personnes, par blessures physiques ou des troubles de la santé, ou indirecte, au travers de dégâts subis par les biens et l'environnement.

Selon la norme OHSAS 18001 expliquée dans [GEY 05] :

- ✓ Un danger est une source ou une situation pouvant nuire par blessure ou atteinte à la santé, dommage à la propriété et à l'environnement du lieu de travail ou une combinaison de ces éléments. Les dangers liés à un système sont inhérents au fonctionnement ou au dysfonctionnement du système, soit extérieur au système (conditions naturelles difficiles, actions humaines externes…),
- ✓ Un événement dangereux est un événement susceptible de causer un dommage,
- ✓ Un dommage est une lésion physique, une atteinte à la santé ou aux biens. On parle de dommage corporel ou de dommage matériel.

Plusieurs auteurs et dictionnaires confondent le terme danger au terme risque, ce qui explique l'utilisation indifférente de ces deux termes par plusieurs personnes.

2.2. Notion de risque

Le risque donne une mesure de la combinaison de deux facteurs qui sont la gravité d'un danger (ou sa conséquence) et la fréquence d'occurrence. Sa réduction peut être obtenue par la prévention (réduction de la fréquence d'occurrence) ou la protection (réduction de la gravité).

Selon Gouriveau [GOU03], le risque peut être défini par l'association d'événements causes et conséquences d'une situation donnée. Les événements causes peuvent être caractérisés par leur occurrence (P) et les événements effets par leur impact (I).

La définition du risque se retrouve aussi dans les normes, par exemple, selon l'EN ISO 12100-1 [NF 04], c'est la combinaison de la probabilité d'un dommage et de sa gravité.

Selon la norme OHSAS 18001 expliquée dans [GEY 05] :

Un risque est la combinaison de la probabilité et de la conséquence de la survenue d'un événement dangereux spécifié.

Qualitativement, le risque se caractérise d'une part par l'ampleur des dommages, suite à l'occurrence d'un événement redouté, selon un critère de gravité le plus souvent traduit par des termes comme catastrophique, critique, marginal, mineur, insignifiant et d'autre part par son caractère incertain lié à l'apparition d'un événement redouté provoquant le dommage à partir d'une situation dangereuse déterminée.

De manière plus formelle, un risque peut être mesuré par sa criticité, qui est fonction de sa probabilité et de sa gravité :

$$c = p \times g$$

Le critère de Farmer [FAR 67] permet de définir les notions de risque acceptables et inacceptables (figure 2.1).

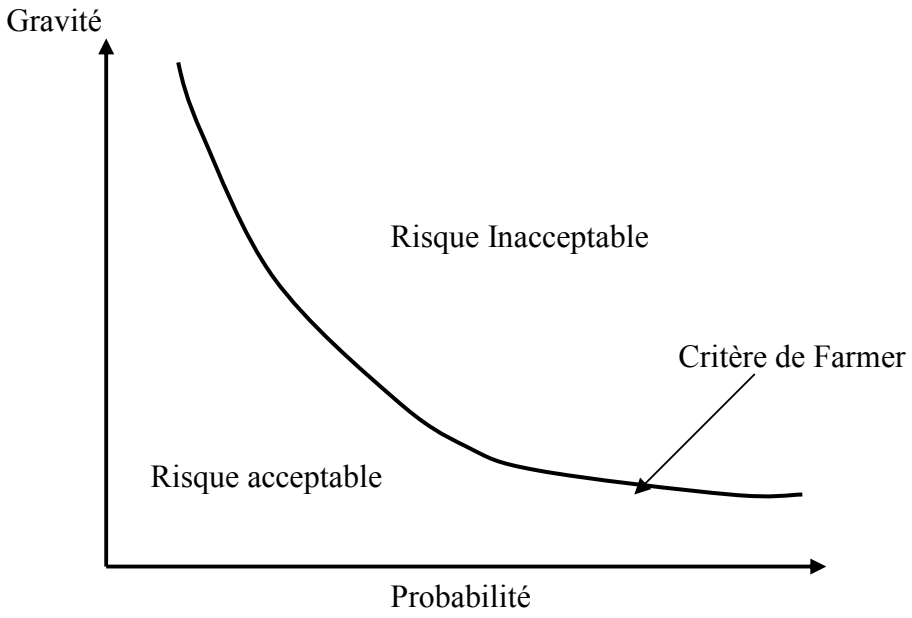


Figure 2.1 : Critère de Farmer

MAZOUNI [MAZ 07] propose une méthodologie générique qui est basée sur la connaissance préalable du concept d'accident, de ses mécanismes de causalité ainsi que son processus de matérialisation. Cette méthodologie générique permet d'exploiter efficacement l'échange du savoir-faire en matière d'APR (Analyse Préliminaire des Risques).

Cette méthodologie consiste à modéliser un processus accidentel adapté pour l'APR afin d'observer sa réalisation d'une manière spatio-temporelle. La modélisation est de type état/transition pour le processus accidentel d'APR, c'est-à-dire que l'identification des scénarios d'accident est basée sur le développement du processus accidentel en fonction de l'occurrence des différents événements. Le modèle proposé prend en compte l'implication de plusieurs Entités Cibles de Danger (**ECD**) dans un même accident avec une Entité Source de Danger (**ESD**).

La méthodologie proposée permet d'organiser des barrières de défense à chaque phase élémentaire du processus accidentel. Ainsi concernant la situation d'exposition, il convient de réduire les fréquences et les durées d'exposition tandis que l'objectif pendant la situation dangereuse serait d'éviter l'apparition de l'événement redouté et enfin durant la situation d'accident, on se contente de minimiser les préjudices pouvant être portés à l'homme, à l'environnement ainsi qu'au système et à ses interfaces.

Dans la suite de ce chapitre, les concepts d'analyse de risque et d'évaluation de risque sous-jacents à la notion de risque seront traités ainsi que les relations entre le risque et l'intégrité de sécurité.

2.3. Notion de sécurité

Nous commençons par une définition de la *sécurité*. C'est l'absence de risque inacceptable [ISO 99] [CEI 00]. Ce risque inacceptable est dû aux blessures ou atteintes à la santé des personnes, directement ou indirectement, résultant d'un dommage au matériel ou à

l'environnement. Selon [VIL 88], la sécurité est l'aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

Dans le domaine de la maîtrise des risques, la notion de sécurité concerne la sécurité innocuité [LAP 95]. La prise en compte des événements critiques tels que l'intrusion de personnes malveillants dans le domaine des systèmes informatiques est concernée par la sécurité confidentialité. [LAP 95] précise bien ces deux aspects concernant le paramètre sécurité, la sécurité innocuité (*safety*) qui est liée à la non occurrence de conséquences catastrophiques pour les personnes, les biens et l'environnement et la sécurité confidentialité (*security*) qui est liée à la non occurrence de divulgations non autorisées des informations et au respect de l'intégrité de ces informations. Dans ce mémoire, nous nous intéressons uniquement au premier aspect de la sécurité.

2.4. Sécurité fonctionnelle

La norme CEI 61508 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 basées sur une autre technologie et des dispositifs externes de réduction de risque.

La norme CEI 61511 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 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

La sécurité fonctionnelle permet 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. Normes relatives aux systèmes instrumentés de sécurité

3.1. Norme CEI 61508

En 1984, le comité technique 65 de la CEI a commencé une tâche de définition d'une nouvelle norme internationale relative à la sécurité. Cette norme CEI 61508 [CEI 00] est la seule norme multisectorielle traitant de l'ensemble de la problématique des systèmes électriques, électroniques et programmables E/E/EP, c'est-à-dire qu'elle traite à la fois le matériel et le logiciel. C'est également la seule norme très technique qui apporte des clés, auxquelles il suffit de se conformer pour atteindre un objectif. Cette norme est orientée performances en laissant à l'utilisateur le soin de réaliser son analyse de risque et elle lui propose des moyens pour réduire ce risque. Elle ne concerne pas les systèmes simples, pour lesquels le mode de défaillance de chaque élément est clairement défini et pour lesquels le comportement du système peut être totalement déterminé dans le cas d'une défaillance. Par exemple, un système comportant des fins de course et des relais électromécaniques reliés à un disjoncteur peut être étudié sans avoir recours à la CEI 61508.

La norme CEI 61508 repose sur deux concepts qui sont 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. Elle comprend 7 parties :

1. Définition des prescriptions générales qui sont applicables à tous types de matériel,
2. Prescriptions spécifiques et supplémentaires pour les systèmes E/E/PE (S. E/E/PE) - aspect matériel,
3. Prescriptions spécifiques et supplémentaires pour les S. E/E/PE - aspect logiciel,
4. Définitions et abréviations utilisées,
5. Lignes directrices pour la détermination des niveaux d'intégrité de sécurité - méthode et exemple,
6. Lignes directrices pour la mise en oeuvre des prescriptions relatives aux S. E/E/PE,
7. Présentation des techniques et des mesures.

La norme CEI 61508 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.

La figure 2.2 [SMI 04] montre la norme CEI 61508 générique et ses normes filles par secteur d'activité.

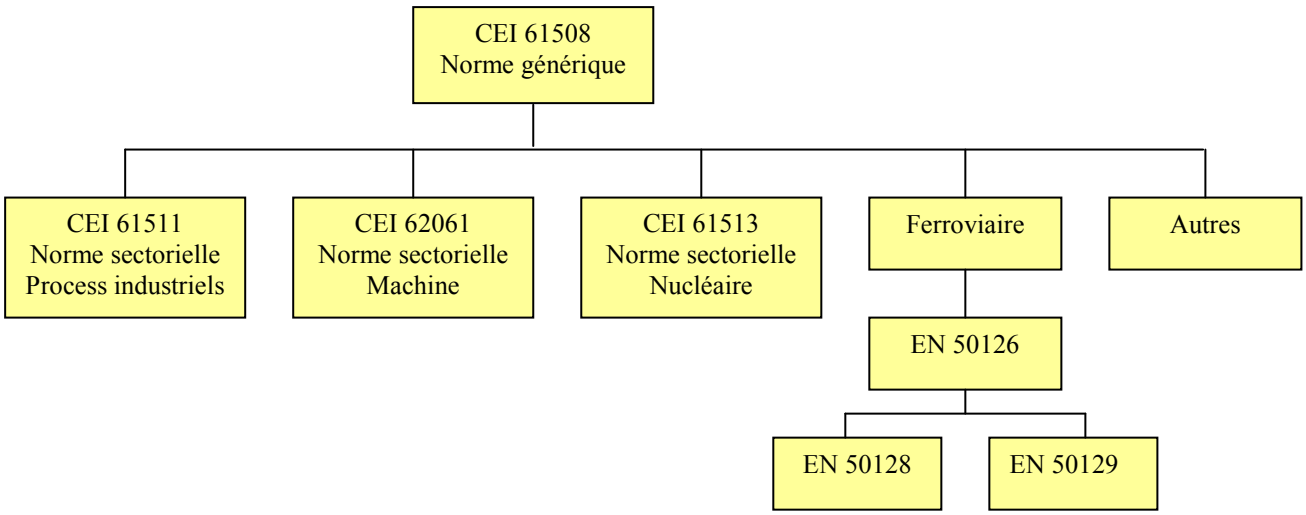


Figure 2.2 : Norme CEI 61508 et normes dérivées [SMI 04]

La norme IEC 61508 est générique. Les normes sectorielles qui en sont issues sont totalement compatibles. Ceci signifie qu'il ne faut pas penser trouver une réduction du périmètre fonctionnel ou des entorses aux principes de bases de la CEI 61508 dans ses normes filles. Les normes sectorielles ne font que préciser les modalités d'application.

Les points importants de la norme :

- ✓ Elle concerne toutes les phases du cycle de vie des matériels et du logiciel (depuis la conceptualisation, en passant par la conception, l'installation, l'exploitation, la maintenance, jusqu'à la mise hors service);

- ✓ Elle fournit une méthode de développement pour réaliser la sécurité fonctionnelle des systèmes relatifs à la sécurité;
- ✓ Elle définit des niveaux d'intégrité de sécurité (SIL) des systèmes E/E/PE relatifs à la sécurité;
- ✓ Elle décrit une approche basée sur l'analyse de risque pour déterminer les niveaux d'intégrité de sécurité (SIL) (voir § 5.2 pour les définitions des niveaux de SIL) à atteindre pour un risque donné;
- ✓ Elle fixe des objectifs quantitatifs de défaillances dangereuses des systèmes de sécurité en fonction des niveaux d'intégrité de sécurité;
- ✓ Elle décrit les principes, techniques et mesures pour la réalisation de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité, mais n'utilise pas le concept de sécurité intrinsèque, adapté à des systèmes peu complexes dont les modes de défaillances sont connus.

3.2. Norme CEI 61511

La norme sectorielle CEI 61511 concerne les systèmes instrumentés de sécurité pour le secteur les processus industriels. Cette norme comprend trois parties :

1. Cadre, définitions, exigences pour le système, le matériel et le logiciel,
2. Lignes directrices pour l'application de la CEI 61511-1,
3. Conseils pour la détermination des niveaux exigés d'intégrité de sécurité.

Cette norme établit des prescriptions relatives au cycle de vie en sécurité comprenant la spécification, la conception, l'installation, la maintenance et le démantèlement d'un système instrumenté de sécurité, afin d'avoir toute confiance dans sa capacité à amener le procédé dans un état de sécurité.

La figure 2.3 illustre la relation générale entre la CEI 61511 et sa norme mère CEI 61508 :

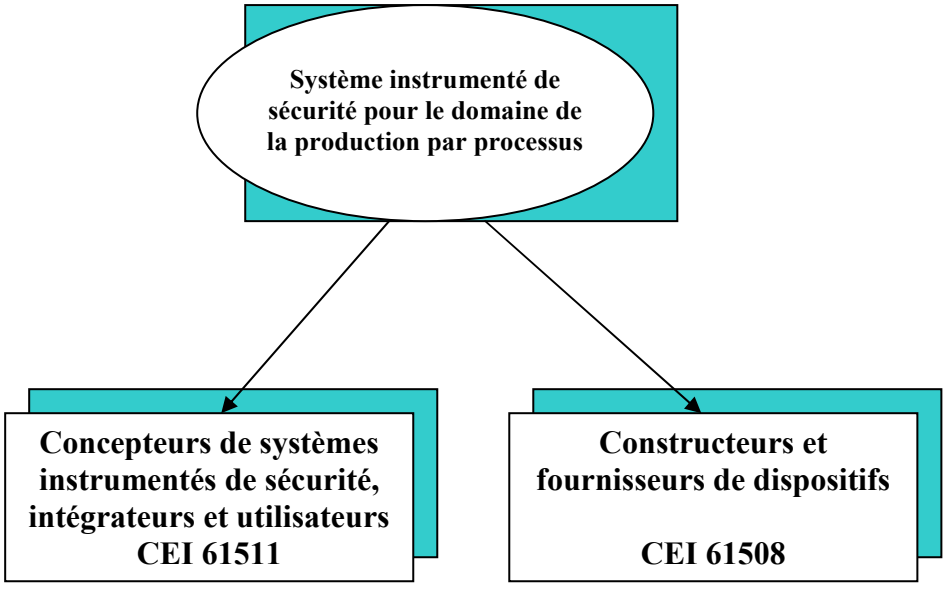
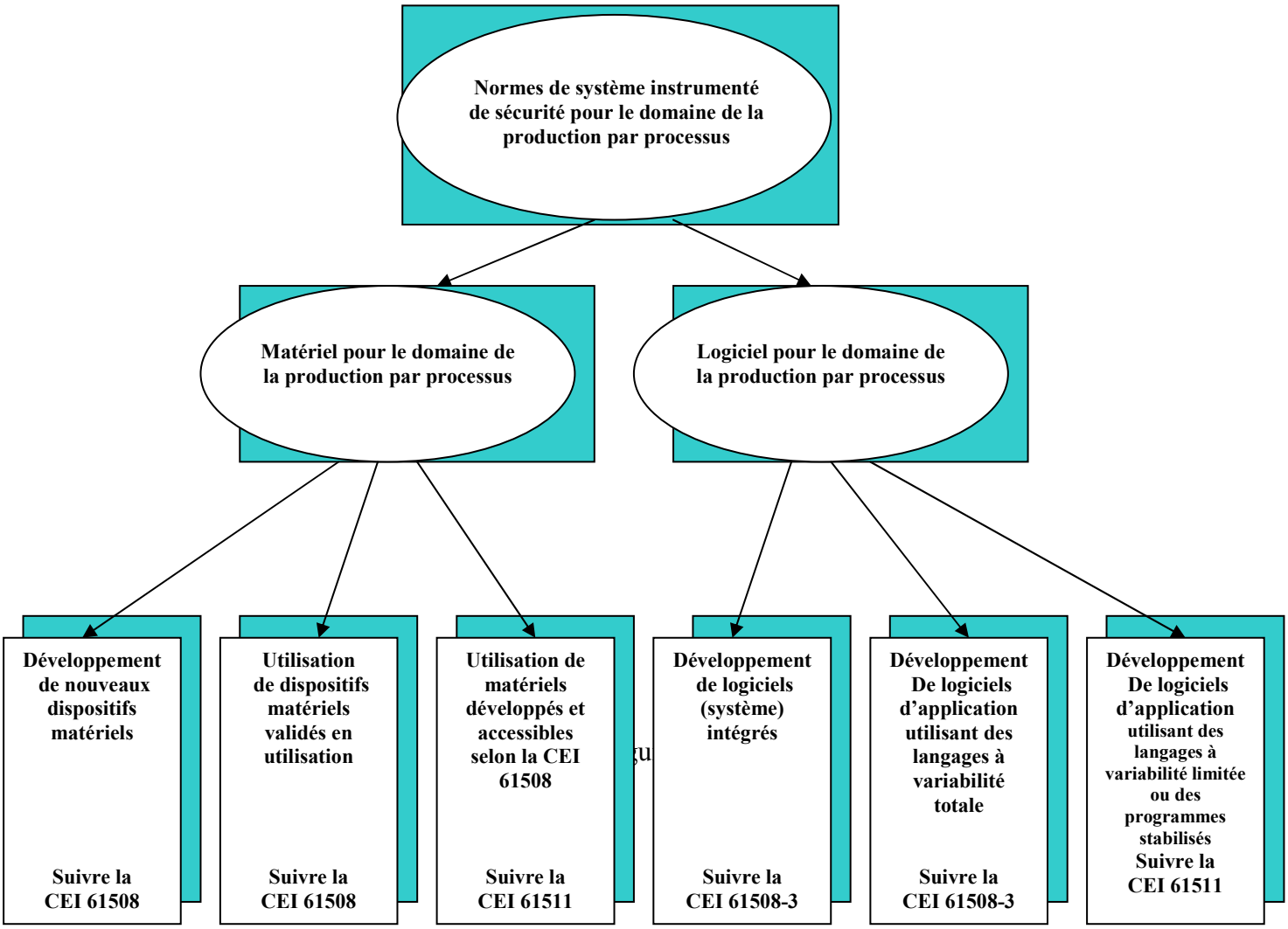


Figure 2.3 : Relation générale entre la CEI 61508 et la CEI 61511 [CEI 03]

La norme CEI 61511 restreint le périmètre aux systèmes pour des applications SIL 1 à 3 (les applications SIL 4 ne pouvant être traitées par un SIS seul). Les applications qui nécessitent l'utilisation d'une fonction instrumentée de sécurité de niveau d'intégrité de sécurité SIL 4 sont rares dans l'industrie de processus. Ces applications doivent être évitées en raison de la difficulté d'atteindre et de maintenir de tels niveaux élevés de performance tout au long du cycle de vie de sécurité [CEI 03].

La CEI 61511 a une volonté de simplification de la CEI 61508 en reprenant cette dernière mais en la limitant strictement aux éléments pertinents pour l'industrie des procédés continus. La relation entre ces deux normes pour le matériel et le logiciel est illustrée par la figure 2.4 [KOS 06] [CEI 03].



2.4 : Relation entre la norme CEI 61511 et la norme CEI 61508 pour le matériel et le logiciel [CEI 03]

Les spécifications indépendantes des secteurs se situent entre l'allocation des prescriptions de sécurité et les phases d'installation et de réception du cycle de vie de sécurité complet. Les normes sectorielles, telles que la norme CEI 61511, font habituellement référence à ces

spécifications plutôt que de les répéter. En conséquence, la plupart des utilisateurs ont systématiquement besoin de la norme CEI 61508 [RIC 05].

3.3. Norme CEI 62061

La norme CEI 62061 [CEI 05] est spécifique au secteur des machines dans le cadre de la CEI 61508. Elle est destinée à faciliter la spécification du fonctionnement des systèmes de commande électriques relatifs à la sécurité par rapport aux dangers significatifs des machines.

Cette norme internationale est destinée à être utilisée par les concepteurs de machines, les fabricants et les intégrateurs de systèmes de commande, et autres, impliqués dans la spécification, la conception et la validation de systèmes de commande électriques relatifs à la sécurité. Elle donne les exigences nécessaires à la réalisation du fonctionnement requis.

La CEI 62061 s'est limitée à l'utilisation des trois premiers niveaux d'intégrité de sécurité (SIL).

L'IEC 62061 a été rédigée dans l'objectif de devenir une norme internationale harmonisée pour la directive Machine. Ceci a été rendu possible en réduisant le périmètre de la CEI 61508 pour n'inclure que des exigences concernant des produits. La commission européenne reconnaît implicitement que l'EN 954-1 [EN 96] est notoirement insuffisante dès que les chaînes de sécurité des machines contiennent des automatismes programmés. Elle recommande (sans encore l'imposer) d'appliquer la CEI 62061 [RIC 05].

3.4. Norme ISA-84

La norme ISA-84 était acceptée par l'institut national américain des normes (American National Standards Institute, ANSI) en mars 1997. Elle spécifie les exigences pour la conception, l'installation, l'utilisation et la maintenance des systèmes instrumentés de sécurité [SUM 00a].

La norme ISA-84 dispose uniquement de trois niveaux d'intégrité de sécurité, SIL1 à SIL3. C'est une norme nationale et incomplète par rapport à la norme CEI 61511 qui est une harmonisation de normes de plusieurs pays.

En 2004, le comité d'ISA SP84 a voté pour adopter le CEI 61511 comme nouvelle version d'ISA-84 (ANSI/ISA S84.00.01- 2004) [ISA 04]. Il y a, cependant, une différence significative entre la norme ISA-84 et la norme CEI 61511. ISA-84 a ajouté une clause première génération dans la nouvelle (2004) version qui permet l'utilisation continue des systèmes instrumentés de sécurité qui suivent la version originale de la norme [ISA 96]. ISA est en cours de développement de directives et exemples d'implémentation basés sur le standard. Ceux-ci seront édités en tant que rapports techniques [ARC 05].

4. Systèmes instrumentés de sécurité et terminologies relatives

4.1. Système instrumenté de sécurité

La norme CEI 61511 [CEI 03] définit les systèmes instrumentés de sécurité de la façon suivante : *système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unités logique(s) et d'élément(s) terminal(aux)*.

La norme CEI 61508 [CEI 00] définit quand à elle les systèmes relatifs aux applications de sécurité par : *un système E/E/PE (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité*.

Les systèmes instrumentés de sécurité sont donc utilisés comme moyens de prévention et comportent une proportion grandissante de systèmes électriques, électroniques ou encore électroniques programmables (E/E/EP). Ces systèmes sont complexes ce qui rend difficile dans la pratique la connaissance de chaque mode de défaillance par l'examen des comportements possibles et la prévision des performances en terme de sécurité.

Un système instrumenté de sécurité est un système visant à mettre le procédé en 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 (explosion, feu…).

Un certain nombre de propriétés caractérisent les systèmes instrumentés de sécurité :

- Les systèmes instrumentés de sécurité nécessitent une source d'énergie extérieure pour remplir leur fonction de sécurité.
- On retrouve tout ou partie de ces différents éléments pour constituer des chaînes de sécurité.
- Plusieurs capteurs ou actionneurs peuvent être reliés à une même unité de traitement.
- Toutes les combinaisons de capteurs, d'unité de traitement et d'actionneurs qui sont exigées pour accomplir des fonctions de sécurité sont considérées comme une partie de systèmes instrumentés de sécurité.

Les capteurs, l'unité de traitement, les éléments finaux sont des équipements de sécurité et réalisent des sous-fonctions de sécurité. L'ensemble des sous-fonctions réalise la fonction de sécurité.

4.2. Fonction instrumentée de sécurité

La figure 2.5 illustre la définition d'un système instrumenté de sécurité et des fonctions instrumentées de sécurité qui sont exécutées. Cette figure illustre, entre autres, une fonction instrumentée de sécurité (SIF n°1) qui protège la température de processus et fait fermer une vanne d'isolement en cas de dérive de température de procédé vers un état dangereux. Les autres fonctions instrumentées de sécurité exécutées dans cet exemple de SIS sont la protection du niveau et la protection du débit.

Une fonction instrumentée de sécurité (SIF, *Safety Instrumented Function*) est utilisée pour décrire les fonctions de sécurité implémentées par un système instrumenté de sécurité. Une fonction instrumentée de sécurité peut être considérée comme une barrière de protection fonctionnelle lorsque le système instrumenté de sécurité est considéré comme un système réalisant cette barrière de sécurité [SKL 06].

Une fonction instrumentée de sécurité est à réaliser par un système instrumenté de sécurité (ou par une combinaison des composantes de ce système), par un système relatif à la sécurité basé sur une autre technologie ou par un dispositif externe de réduction de risque.

Une fonction instrumentée de sécurité est spécifiée pour s'assurer que les risques sont maintenus à un niveau acceptable par rapport à un événement dangereux spécifique.

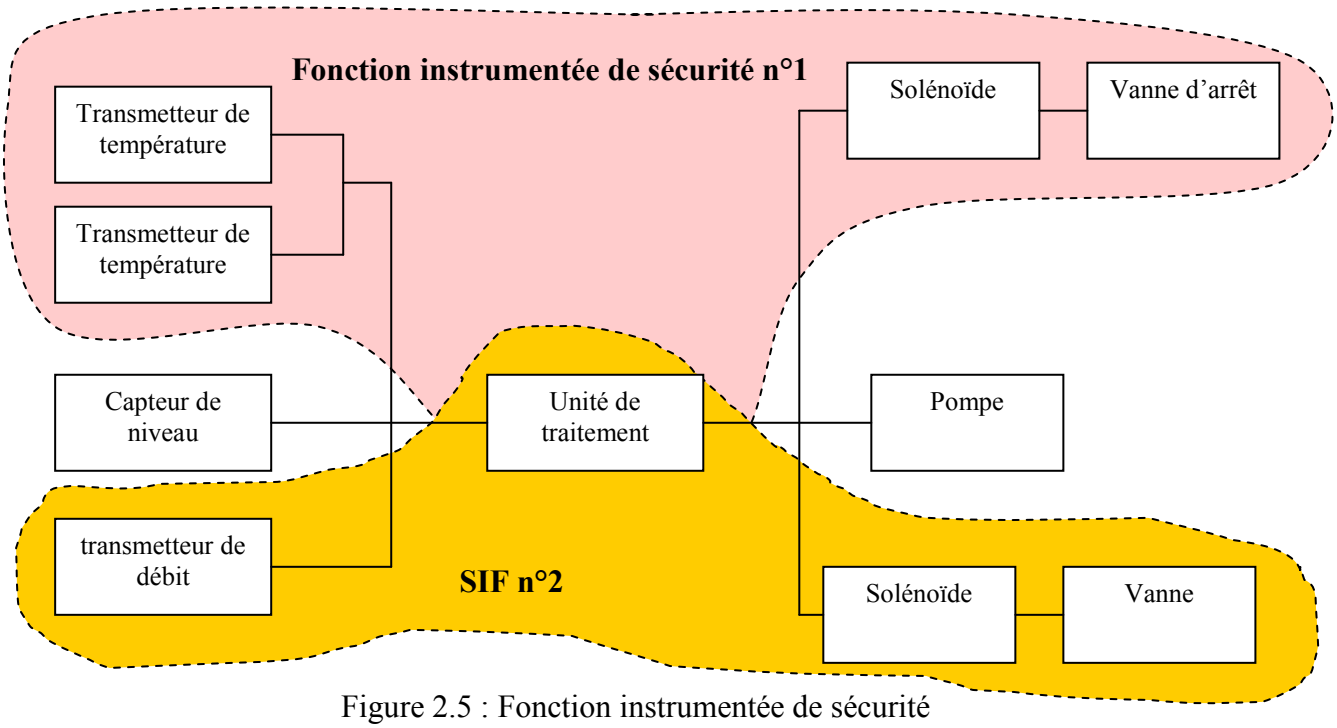


Figure 2.5 : Fonction instrumentée de sécurité

Un système instrumenté de sécurité contient habituellement plusieurs fonctions instrumentées de sécurité. Si les exigences d'intégrité de la sécurité pour ces fonctions instrumentées de sécurité diffèrent, alors les exigences applicables au niveau d'intégrité de la sécurité le plus élevé s'appliquent à l'intégralité du système instrumenté de sécurité, sauf si l'implémentation garantit une indépendance suffisante entre les fonctions de sécurité. Pour une situation donnée, plusieurs fonctions de sécurité peuvent conduire à réduire la fréquence d'occurrence du danger. Les probabilités de défaillance des différentes fonctions de sécurité ne peuvent s'additionner que si les fonctions sont indépendantes entre elles. Dans ce mémoire, nous prenons comme hypothèse que chaque SIS ne peut réaliser qu'une seule SIF.

L'architecture fonctionnelle d'un système instrumenté de sécurité qui est composée d'un ensemble de fonctions instrumentées de sécurité est constituée de trois fonctionnalités de base, la détection (ou la mesure), la décision et l'actionnement.

Les exigences de niveaux d'intégrité de sécurité sont allouées aux fonctions instrumentées de sécurité spécifiques. Pour évaluer l'intégrité de sécurité d'un point de vue matériel, il est nécessaire de faire une analyse des configurations de l'architecture matérielle supportée par la fonction instrumentée de sécurité spécifiée [LUN 06].

D'une autre façon, c'est la projection de l'architecture fonctionnelle sur l'architecture matérielle qui est un ensemble de composants interconnectés qui forme l'architecture opérationnelle [FAU 02] [CON 99].

4.3. Le système instrumenté de sécurité comme couche de protection

L'application de couches de protection multiples pour mettre le procédé en sécurité est souvent utilisée dans les industries de transformation [WIE 02]. Pour ce type d'industries, l'installation en sécurité peut être définie par une situation où tous les risques sont réduits à un risque tolérable [KNE 02]. Des critères clairs et non ambigus doivent être définis en regard des niveaux de risque tolérable. Des mesures pour la mise en sécurité du procédé doivent être

dédiées à chaque spécificité de protection. Par exemple, pour protéger une unité particulière d'une installation contre une surpression, les dispositions de sécurité doivent se rapporter à la première couche comprenant un transmetteur de pression, une unité de traitement et un actionneur et à la seconde couche de protection comportant une soupape de sécurité de surpression. Les deux couches de protection forment des systèmes relatifs à la sécurité (Safety related systems SRS). La première couche est composée par des systèmes à base de technologie E/E/EP (électrique, électronique et électronique programmable). Ce type de systèmes est appelé systèmes instrumentés de sécurité (SIS). La seconde couche désigne les SRS de type mécanique.

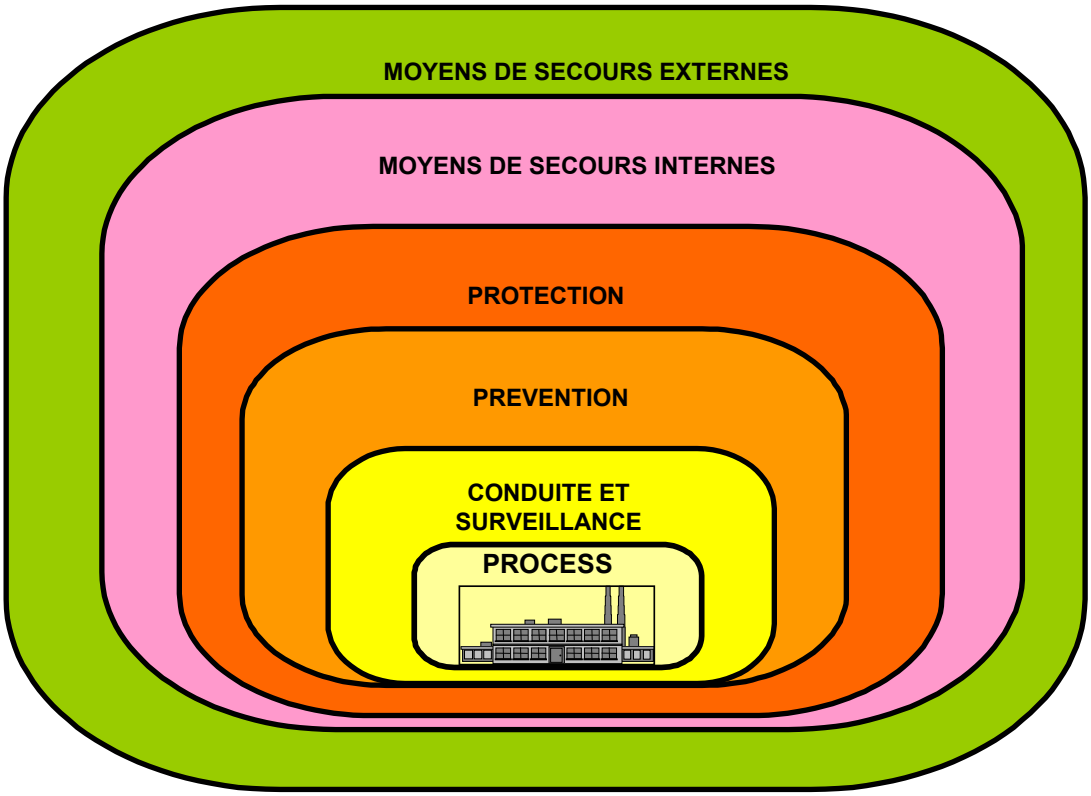


Figure 2.6 : Concept de couches de protection

La figure 2.6 montre le concept des couches de protection et la composition des différents types de systèmes relatifs à la sécurité (SRS) comme définis dans la norme CEI 68511-3. Il est à noter qu'il existe une distinction claire entre les BPCS et les SIS comme composantes des couches de protection. L'objectif primaire d'un BPCS est d'optimiser les conditions de conduite de procédé afin de maximiser la qualité et la production. Les systèmes instrumentés de sécurité s'appliquent pour prévenir des situations dangereuses (prévention) et réduire les conséquences d'événements dangereux (protection). La distinction est motivée par le fait que le BPCS n'est nécessairement pas utilisé pour contribuer à la réduction de risque et parfois il est lui-même source de risques potentiels.

Les méthodes de réduction sont de différents types et concernent tout d'abord le procédé dont la conception doit être plus au moins sûre. La conduite et la surveillance sont assurées par les systèmes de commande de procédés de base (BPCS), les systèmes de surveillance (alarmes du procédé) et par la surveillance des opérateurs.

La partie prévention des couches de protection est assurée par les dispositifs de sécurité mécaniques, par les alarmes suivies d'action et par les systèmes instrumentés de sécurité de prévention. La protection est assurée par des dispositifs de sécurité mécaniques, la supervision par l'opérateur et par les systèmes instrumentés de sécurité d'atténuation [KNE 02]. Les moyens de secours internes et externes concernent respectivement les procédures d'évacuation lors de l'occurrence d'une situation critique ainsi que la réaction du public après une radiodiffusion d'urgence.

Il faut noter qu'il existe un amalgame à propos de l'emplacement des systèmes instrumentés de sécurité comme couche de protection. Certains auteurs qualifient la couche allouée à ce type de systèmes comme une couche de prévention [KNE 02] (la norme aussi d'ailleurs) [CEI 03] alors que ce type de systèmes est voué uniquement à la protection par la réduction du risque nécessaire de telle sorte que ce risque devienne tolérable.

Il faut aussi différencier le BPCS qui est le système de commande de base du processus et le SIS qui est le système instrumenté de sécurité. En effet, le BPCS est aussi composé de capteurs, de régulateurs et d'éléments finaux. Bien que les architectures apparaissent similaires, les fonctions diffèrent beaucoup entre le BPCS et le SIS [GOB 05]. La fonction primaire d'une boucle de régulation est généralement de maintenir une variable de processus dans des limites prescrites. Le SIS surveille une variable de processus et ordonne l'action lorsque c'est exigé.

Les SIS sont rarement activés et durant les opérations normales du processus, ils demeurent statiques, dormants. La période moyenne entre l'occurrence d'événements dangereux est souvent estimée à plus d'une dizaine d'années [GOB 05]. Avec le BPCS, les signaux de commande sont normalement dynamiques. Les modes de défaillances diffèrent aussi entre un BPCS et un SIS.

Pour éviter qu'une cause unique ou *cause commune* affecte simultanément les fonctions de contrôle (BPCS) et de sécurité (SIS), la norme IEC 61508 recommande [SMI 04]:

- ✓ pour les fonctions à faible criticité (SIL1 à 2) : la distinction des fonctions de pilotage et de sécurité notamment du point de vue logiciel. A ce niveau, la norme autorise l'utilisation d'équipements (matériels) communs qui assurent simultanément des fonctions de pilotage et de sécurité, ils sont alors considérés comme des SRS et doivent êtres conçus comme tels, notamment du point de vue du SIL.
- ✓ pour les fonctions à criticité moyenne (SIL2 à 3) : distinction de la circuiterie, (électrique, ou autre : pneumatique par exemple), des capteurs et actionneurs.
- ✓ pour les fonctions à haute criticité (SIL4) : séparation intégrale physique, électrique et, dans la mesure du possible, géographique des systèmes.

4.4. Problèmes typiques des systèmes instrumentés de sécurité

Une étude réalisée par [HSE 95] a illustré l'origine d'un nombre de défaillances de systèmes conduisant à des événements dangereux très sérieux.

Les défaillances des systèmes ne sont pas tout simplement dues à des opérations incorrectes. En effet, les défaillances concernent les différentes étapes de la durée de vie d'un système (cf figure 2.7).

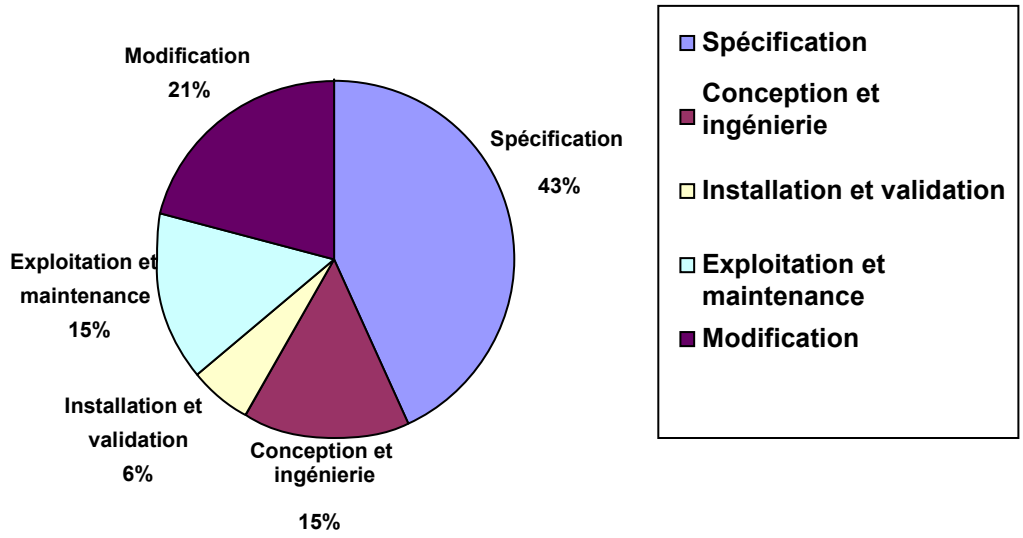


Figure 2.7 : Causes primaires des défaillances des systèmes de commande [HSE 95]

Shell [SHE 98] a réalisé une autre étude illustrative à l'usine nationale de GNL en Oman au Moyen-Orient. Le procédé de production complet a été composé des systèmes de rétablissement de champ, d'une installation de transformation centrale, et d'un complexe de liquéfaction. Pendant une étude de sécurité basée sur l'intégrité de sécurité SIL, la conclusion est que :

- ✓ 67% des fonctions instrumentées de sécurité (SIF) semblent sur-calibrées en terme de SIL,
- ✓ 27% n'exigent aucun changement. Elles sont correctement calibrées,
- ✓ 6% des SIF semblent sous-calibrées.

Shell a réalisé un certain nombre de ces études sur différents sites qui ont présenté des résultats comparables.

Les fautes pourraient avoir été produites pendant l'évaluation des risques et la spécification des conditions de sécurité ; des défaillances pourraient également avoir été faites pendant la conception et l'exécution du SIS, ou pendant la validation. Généralement après avoir passé en revue les deux études précédentes, la conclusion tirée est que les défaillances pourraient se produire à différentes étapes du cycle de vie.

Dans les deux sections suivantes, nous allons nous intéresser aux concepts sous-jacents à la notion de risque (définie au §2.2) et les relations entre le risque et l'intégrité de sécurité. Ces concepts se rapportent à l'analyse de risque et à l'évaluation de risque.

5. Analyse de risque du procédé

La détermination du SIL requis pour un système est étroitement liée à la notion de risque. Plusieurs facteurs influent sur le niveau d'intégrité comme par exemple la gravité des blessures, le nombre de personnes exposées au risque, la fréquence à laquelle une ou des personnes sont exposées au danger et la durée de cette exposition. L'analyse de risque s'avère indispensable pour contribuer à déterminer le risque tolérable dans une situation spécifique.

L'analyse de risque comporte le développement d'une évaluation de combinaisons de risques par la collecte et l'intégration des informations relatives aux scénarios des fréquences et des conséquences. C'est une composante majeure du management de risques dans une entreprise [WAN 04].

Une analyse de dangers et de risques doit être réalisée dès la conception pour le procédé et ses équipements associés par exemple le BPCS (système de commande du procédé "Basic Process Control System"). Cette analyse se rapporte à la description de ces événements dangereux et des facteurs y contribuant, à la description des conséquences de ces événements, à la détermination des exigences pour la réduction de ce risque, à l'affectation de fonction de sécurité aux couches de protection, etc.

Cette analyse de risques se veut être un instrument de prévention et de protection et se manifeste sous forme de méthodes comportant des phases d'identification, d'évaluation et de hiérarchisation [TIX 02].

5.1. Réduction du risque nécessaire

La réduction de risque nécessaire est celle qui doit être obtenue pour l'atteinte du risque tolérable d'une situation dangereuse. Le but de la détermination du risque tolérable d'un événement dangereux est d'indiquer ce qui est raisonnable par rapport à la fréquence de l'événement dangereux et ses conséquences.

Lorsqu'un risque est qualifié d'inacceptable, on utilise dans ce cas des moyens de prévention pour diminuer la probabilité de l'événement redouté ou des moyens de protection pour diminuer la gravité de cet événement redouté. Une combinaison des deux est possible offrant la possibilité de franchir la zone où le risque est inacceptable vers la zone d'acceptabilité.

La prévention des accidents se rapporte à l'élimination de dangers ou sur la diminution de l'occurrence d'événements redoutés par l'amélioration de la sécurité des dispositifs de contrôle ou par l'implantation des moyens empêchant l'apparition ou la propagation des dangers (SIS…).

La protection vient après l'échec des moyens de prévention et se rapporte à l'atténuation des conséquences d'un accident par des moyens limitant les dommages (systèmes de secours, procédures d'urgence).

La figure 2.8 illustre le concept de réduction de risque à un niveau tolérable. Les niveaux de protection sont conçus pour réduire la fréquence de l'événement dangereux et ses conséquences.

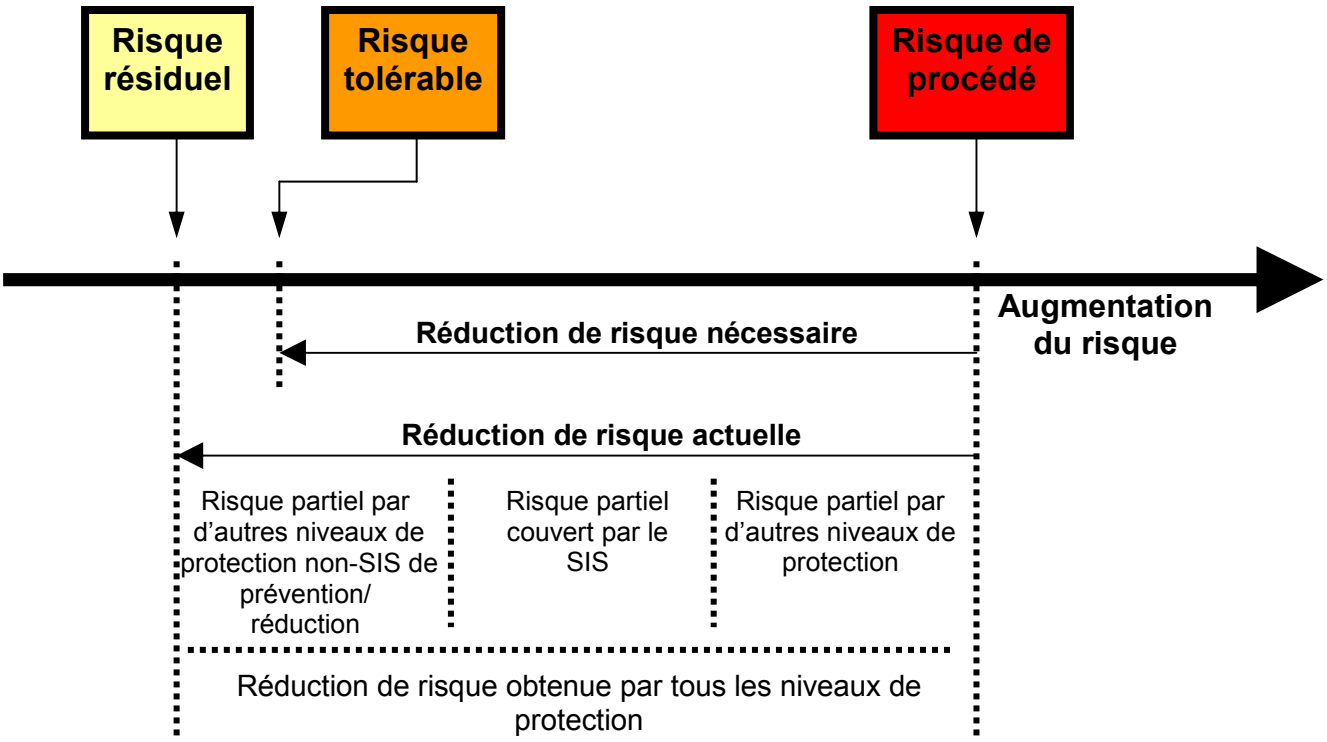


Figure 2.8 : Réduction de risque – concepts généraux

La réduction du risque nécessaire peut être obtenue en combinant un ou plusieurs systèmes instrumentés de sécurité (SIS) ou d'autres niveaux de protection. Une personne peut faire partie intégrante d'une fonction de sécurité. Par exemple elle peut recevoir des informations sur l'état du procédé, et exécuter une action de sécurité en fonction de ces informations. Si une personne fait partie d'une fonction de sécurité, il convient alors de prendre en compte les facteurs humains.

6. Evaluation du risque et détermination du niveau d'intégrité de sécurité

Dans cette section, l'évaluation du risque qui est liée à l'intégrité de sécurité est traitée par la proposition d'une approche particulière préconisée par la norme permettant de parvenir à un risque tolérable.

6.1. Risque tolérable et concept ALARP

6.1.1. Concept ALARP

Le principe ALARP [CEI 00] (***A**s **L**ow **A**s **R**easonably **P**racticable, aussi bas que raisonnablement possible*) appliqué au Royaume-Uni (figure 2.10) intègre une zone pour un risque inacceptable, une zone d'acceptation de risque et une zone ALARP dans laquelle les objectifs globaux de sécurité sont fixés. Si le risque analysé se trouve dans cette zone, les moyens mis en œuvre pour atteindre le niveau de sécurité désiré doivent être évalués ainsi que la réduction du risque qu'ils apportent.

La notion de raisonnable considère en particulier le coût lié à la réduction de risque et le ratio gains obtenus / niveau d'investissement.

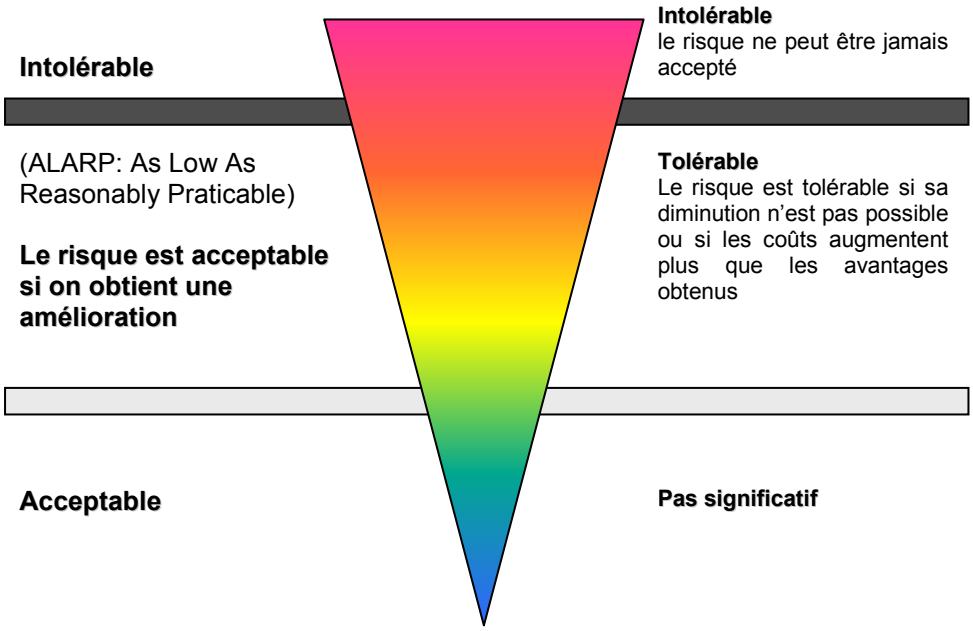


Figure 2.9 : Risque tolérable et ALARP

La figure 2.9 illustre le principe ALARP. Elle fait apparaître trois zones, une zone d'acceptation du risque, une zone de rejet de risque et une zone appelée zone ALARP dans laquelle les objectifs de sécurité sont fixés. Les zones sont délimitées par des fréquences (par heure) de risques données. A titre d'exemple, la zone ALARP peut être délimitée par l'intervalle [$10^{-9}10^{-6}$] [CEN 00]. Si le risque analysé se trouve dans cette zone, les moyens à mettre en œuvre pour atteindre le niveau d'intégrité de sécurité désiré doivent être évalués ainsi que la réduction du risque qu'ils apportent.

D'autres principes d'acceptation de risques existent tels que le principe allemand MEM et le principe français GAME [CEN 00].

Le principe MEM (*Mortalité Endogène Minimale*) fixe les objectifs globaux de sécurité par référence à la mortalité endogène minimale d'un individu, c'est-à-dire le risque ambiant pour une personne âgée de 5 à 15 ans (fixé à 2.10^{-4}/an). Les risques liés aux systèmes techniques sont considérés comme contribuant à 5% du risque individuel.

Le principe français GAME (*Globalement Au moins Equivalent*) impose pour un nouveau système le respect des mêmes exigences de sécurité qu'atteint un système équivalent existant. Ce principe nécessite de connaître les objectifs de sécurité et le comportement relatif à la sécurité du système de référence.

6.1.2. Estimation du risque tolérable

Les risques identifiés doivent être estimés en gravité et en probabilité.

La détermination de la gravité se rapporte à l'évaluation des conséquences à partir de l'intensité des effets, et de la vulnérabilité du voisinage.

La détermination de la probabilité se fait à partir des éléments fournis par diverses bases de données par combinaison des probabilités des évènements causals, des situations circonstancielles,…

Afin d'appliquer le principe ALARP il est nécessaire de définir trois régions relatives à la probabilité et la conséquence d'un incident. Pour tenir compte du concept ALARP, l'adaptation d'une conséquence avec une fréquence tolérable peut être faite par des classes de risque. Le Tableau 2.1 est un exemple montrant trois classes de risque (I, II, III) pour un certain nombre de conséquences et de fréquences. Le Tableau 2.2 interprète chacune des classes de risque employant le concept ALARP. Les descriptions pour chacune des quatre classes de risques sont basées sur la figure 2.11. Ces classes de risques sont les suivantes :

- ✓ Classe de risque I : risque intolérable
- ✓ Classe de risque II et III : ces classes sont situées dans la zone ALARP,
- ✓ Classe de risque IV : cette classe est la zone d'acceptabilité.

Probabilité	**Classes de risque**			
	Conséquence catastrophique	Conséquence critique	Conséquence marginale	Conséquence negligeable
Fréquent	I	I	I	II
Probable	I	I	II	III
Ocasionnel	I	II	III	III
Peu fréquent	II	III	III	IV
Improbable	III	III	IV	IV
Non crédible	IV	IV	IV	IV

Tableau 2.1: Exemple de classification de risques [CEI 00]

L'appréciation du risque est une fonction de la gravité et de la fréquence. Il est souvent difficile d'apprécier l'un ou les deux et encore plus la combinaison des deux. Dans une démarche d'analyse du risque, il faut prendre acte de cette difficulté. L'essentiel est de pouvoir au moins classer les risques entre eux, selon une échelle que l'on s'est donnée. Le point important est alors la calibration initiale de cette échelle.

C'est l'objet des méthodes de classement du risque. L'intérêt est de pouvoir comparer les risques et de leur affecter la bonne réponse.

Risk class	Interpretation
Classe I	Risque intolerable
Classe II	Risque indésirable, tolérable uniquement s'il est possible de réduire le risque ou si le coût de la réduction est disproportionné par rapport à l'amélioration possible
Classe III	Risque tolérable si le coût de la réduction de risque est supérieur à l'amélioration apportée
Classe IV	Risque négligeable

Tableau 2.2 : Interprétation des classes de risques

6.2. Niveaux d'intégrité de sécurité

Les normes CEI 61508 et CEI 61511 définissent le niveau d'intégrité de sécurité (Safety Integrity Level : SIL) pour définir le niveau de réduction du risque, c'est-à-dire le niveau d'intégrité de sécurité que doit avoir le système de protection. Plus le SIL à une valeur élevée, plus la réduction du risque est importante. Par exemple un système de SIL 4 apporte une réduction de risque entre 10000 à 100000 alors qu'un système de SIL 1 comporte un facteur de réduction de risque compris entre 10 à 100 seulement.

Les SILs se caractérisent par des indicateurs discrets positionnés sur une échelle à quatre niveaux. Le SIL 4 désigne le degré de sécurité le plus élevé du fait de l'exigence forte de sécurité imposée et le SIL 1 désigne l'exigence la plus faible. Les SILs sont employés pour spécifier les exigences de sécurité des fonctions de sécurité réalisée par des systèmes E/E/EP relatifs à la sécurité selon la norme CEI 61508 [CEI 00] ou des fonctions instrumentées de sécurité selon la norme CEI 61511 [CEI 03]. L'utilisation des niveaux SILs permet de prendre en compte les défaillances rares mais possibles des systèmes de sécurité en plus des défaillances inhérentes au système opérationnel menant aux événements dangereux identifiés pendant l'analyse de risque [BEU 06]. Les SILs sont attribués aux fonctions de sécurité sur la base de l'étude des défaillances dangereuses de caractère systématique ou de caractère aléatoire.

Les défaillances systématiques sont reliées de façon déterministe à une cause [CEI 03]. Ce sont des défaillances latentes qui se révèlent durant la phase d'exploitation du système opérant sous certaines conditions. Les erreurs de conception et les défauts logiciels ainsi que certaines défaillances matérielles liées à l'environnement se rapportent à ces défaillances systématiques. Ces défaillances ne peuvent être éliminées que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés. Elles ne sont pas quantifiables à cause de leurs causes difficilement prévisibles.

Les défaillances aléatoires concernent les défaillances du matériel. Elles surviennent de manière aléatoire et résultent de divers mécanismes de dégradation au sein du matériel [CEI 03]. La norme indique que ces défaillances sont quantifiables. Les mécanismes de dégradation se produisent à des probabilités différentes dans divers composants et les défaillances surviennent à des probabilités prévisibles mais à des instants imprévisibles (cas aléatoires).

L'une des différences majeures entre les défaillances aléatoires du matériel et les défaillances systématiques est que les taux de défaillances du système, engendrés par les défaillances aléatoires du matériel peuvent être prédits alors que les défaillances systématiques ne peuvent pas être prédites. C'est-à-dire que les taux de défaillance du système issus des défaillances de matériel peuvent être quantifiés contrairement à ceux issus des défaillances systématiques qui ne peuvent pas être prédits de manière statistique du fait que les événements conduisant à ce type de défaillances ne peuvent pas être facilement prédits.

La norme IEC s'applique aussi bien aux systèmes de sécurité qui fonctionnent sur sollicitation (lorsqu'une défaillance apparaît) que ceux qui travaillent en permanence pour maintenir un procédé dans un état non dangereux. Le premier cas (système sur sollicitation) peut être illustré par un système d'arrêt d'urgence qui va commander l'ouverture d'une vanne de sécurité si la pression dans un ballon devient trop élevée. Le deuxième cas (fonctionnement permanent) peut être illustré par le contrôle de la vitesse d'une machine à papier, qui doit être maintenu à une vitesse très lente pendant que les opérateurs sont en train de réaliser une opération de maintenance [MES 05].

Le mode de fonctionnement à faible sollicitation est considéré lorsque la fréquence de demande n'est pas plus grande qu'une par an et est au plus égale à deux fois la fréquence des tests périodiques [CEI 00]. Ce mode est généralement attribué aux systèmes de protection, activité lors de l'occurrence d'un événement redouté. 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 PFD_{avg} (*Average Probability of Failure on Demand*) est évaluée sur un intervalle [0, t].

Le mode de fonctionnement continu ou à forte sollicitation implique une forte demande du système instrumenté de sécurité. Il est considéré lorsque la fréquence de demande est élevée ou continue, c'est-à-dire qu'elle plus grande qu'une par an ou supérieure à deux fois la fréquence des tests périodiques [CEI 00]. Ce mode est généralement attribué aux systèmes de prévention d'événements redoutés. A partir de l'architecture du système instrumenté de sécurité réalisant la fonction instrumentée de sécurité fortement sollicitée, la probabilité de défaillance dangereuse par heure PFH (Probability of a dangerous Failure per Hour) est évaluée sur un intervalle de temps [0, t].

Pour chaque fonction instrumentée de sécurité fonctionnant en mode de sollicitation respectivement en mode continu, le SIL requis doit être spécifié en accord avec le tableau 2.3 respectivement le tableau 2.4 [CEI 03].

FONCTIONNEMENT A LA SOLLICITATION		
Niveau d'intégrité de sécurité (SIL)	**Probabilité moyenne de défaillance à la sollicitation (PFD_{avg})**	**Réduction de risque cible (RR)**
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	$100\,000 \leq RR < 10\,000$
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	$10\,000 \leq RR < 1\,000$
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	$1\,000 \leq RR < 100$
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	$100 \leq RR < 10$

Table 2.3 : Niveaux d'intégrité de sécurité : Probabilité de défaillances lors d'une sollicitation

FONCTIONNEMENT A MODE CONTINU	
Niveau d'intégrité de sécurité (SIL)	**Probabilité de défaillance dangereuse par heure**
4	$10^{-9} \leq PFD_{avg} < 10^{-8}$
3	$10^{-8} \leq PFD_{avg} < 10^{-7}$
2	$10^{-7} \leq PFD_{avg} < 10^{-6}$
1	$10^{-6} \leq PFD_{avg} < 10^{-5}$

Table 2.4 : Niveaux d'intégrité de sécurité : Probabilité de défaillances dangereuses de la SIF

Il est à noter que le concept de SIL s'applique au système instrumenté de sécurité (SIS) dans son intégralité et pas à un sous-ensemble (par exemple un capteur).

Dans ces deux tableaux, les fonctions instrumentées de sécurités ainsi que les systèmes instrumentés de sécurité sont différenciés selon le mode de fonctionnement par l'utilisation des paramètres PFD_{avg} et PFH. Chaque SIL est délimité par une borne maximale et une borne minimale.

6.3. Allocation des SILs aux fonctions instrumentées de sécurité

Les méthodes quantitatives et qualitatives d'allocation des niveaux d'intégrité de sécurité à un système instrumenté de sécurité ou à une fonction instrumentée de sécurité examinent les différents dangers provenant du système opérationnel sans la prise en compte de dispositifs de sécurité. Elles élaborent ensuite le SIL de la fonction instrumentée de sécurité qui doit être implantée pour réduire la criticité du danger analysé.

L'objectif global est de décrire une procédure d'identification des fonctions instrumentées de sécurité requises, d'établir leur niveau d'intégrité de sécurité et de les mettre en œuvre dans un système instrumenté de sécurité afin d'obtenir la cible de sécurité voulue pour le procédé.

Les différentes méthodes listées ci-dessous font appel à une appréciation plus ou moins objective de la fréquence et de la gravité. Elles ont néanmoins toutes en commun d'assurer la cohérence du classement des risques.

6.3.1. Les méthodes quantitatives

La méthode de la matrice de risques spécifie une zone d'acceptation du risque dans un tableau de criticité (cf. tableau 2.1), cette matrice permet l'analyse d'un événement dangereux compte tenu de sa fréquence d'occurrence et de la gravité de ses conséquences.

A l'aide du tableau de criticité, le risque R_{np} (la notation *np* désignant *not protected*, est reprise de la norme CEI 61508) est évalué selon la combinaison du niveau de gravité G de l'événement dangereux avec la fréquence F_{np} liée à la demande de la fonction de sécurité empêchant la situation dangereuse. La réduction relative du risque est évaluée par la relation [KOS 06] :

$$PFD_{avg} = F_t / F_{np} = R_t / R_{np}$$

Où F_t est la fréquence cible (spécifiée pour le niveau du risque tolérable) et R_t est le risque tolérable.

La détermination du niveau d'intégrité de sécurité dépend de la réduction de risque nécessaire pour atteindre le risque tolérable. Dans le contexte de prévention du risque, la fonction instrumentée de sécurité diminue la fréquence d'occurrence de l'événement dangereux pour réduire le risque. Dans ce cas elle doit, au minimum, ramener la fréquence F_{np} à F_t (fréquence de risque tolérable).

La relation précédente peut s'écrire donc :

$$PFD_{avg} \leq F_t / F_{np}$$

Les étapes nécessaires pour l'obtention du niveau d'intégrité de sécurité sont les suivantes [KOS 06] :

- ✓ La détermination de la fréquence F_{np} (relative au procédé sans addition de mesures de protection),
- ✓ La détermination de la conséquence (N) sans addition des mesures de protection. La conséquence N est donnée par la relation : $R_{np}.F_{np} = N$,
- ✓ La détermination par l'utilisation de la matrice de risques (tableau 2.1) si le risque tolérable est atteint pour la fréquence F_{np} et la conséquence N. Si ceci mène à la classe de risque I, alors la réduction de risque est exigée. La classe de risque IV concerne le risque tolérable. Les classes de risque II et III exigeraient d'avantage de recherche (utilisation du concept ALARP),
- ✓ La détermination de la probabilité de défaillance sur demande PFD_{avg} pour le système instrumenté de sécurité pour atteindre la réduction du risque nécessaire pour la conséquence donnée de la situation considérée,
- ✓ Pour l'évaluation de la PFD_{avg}, le niveau d'intégrité de sécurité peut être déterminé à partir du tableau 2.3. Par exemple si $10^{-3} < PFD_{avg} < 10^{-2}$ alors le niveau d'intégrité de sécurité est SIL2.

D'autres méthodes qualitatives reposant sur le jugement d'expert sont utilisées. Dans ces méthodes, la réduction du risque se révèle implicite.

6.3.2. Les méthodes qualitatives

6.3.2.1. Graphe de risque

Il s'agit d'une méthode qualitative qui permet de déterminer le niveau d'intégrité de sécurité d'une fonction instrumentée de sécurité à partir de la connaissance des risques associés au procédé et au système de conduite de procédé de base.

Le risque est défini comme étant une combinaison de la probabilité d'occurrence d'un dommage et de la gravité de ce dommage. En général, dans le secteur des process continus, le risque est une fonction des quatre paramètres suivants [FAE 00] :

Paramètre		Description
Conséquence	**C**	Nombre d'accidents mortels et/ou de blessures graves pouvant résulter de l'occurrence de l'événement dangereux. Déterminé en calculant les nombres d'accidents dans la zone exposée lorsque celle-ci est occupée en tenant compte de la vulnérabilité à l'événement dangereux.
Occupation	**F**	Probabilité que la zone exposée soit occupée. Déterminée en calculant la fraction de temps d'occupation de la zone. Il convient de prendre en compte la possibilité d'une probabilité accrue de personnes se trouvant dans la zone exposée afin de rechercher les situations anormales pouvant exister lors de la progression vers l'événement dangereux.
Probabilité d'éviter le phénomène dangereux	**P**	Probabilité que des personnes exposées peuvent éviter la situation de phénomène dangereux qui existe si la fonction instrumentée de sécurité échoue à la sollicitation. Dépend s'il existe des méthodes indépendantes d'alerte des personnes exposées au phénomène dangereux et s'il existe des moyens pour y échapper.
Taux de demande	**W**	Nombre de fois par an que l'événement dangereux se produit si aucun système instrumenté de sécurité n'a été adapté. Peut être déterminé en considérant toutes les défaillances pouvant générer l'événement dangereux et en estimant le taux global d'occurrence.

Tableau 2.5 : Paramètres de risques relatifs au danger

L'affectation de valeurs numériques aux paramètres du tableau 2.5 constitue la base de l'évaluation du risque de procédé qui existe en l'absence de la fonction instrumentée de sécurité concernée.

Le graphe ou diagramme de risque (figure 2.10) associe des combinaisons particulières des paramètres de risque aux niveaux d'intégrité de sécurité. La relation entre les combinaisons des paramètres de risque et les niveaux d'intégrité de sécurité est établie en prenant en compte le risque tolérable associé à des phénomènes dangereux spécifiques.

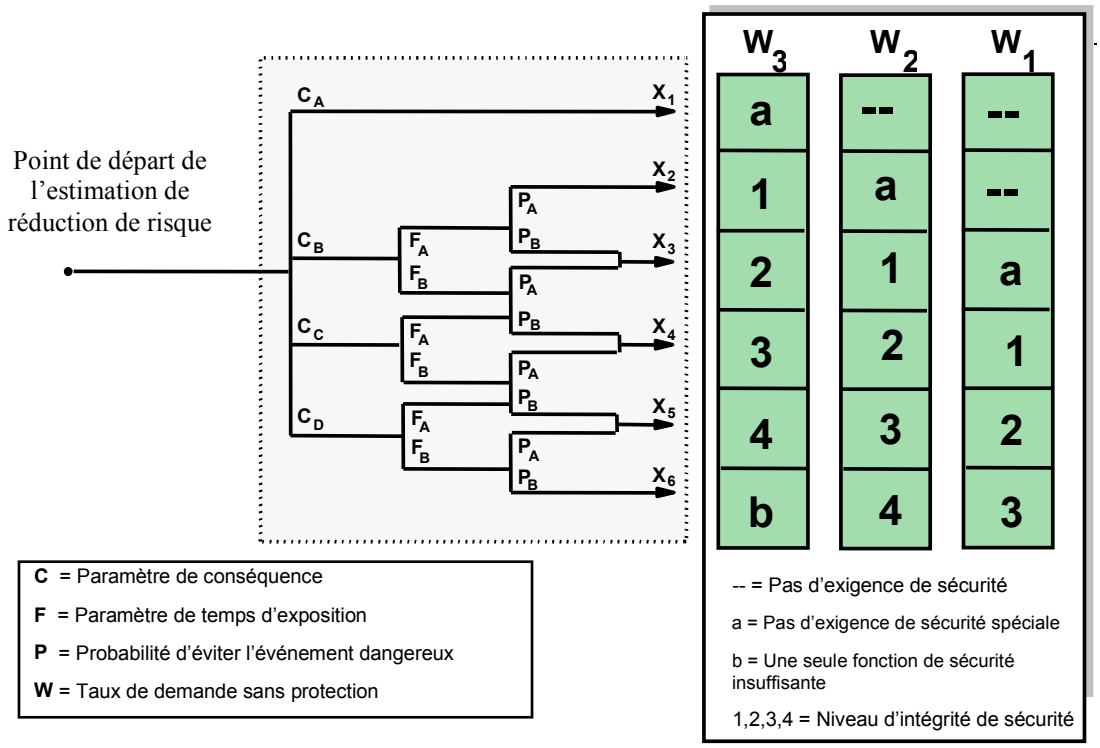


Figure 2.10 : Schéma général de graphe de risque

A l'aide de ce graphe de risque, la fonction de sécurité à implanter pour prévenir un danger de faible probabilité sera réalisée en tenant compte des exigences relatives au SIL1.

Un exemple de classification des paramètres du graphe de risques est montré au tableau 2.6.

Paramètre		**Classification**
Gravité des Conséquences	$\mathbf{C_A}$	Blessure mineure
	$\mathbf{C_B}$	Blessure sérieuse ou victime
	$\mathbf{C_C}$	Plusieurs victimes
	$\mathbf{C_D}$	Grand nombre de victimes
Temps d'exposition (Occupation)	$\mathbf{F_A}$	Rare
	$\mathbf{F_B}$	Fréquent
Probabilité d'éviter le phénomène dangereux	$\mathbf{P_A}$	Possible
	$\mathbf{P_B}$	invraisemblable
Probabilité d'apparition d'un accident (Taux de demande)	$\mathbf{W_1}$	Très faible probabilité
	$\mathbf{W_2}$	Faible probabilité
	$\mathbf{W_3}$	Forte probabilité

Tableau 2.6 : Légende de la classification des paramètres de risques

Dans cet exemple tiré de [GOB 98], les conséquences portent uniquement sur l'atteinte à la vie de personnes. La prise en compte des dégâts matériels et de dommages causés à l'environnement nécessite l'utilisation de graphes additionnels.

6.3.2.2. Matrice de gravité des événements dangereux

La matrice de gravité de risques intègre plusieurs fonctions instrumentées de sécurité sous réserve de leur indépendance contrairement à la méthode de graphe de risque qui ne prend qu'une fonction instrumentée de sécurité. Les trois composantes de la matrice sont la gravité des conséquences, la probabilité de l'occurrence des accidents et le nombre de dispositifs de sécurité déjà mis en place pour empêcher le développement du danger en accident.

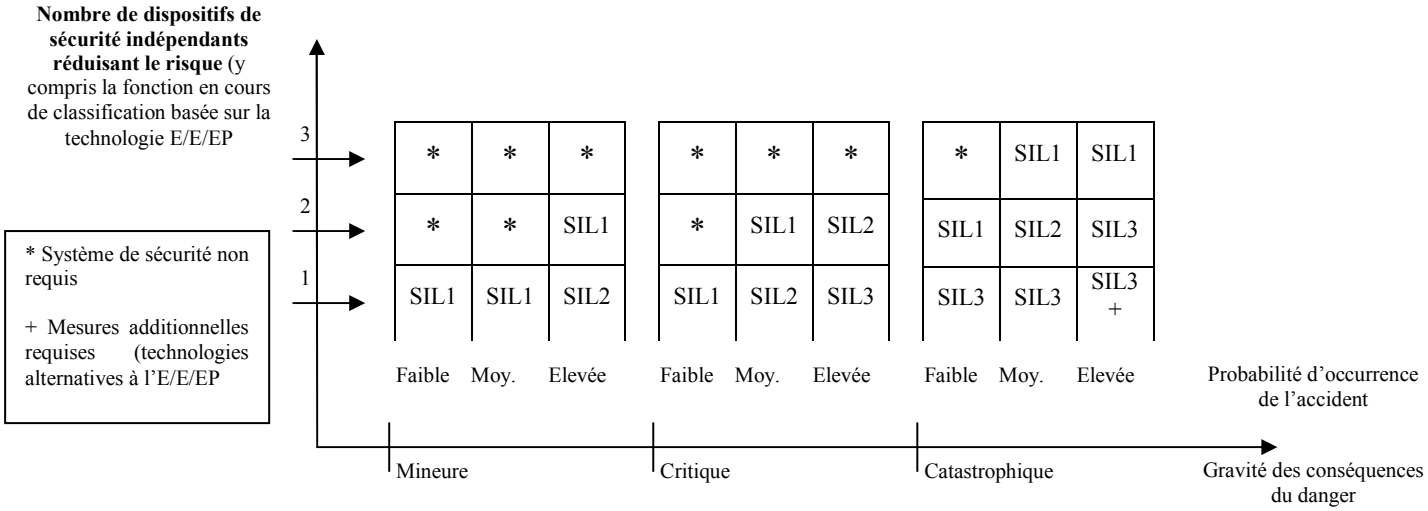


Figure 2.11 : Exemple de matrice de gravité des événements dangereux

L'exemple représenté sur la figure 2.11 est tiré de la norme CEI 61508. Suivant la mise à disposition d'un dispositif de sécurité permettant la prévention d'un danger d'occurrence faible et dont les conséquences sont critiques, le niveau d'intégrité de la fonction de sécurité sera réalisé en tenant compte des exigences relatives au SIL 1.

7. Les limites de la norme CEI 61508 et sa situation vis-à-vis des SAID

Tant les industriels que les chercheurs se posent des questions sur l'application de la norme CEI 61508 et avancent quelques commentaires et interprétations à propos de cette norme. Celle-ci n'aborde pas le délicat problème de l'utilisation des instruments intelligents dans les systèmes d'automatisation et le champ reste libre de telle sorte que certains fournisseurs revendiquent des instruments intelligents certifiés CEI 61508.

7.1. Limites de la norme CEI 61508

Il ne s'agit pas de faire une interprétation de la norme CEI 61508 traitant la sécurité fonctionnelle mais tout simplement de poser la problématique sur la difficile utilisation de la

norme. Il est à noter que les lecteurs de cette norme ressentent rapidement la nécessité d'être guidés, tant les notions qui y sont exposées peuvent paraître complexes, inhabituelles ou difficiles à mettre en œuvre.

Cette complexité la rend parfois difficilement applicable. Il faut rappeler que la norme est composée de sept volumes contenant 500 pages environ et elle préconise plus de 1000 prescriptions.

Beaucoup de prescriptions ne sont pas assignées à une certaine gamme des niveaux d'intégrité de sécurité ou à la complexité de la conception [FAL 04]. Ceci rend la norme difficile à utiliser pour de plus petits projets et rend la gestion de la sécurité fonctionnelle trop chère pour des petites et moyennes entreprises.

L'ambiguïté possible dans l'interprétation encourage les utilisateurs à employer la norme comme boîte à outils et à mettre en application plutôt les aspects qu'ils appréhendent [FAL 04]. Les utilisateurs en Amérique du Nord semblent être principalement préoccupés par la sécurité de matériel (taux de défaillances dangereuses, taux de défaillances en sécurité) [GOB 05] tandis qu'en Europe (Allemagne) [FAL 04], beaucoup d'utilisateurs semblent être préoccupés davantage par la sécurité de logiciel. La norme laisse également une bonne part à l'interprétation. Les interprétations diffèrent entre les experts sur les contraintes architecturales de matériel et la prise en compte du diagnostic. Les normes européennes du secteur industriel telles que la norme EN 954-1 n'acceptent pas des systèmes où le mode de défaillance d'un composant simple pourrait mener à un état peu sûr contrairement à la CEI 61508.

La norme CEI 61508 définit l'intégrité de sécurité comme propriété de l'installation complète de sécurité du capteur à l'actionneur. En outre, les parties 2 et 3 de la norme entrent dans le détail dans la conception et la "vérification et validation" (V&V) des systèmes électroniques programmables. Ceci mène souvent à la confusion auprès des fournisseurs qui n'hésitent pas à attribuer un niveau de SIL à leurs instruments. Pourtant, cela n'a aucun sens, le niveau de SIL étant strictement associé à une fonction de sécurité donnée. Pour réaliser cette fonction, l'utilisateur met en œuvre plusieurs sous-systèmes : capteur, traitement, actionneur. Dans chacun des sous-systèmes, des composants peuvent être mis en redondance. La PFD_{avg} de l'ensemble doit être calculée à partir des caractéristiques des composants et des architectures mises en œuvre.

Le SIL ne saurait être en aucun cas une caractéristique intrinsèque d'un instrument. Ce que nous pouvons considérer est uniquement une compatibilité avec un niveau de SIL. Cela correspond à une PFD_{avg} comprise dans la plage correspondant au SIL requis, cette PFD_{avg} étant affectée d'une période de test définie.

La norme demande des informations sur la conception des éléments entrant dans la chaîne de sécurité. Dans certains cas, il est possible de disposer de ces informations et de connaître le niveau de fiabilité du dispositif entrant dans la chaîne de sécurité. Le manque d'informations sur la conception pour les éléments constituant la boucle fait en sorte qu'il faut alors s'appuyer sur les retours d'expérience du fournisseur, qui peut fournir des informations précises sur la fiabilité de ses produits. Et à partir de là, il est possible de concevoir la chaîne de sécurité.

La probabilité de défaillance sur demande devrait être aussi renommée, car sa dénomination prête à confusion. Il ne s'agit nullement d'une défaillance à la sollicitation classique, mais d'une indisponibilité moyenne sur un intervalle temporel spécifié [INA 05].

Les formules littérales proposées dans le volume 6 de la norme, qui permettent le calcul de la probabilité de défaillance à la demande pour différentes architectures de systèmes, ont fait l'objet de quelques critiques [GUO 07] [ZHA 03] [HOK 04]. Ces relations sont données sans explications ou justifications et elles ont induit plus d'interrogations, voire de critiques, que de solutions satisfaisantes [INA 05].

Par exemple, le cas de l'architecture 1oo1 (*1 out of 1*) décrite dans la partie CEI 61508-6 de la norme qui dispose d'un seul canal et ne présente donc pas de redondance. A cette architecture, la norme affecte une durée moyenne d'indisponibilité t_{CE} telle que :

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

λ_D : Taux de défaillances dangereuses

λ_{DU} : Taux de défaillances dangereuses non détectées

λ_{DD} : Taux de défaillances dangereuses détectées

T_1 : durée du test périodique

MTTR : Durée moyenne de réparation

La probabilité moyenne de défaillance sur demande (indisponibilité moyenne) en est déduite :

$$PFD_{avg} = \lambda_D . t_{CE}$$

La norme ne donne pas de justification pour la détermination de ce genre de relations. [INA 05] a essayé d'élucider ceci par l'utilisation d'un modèle markovien multi-phases. Les résultats ont montré qu'il faut avancer plusieurs hypothèses telles que l'utilisation de taux de réparation fictif, le choix de l'ordre de quelques approximations, l'assimilation de la durée moyenne d'indisponibilité à la durée moyenne de non fonctionnement (MDT) [ZHA 03], l'approximation qui consiste à confondre la MTBF (*Mean Time Between Failures* ou durée moyenne entre deux défaillances successives) et la MTTF (*Mean Time To Failure* ou durée moyenne de bon fonctionnement avant la première défaillance)…

Les résultats montrent aussi que la norme est conservative, puisqu'elle donne des résultats légèrement pessimistes.

[SIG 05] stipule que le concept d'intégrité de sécurité est nécessaire mais pas suffisant pour caractériser correctement le niveau d'intégrité de sécurité d'un système instrumenté de sécurité. En effet, les formules centrées sur la détermination d'un indicateur moyen ne prennent pas en compte les dépassements répétés du seuil haut du domaine SIL concerné ni leurs conséquences négatives sur le niveau de sécurité réel du SIS étudié.

7.2. Positionnement vis-à-vis des SAID

La norme CEI 61508, bien qu'elle soit relative aux systèmes électriques, électroniques et électroniques programmables dédiés à la sécurité, ne traite pas explicitement le cas des systèmes d'automatisation à intelligence distribuée ni celui des instruments intelligents qui les composent.

Les seuls endroits où la norme fait allusion à ce type d'instruments figurent dans la partie 4 relative aux définitions et abréviations. On y trouve suite à la définition donnée à l'électronique programmable que celle-ci est une technologie basée sur l'informatique, pouvant comprendre du matériel, du logiciel, ainsi que les unités d'entrée et de sortie. La

norme précise que ce terme recouvre les appareils microélectroniques basés sur une ou plusieurs unités centrales de traitement associées à des mémoires. Et parmi les exemples des dispositifs électroniques programmables, la norme cite les microprocesseurs, les microcontrôleurs, les automates programmables, les circuits intégrés spécifiques à une application (ASIC), les automates logiques programmables et finalement les capteurs intelligents comme faisant partie des autres appareils basés sur la technologie informatique.

De plus, la norme dans cette même partie 4 présente un système électronique programmable (PES, *Programmable Electronic System*) comme étant un système de commande, de protection ou de surveillance basé sur un ou plusieurs dispositifs électroniques programmables recouvrant ainsi tous les éléments du système tels que l'alimentation, les capteurs jusqu'aux actionneurs en passant par les voies de communication.

L'illustration est faite sur la figure 2.12 suivante :

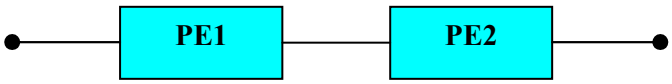


Figure 2.12 : Structure d'un PES avec deux dispositifs électroniques programmables [CEI 00]

Cette figure montre la façon dont est représenté le PES dans la norme CEI 61508, il y a une distinction de l'électronique programmable des dispositifs PE1 et PE2 qui se retrouvent en série et qui peuvent représenter par exemple un capteur intelligent et un automate programmable. L'électronique programmable peut par conséquent naturellement être présente en divers endroits du PES.

Une manière dont la norme traite la répartition de cette électronique programmable est de considérer une certaine redondance parallèle si on considère que la figure précédente à trait à une redondance série. Dans ce cas de figure aussi, le PES est composé de canaux distincts incorporant séparément de l'électronique programmable.

Nous constatons bien qu'implicitement il s'agit ici d'un partage de tâches et d'une distribution de l'électronique programmable à travers les différents dispositifs qui constituent le PES.

L'autre aspect absent ou presque de la norme est celui relatif aux réseaux de communication et particulièrement les réseaux de terrain. La norme reste muette sur cet aspect ainsi que sur l'interface matériel / logiciel. Sur l'aspect logiciel, la norme se contente de dresser uniquement des recommandations.

Parmi ce type de recommandations, la norme spécifie le langage de programme figé (*FPL*, *Fixed program language*) dans lequel l'utilisateur est limité à l'ajustement de quelques paramètres (par exemple la gamme d'un transmetteur de pression, les seuils d'alarme, les adresses de réseau). La norme spécifie aussi le langage de variabilité limitée (*LVL, Limited Variability Language*) qui est conçu pour être compréhensible par les utilisateurs du domaine du processus et fournit la possibilité de combiner des fonctions de bibliothèque spécifiques à une application.

Les exemples représentatifs de dispositifs avec FPL sont les capteurs intelligents et les vannes intelligentes et un exemple des systèmes utilisant les LVL est celui d'un automate programmable standard.

8. Paramètres de performance en sécurité pour les systèmes instrumentés de sécurité

La norme CEI 61508 [CEI 00] 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). Leur évaluation comme l'exige la norme CEI 61508 pose quelques problèmes liés à leur spécificité. 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.

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 PFD_{avg} (*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 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 [CEI 00]. 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 [WOL 05].

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. Un système est sûr si ses défaillances ne sont pas dangereuses.

La figure 2.13 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 [MAR 01].

Figure 2.13: Système avec modes de défaillances

La fiabilité n'est pas suffisante à elle seule. Dans plusieurs applications, il est aussi important que le système tombe en panne d'une manière prévisible (défaillance sûre).

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 les 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 2.14 suivante :

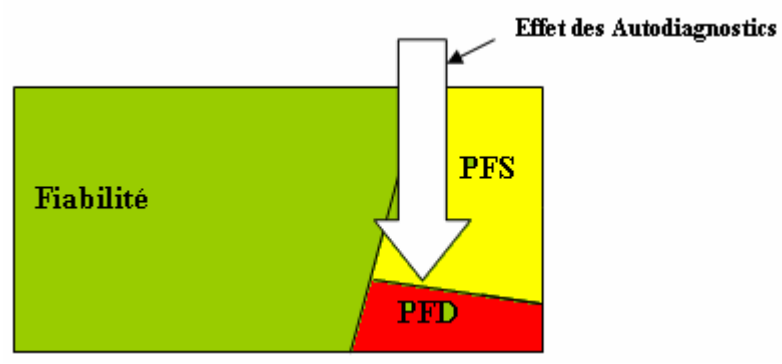


Figure 2.14 : Effet des autodiagnostics sur le système instrumenté de sécurité

La norme CEI 61508 [CEI 00] (partie 6, annexe C) considère que la répartition entre défaillances non dangereuses (sûres) et défaillances dangereuses peut être déterministe pour des composants simples. Pour des composants complexes, dont il n'est pas possible d'effectuer une analyse détaillée de chaque mode de défaillance, une répartition des défaillances en 50 % de sûres et 50 % de dangereuses est généralement acceptée :

$\lambda_D = \lambda_S = 0.5\ \lambda$

où λ est le taux de défaillance du composant.

La norme définit pour les produits (et non pas le système entier) tels que les capteurs, actionneurs et unités de traitements, un taux des défaillances en sécurité *SFF* (*Safe Failure Fraction*).

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

Cette métrique est un ratio de taux de défaillances et ne dépend pas du taux total de défaillances. Le résultat est un nombre entre zéro et un. Il est souhaitable d'avoir un SFF suffisamment important. Le *SFF* mesure la tendance de l'instrument à avoir des défaillances sûres ou détecter des défaillances dangereuses.

Nous allons déterminer tout d'abord les taux de défaillances dangereuses et sûres pour chaque composant.

$\frac{\lambda_S}{\lambda} = S\%$, d'où $\lambda_S = \lambda\ S\%$ et $\lambda_D = \lambda\ (1 - S\%)$

Avec $\lambda_S = \lambda_{SD} + \lambda_{SU}$

$\lambda_{DD} = CD\ \lambda_D$, avec CD le facteur de couverture de diagnostic des défaillances dangereuses.

$\lambda_{DU} = (1 - CD)\ \lambda_D$

$SFF = S\% + (1 - S\%)\ CD$, il y a indépendance de λ total.

$\lambda(t) = \lambda$. Le taux de défaillance constant est pris comme hypothèse pour la plupart des estimations statistiques, cela s'applique seulement si la durée de vie utile des composants n'est pas dépassée [CEI 00]. Dans notre cas, et comme c'est préconisé par la norme, nous considérons des taux de défaillance des composants constants sur toute la durée de vie du système.

et $R\ (t)\ =\ e^{-\lambda t}$, *R(t)* représente la fiabilité

La probabilité de défaillance est donnée par : $F\ (t)\ =\ 1\ -\ e^{-\lambda t}$, elle est appelée aussi parfois défiabilité.

Si la demande est rare, alors dans ce cas : $e^{-\lambda t}\ \approx\ 1\ +\ \lambda\ t$, l'approximation est arrêtée au premier ordre.

La probabilité de défaillance vaut alors : $PF(t) = \lambda t$, et la probabilité de défaillance moyenne est donnée par : $PF_{avg} = \frac{1}{T}\int_0^T PF(t)dt$

La probabilité de défaillance sur demande qui concerne le système entier est donnée par :

$PFD_{avg} = \frac{1}{Ti}\int_0^{Ti} PFD(t)dt$, avec la durée Ti qui représente l'intervalle entre deux tests périodiques.

Dans le cas de l'approximation faite ci-dessus, on aura : $PFD_{avg} = \frac{\lambda Ti}{2}$

9. Conclusion

Les systèmes instrumentés de sécurité sont utilisés pour détecter des situations dangereuses et diminuer leurs conséquences pour atteindre des niveaux de risques tolérables. La norme générique CEI 61508 et sa norme fille CEI 61511 pour le secteur des procédés continus deviennent les normes de référence pour la spécification et la conception de ce type de systèmes (SIS).

La norme CEI 61508 utilise une approche basée sur le risque pour déterminer les exigences d'intégrité de la sécurité des systèmes E/E/PE concernés par la sécurité. D'autre part, elle utilise un modèle global de cycle de vie de la sécurité comme cadre technique pour les activités nécessaires pour garantir que la sécurité fonctionnelle soit atteinte par les systèmes E/E/PE concernés par la sécurité.

L'appréciation du risque est une fonction de la gravité et de la fréquence. Il est souvent difficile d'apprécier l'un ou les deux et encore plus la combinaison des deux. Dans une démarche d'analyse du risque, il faut prendre acte de cette difficulté. L'essentiel est de

pouvoir au moins classer les risques entre eux, selon une échelle que l'on s'est donnée. Le point important est alors la calibration initiale de cette échelle. C'est l'objet des méthodes de classement des risques. L'intérêt est de pouvoir comparer les risques et de leur affecter la bonne échelle.

Les niveaux d'intégrité de sécurité issus de la norme sont des objectifs de sécurité utiles à l'évaluation des risques. Ils donnent une mesure de la réduction du risque obtenue par les moyens de protection fournis par le SIS.

Néanmoins, cette norme présente des limites d'utilisation et elle est sujette à de nombreuses critiques relatives à la forme et au fond telles que la difficulté de l'application des formules, la confusion pour la détermination du niveau d'intégrité de sécurité pour certaines définitions de base et méthodes proposées [HOK 04]…

Les contraintes éprouvées par les utilisateurs pour l'application de la norme pour les architectures les plus simples les poussent à entreprendre des modélisations pour les systèmes les plus complexes.

D'un point de vue opérationnel, il est naturellement préférable de recourir à des méthodes éprouvées, telles que l'arbre des défaillances, les graphes de Markov ou les réseaux de Petri, plutôt que d'utiliser systématiquement les formules analytiques exposées dans la CEI 61508 [INN 07].

Finalement, la norme reste muette sur l'aspect de la distribution de la gestion des fonctions de sécurité et sa répartition sur l'ensemble de la structure du système instrumenté de sécurité. Le vide laissé par la norme a été exploité par quelques fournisseurs qui ont profité de l'occasion pour annoncer l'utilisation de réseaux de terrain dans la fabrication des systèmes instrumentés de sécurité.

Chapitre 3 : Vers une sécurité intelligente

Vers une sécurité intelligente

1. Introduction

L'évolution des équipements d'automatisation a poussé d'une part à l'utilisation des instruments dans des équipements sécuritaires qui deviennent plus "intelligents", aptes à communiquer avec les équipements de production et, pourquoi pas, avec l'homme, de manière à optimiser leur comportement (optimisation de la sécurité). D'autre part, il est devenu possible d'intégrer aux équipements "intelligents" une fonction sécuritaire apte à appréhender son environnement et à réagir localement en fonction du rôle de l'équipement auquel elle est associée.

Les instruments intelligents sont des instruments de processus de base qui contiennent des microprocesseurs. L'utilisation de microprocesseurs présente un défi dans de nombreuses industries, en particulier pour des architectures critiques ou de sécurité.

Le concept de sécurité intelligente est inhérent à l'utilisation d'instruments intelligents dans les systèmes instrumentés de sécurité. Plusieurs fabricants revendiquent la certification de produits intelligents dans les applications de sécurité en lançant des "smart SIS " mais sans réelle justification au niveau des performances fiabilistes. Des chercheurs emploient aussi le vocable "sécurité intelligente" dans des applications diverses couvrant le nucléaire [YAN 05] [CHU 03] [BAE 01], le ferroviaire [JIA 03] ou encore les systèmes de transport [FAR 04].

La première partie de ce chapitre positionne la problématique de l'utilisation des instruments intelligents dans les applications sécuritaires en situant aussi quelques différences qui existent entre les systèmes classiques et les systèmes intelligents.

La seconde partie traite de l'introduction du concept de l'intelligence dans un système instrumenté de sécurité par l'utilisation d'une part d'un réseau de communication typiquement un réseau de terrain et ensuite par la distribution des traitements au plus près du processus, c'est-à-dire dans les dispositifs de terrain tels que les capteurs et actionneurs.

Dans la dernière partie, nous proposons une méthodologie d'évaluation des systèmes instrumentés de sécurité auxquels il y a eu incorporation d'instruments intelligents pour devenir des Systèmes Instrumentés de Sécurité à Intelligence Distribuée (SISID).

2. Contexte et problématique

L'utilisation des instruments intelligents dans l'industrie des procédés a été facilitée par l'augmentation des performances dans les microprocesseurs utilisés en milieu industriel, notamment en instrumentation. 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 [NOB 04].

Les instruments intelligents sont placés dans des applications sécuritaires plus "intelligentes", afin de communiquer avec les équipements de production et, pourquoi pas, avec l'homme, de manière à optimiser leur comportement et/ou l'intégration aux équipements intelligents d'une fonction sécuritaire apte à appréhender son environnement et à réagir localement en fonction du rôle de l'équipement auquel elle est associée.

Il existe actuellement une tendance à l'utilisation des instruments intelligents dans les applications sécuritaires du fait de l'aptitude des systèmes à diagnostiquer les défaillances ainsi que de permettre la mesure de certains paramètres complexes avec une confiance améliorée.

La justification de cette tendance vers l'utilisation des instruments intelligents n'est pas tout à fait prouvée en dépit des revendications de quelques industriels qui se targuent d'offrir des systèmes dédiés à la sécurité en conformité avec les normes en vigueur et incorporant des équipements de terrain intelligents ou encore des moyens de communication internes aux fonctions de sécurité.

En effet, certains constructeurs comme Fisher, Norgren-Herrion, Metso Automation spécialisés dans les automatismes de processus proposent des produits tels que les transmetteurs, les vannes et octroient des niveaux d'intelligence à ces produits dans le cas où le dispositif contient un microcontrôleur ou s'il est doté d'un test en ligne. Les moyens de communication utilisés sont des boucles classiques 4-20 mA ou encore le protocole HART qui n'est pas un réseau de terrain [CIA 99].

2.1. Instruments intelligents versus instruments traditionnels

Les systèmes classiques comportant des capteurs traditionnels produisent habituellement des signaux électriques de basse complexité directement à partir des dispositifs de transduction. La simplicité de ces systèmes a mené à une acceptation de tels dispositifs dans des applications de protection des systèmes critiques de sécurité (nucléaire par exemple). En général ce sont des dispositifs mécaniques et électriques simples, avec un retour d'expérience suffisant, ils sont reliés avec des circuits bien définis avec une faible interaction. Ceci se prête à une abstraction mathématique facile pour les modèles fiabilistes et pour la détermination des modes de défaillance. Par conséquent la probabilité de défaillance dangereuse peut être calculée et évaluée.

Avec la tendance moderne de traiter les données de tels instruments dans les systèmes informatiques (plus généralement numériques), il y a eu un besoin de convertir les valeurs électriques sous des formes de représentations aptes à être traitée par un logiciel. Ceci exige une complexité de matériel et de logiciel bien au-dessus de celle qui existait dans ce type d'instruments classiques [DOB 98]. Les nouvelles fonctions incorporées dans les instruments intelligents sont fortement complexes et intégrées. Ceci rend l'analyse de sécurité difficile, de même que la nature fortement interactive des interfaces, particulièrement quand un réseau de communication est partagé entre plusieurs dispositifs. Cependant ces fonctions disposent de

moyens d'autotest et d'une possibilité de redondance fonctionnelle qui peuvent assurer une diminution acceptable de probabilité de défaillance [DOB 98] [MAC 04].

Un autre aspect de différence qui existe entre les instruments classiques et les instruments intelligents est le facteur temps. En effet, dans les capteurs conventionnels le temps et la synchronisation ne sont pas pris en compte. Le capteur mesure continuellement les paramètres physiques et présente un signal par l'intermédiaire de la boucle de courant 4-20 mA. Par conséquent, le délai entre la mesure et son envoi est normalement négligeable [MEU 04].

Pour les capteurs intelligents ce n'est pas aussi simple. Le temps s'ajoute aux grandeurs physiques. En effet, si une date est fausse, la mesure peut être considérée comme aberrante par le système d'information [ROB 93], en particulier, la mesure fournie est susceptible d'être postdatée ou antidatée.

Notons que conformément au chapitre 1, il y a une différence entre un capteur analogique (classique, niveau 0) et un capteur numérique (niveau 1). La numérisation du signal a permis l'association d'un processeur a proximité du capteur. L'utilisation de la microinformatique va permettre d'exploiter les caractéristiques temporelles des signaux issus des capteurs (transformée de Fourier rapide). Le capteur numérique dispose d'une certaine capacité de calcul assurée par un circuit programmable du type microcontrôleur ou microprocesseur lui permettant de prendre en compte certaines dérives et grandeurs d'influence. L'élément de calcul est constitué, au minimum, d'un microcontrôleur, d'une EEPROM d'un convertisseur analogique numérique et un dispositif de multiplexage pour acquérir séquentiellement les données. En plus il existe un traitement des signaux discrets réalisé par des algorithmes spécifiques. Il existe cependant un certain retard puisque le microprocesseur qui gère le système fonctionne séquentiellement.

Les instruments classiques diffèrent aussi par rapport aux instruments intelligents dans l'aspect de l'intégrité des informations. [MEU 04] précise que l'intégrité des données n'est pas un grand problème dans les capteurs conventionnels. Des paramètres sont placés à l'aide du matériel (commutateurs à résistances par exemple) et sont donc fortement peu sensibles aux influences externes. Pour les capteurs intelligents ces aspects sont plus complexes. Des paramètres sont placés en utilisant des boutons et des affichages et ils sont stockés dans une mémoire (RAM et/ou EEPROM). Le stockage dans la mémoire est nécessaire si le capteur doit maintenir les paramètres après une panne de courant. Les données dans la mémoire peuvent être corrompues du fait de la sensibilité au rayonnement et à la chaleur, et il est nécessaire de faire une détection et une correction d'erreur.

Les instruments intelligents disposent aussi de circuits fortement intégrés et par conséquent les fabricants sont maintenant capables d'offrir des capteurs avec des sorties numériques compatibles au plan logiciel qui n'ont besoin d'aucun circuit de pré-conditionnement. Ces instruments offrent des fonctionnalités nouvelles telles que l'exactitude, la flexibilité, l'autodiagnostic, la communication, la gestion des activité de l'instrument …[DES 06]. Ces fonctions sont conçues pour améliorer la qualité métrologique de la mesure, de la fiabilité du système par l'amélioration de la fiabilité des informations [TAN 96].

[YUR 06] [MAS 98] citent les avantages de l'intégration comprenant outre la diminution du nombre de composants et la chute des coûts une fiabilité inhérente élevée. [DES 06] rajoute que le concept d'instrument intelligent a été défini dans les années 80 pour aborder le manque de fiabilité et que les instruments intelligents contribuent à l'amélioration de la fiabilité et de la réactivité. Cette réactivité est rendue possible par les moyens de traitement disponibles localement au niveau terrain. En effet, l'intégration des fonctionnalités de surveillance et de diagnostic vont permettre de maîtriser la sûreté de fonctionnement du système par le biais de

détection de défauts par des méthodes de surveillance locale. Aussi, les systèmes à architecture répartie vont présenter de l'intérêt par l'emploi d'un nombre de points de mesure élevé permettant au système une coopération accrue grâce notamment à la communication.

Un point de vue tout à fait opposé est exprimé par le tableau suivant des données qui est extrait de [DOB 98]. Il met en évidence l'utilisation de différentes technologies pour des capteurs de pression. Premièrement, l'approche conventionnelle pour un capteur 4-20 mA à l'aide des circuits analogiques a été considérée. Ensuite le même capteur a été considéré où la majeure partie du circuit analogique est remplacée par un simple ASIC analogique. Enfin le capteur "smart " communicant relié par un bus de communication a été considéré. Ce dernier fonctionne en interne numériquement et permet l'amélioration de la fonction de traitement de l'information. L'indicateur de fiabilité considéré ne contient aucune indication relative aux défaillances de logiciel. Pour un système contenant 32 capteurs le taux de défaillances prévu est montré, tenant compte des composants électroniques seulement. Le manque de fiabilité additionnel résultera du logiciel et de tout autre matériel.

Composant	Taux de défaillances (par 10^6 heures)	Taux de défaillance du système comportant 32 capteurs avec un organe d'acquisition de données et le câblage
Capteur analogique 4-20 mA	2.777	97.9
Capteur avec ASIC 4-20 mA	2.318	82.9
Capteur "smart " communicant	5.543	180

Tableau 3.1 : Données de fiabilité relatives aux différents systèmes suivant la nature des capteurs [DOB 98]

La conclusion simple à tirer de ce tableau est que le système comportant des capteurs numériques connectés à l'aide de réseau de terrain pourrait être moins fiable qu'un système à capteurs classiques. D'après notre classification faite dans le chapitre 1, ce cas d'étude s'apparente aux instruments numériques communicants (niveau 1) qui disposent d'une complexité accrue par rapport aux instruments classiques (niveau 0). A ce niveau d'intelligence (niveau 1), les aspects relatifs à la sûreté de fonctionnement ne peuvent guère être améliorés. Notons aussi que l'approche décrite dans le tableau 3.1 est incomplète du fait qu'une seule partie des causes de défaillances est prise en compte.

Les capteurs conventionnels emploient les boucles 4-20 mA pour la communication. Ces boucles ne peuvent pas être employées à des distances très longues. Les réseaux de communication sont souvent capables d'atteindre d'importantes distances moyennant l'emplacement de répéteurs. Dans ce cas, les répéteurs sont nécessaires, ce qui augmente la quantité d'équipement et la possibilité de défaillance.

En conclusion, et suivant cette disparité dans les avis, ceci nous laisse présager une analyse adéquate sur la vraie contribution de l'intelligence dans les systèmes instrumentés surtout

pour des applications relatives à la sécurité en tenant compte de la classification des niveaux d'intelligence dans les instruments.

2.2. Problématique relative à l'utilisation des instruments intelligents dans les boucles de sécurité

L'introduction des instruments intelligents dans des applications sécuritaires basées sur les systèmes instrumentés de sécurité doit avoir pour objectif l'amélioration de la sécurité et non pas le contraire sinon à quoi bon des investissements colossaux en technologies, ressources humaines, formation et coût de revient si le résultat final de cette introduction est similaire ou en deçà du niveau des performances par rapport à des systèmes classiques utilisant des instruments conventionnels.

Pour cela, regardons de près la valeur ajoutée qu'apporte un système d'automatisation à intelligence distribuée (SAID). Celle-ci peut se résumer en la distribution de l'intelligence (ou encore des traitements) en utilisant comme auxiliaire la communication par réseau mais aussi, dans le cas d'architecture répartie, le pouvoir de faire du diagnostic distribué.

Inutile de montrer encore le mérite de l'utilisation de ce type de systèmes surtout en contrôle commande, ceci était l'objet du premier chapitre.

La question qui se pose est relative donc à la sauvegarde des performances dans un système instrumenté de sécurité par l'introduction de l'intelligence dans les différentes fonctions de sécurité, voire l'amélioration de ces performances.

La norme CEI 61508 [CEI 00] spécifie deux indicateurs de la sécurité relatifs aux systèmes électroniques programmables dédiés aux applications de sécurité. Ces deux indicateurs sont la probabilité de défaillance dangereuse (PFD) et la probabilité de défaillance en sécurité (PFS). Leur évaluation comme l'exige la norme CEI 61508 pose quelques problèmes liés à leur spécificité. 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.

La norme exige un certain nombre de recommandations et de prescriptions relatives à l'utilisation des moyens de communication de données pour réaliser des fonctions de sécurité. Notamment lorsqu'une forme quelconque de communication de données est utilisée dans la réalisation d'une fonction de sécurité, la probabilité de défaillance de la fonction de sécurité due au processus de communication doit être estimée en prenant en compte les erreurs de transmission, les répétitions, les suppressions, les insertions, les modifications du séquencement, la corruption, le retard et le masquage. Cette probabilité doit être prise en compte lors de l'estimation de la probabilité de défaillance dangereuse de la fonction de sécurité, due à une défaillance aléatoire du matériel.

Le terme masquage signifie que le contenu exact d'un message n'est pas correctement identifié. Par exemple, un message provenant d'un composant qui n'est pas de sécurité est identifié incorrectement comme un message provenant d'un composant de sécurité.

En particulier, les paramètres suivants doivent être pris en compte en estimant la probabilité de défaillance de la fonction de sécurité due au processus de communication:

a) le taux d'erreur résiduel;

b) le taux de perte d'information résiduel;

c) les limites et la variabilité de la vitesse de transfert de l'information;

d) les limites et la variabilité du temps de retard dû a la propagation de l'information.

La norme explique aussi que la probabilité d'une défaillance dangereuse (en h^{-1}) est égale au quotient de la probabilité d'erreur résiduelle par la longueur du message (en bits) multipliée par la vitesse de transmission sur le bus des messages relatifs à la sécurité ainsi que par un facteur de 3600[1].

Les défaillances de cause commune et celles dues aux processus de communication des données peuvent résulter d'effets autres que les défaillances des composants matériels (par exemple, perturbation électromagnétique, erreurs de décodage, etc.). Toutefois, de telles défaillances sont considérées, pour les besoins de la présente norme, comme des défaillances aléatoires du matériel.

La norme recommande aussi qu'afin de maîtriser les anomalies systématiques, la conception E/E/PES doit avoir des caractéristiques de conception telles que les systèmes E/E/PE relatifs à la sécurité soient tolérants, entre autres, aux erreurs et autres effets provenant d'un processus de communication de données.

La question demeure donc sur la prise en compte des défaillances du réseau de communication et de l'introduction de son modèle de défaillance.

Les architectures des systèmes de sécurité dans l'automatisation peuvent avoir une forme classique où l'intégration de la fonction de sécurité se fait uniquement au niveau des automates programmables industriels (la fonction traitement) ou une forme dans laquelle la sécurité est distribuée avec un traitement local de la sécurité au niveau des périphériques décentralisés tout en gardant un traitement central de la sécurité au niveau des API.

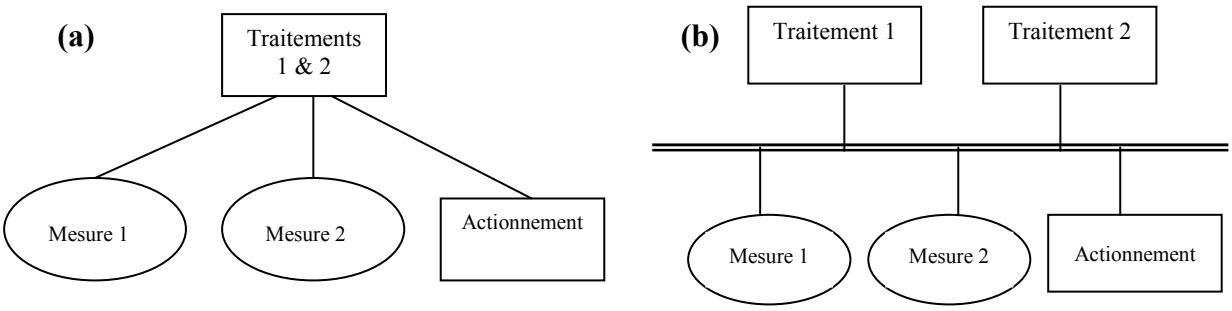


Figure 3.1 : Comparaison entre une architecture centralisée (a) et une architecture distribuée (b)

La présence d'un réseau apporte une fonctionnalité additionnelle, à savoir la communication. La décomposition fonctionnelle de ces deux architectures est proposée par [CAU 04] dans laquelle la fonction de communication constitue un composant du système.

La figure 3.2 montre cette décomposition fonctionnelle pour les deux architectures.

[1] La valeur 3600 correspond à la conversion d'une heure en secondes puisque la vitesse de transmission a pour unité le baud (bit par seconde) et la probabilité d'erreur est donnée avec l'unité h^{-1}.

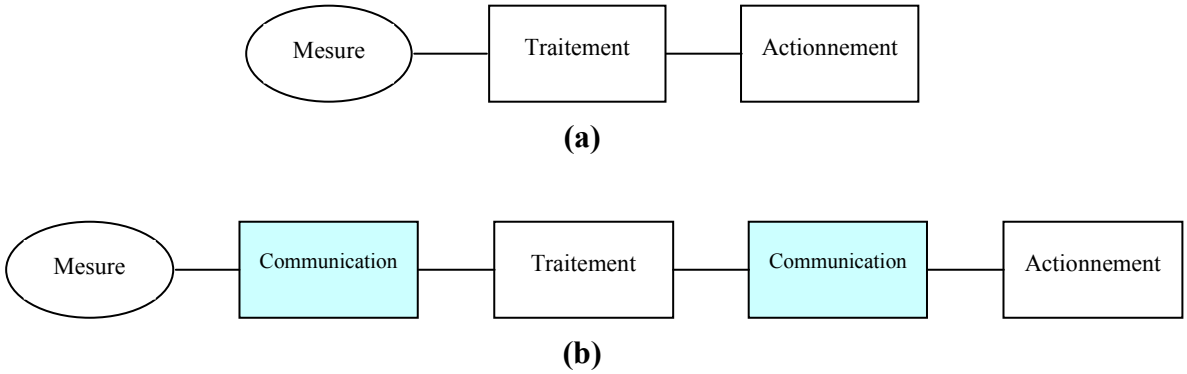


Figure 3.2 : Fonction communication dans l'architecture distribuée [CAU 04]

Ce modèle qui considère que la fonction communication fait partie intégrante du système et peut se présenter sous forme d'un composant à part entière tantôt entre la mesure et le traitement et tantôt entre le traitement et l'actionnement ne peut suffire pour représenter le modèle fiabiliste du système.

La norme, par l'utilisation des blocs diagrammes de fiabilité dans sa partie 6, donne la probabilité moyenne de défaillance sur demande d'une fonction de sécurité du système E/E/PE comme la combinaison de la probabilité moyenne de défaillance sur demande pour tous les sous-systèmes assurant ensemble la fonction de sécurité.

Plus formellement :

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$$

Où

- ✓ PFD_{SYS} est la probabilité moyenne de défaillance sur demande d'une fonction de sécurité du système E/E/EP relatif à la sécurité,
- ✓ PFD_S est la probabilité moyenne de défaillance sur demande du sous-système capteur (fonction mesure),
- ✓ PFD_L est la probabilité moyenne de défaillance sur demande du sous-système logique (fonction traitement),
- ✓ PFD_{FE} est la probabilité moyenne de défaillance sur demande du sous-système élément final (fonction actionnement).

Cette modélisation en diagrammes de fiabilité ne peut cependant s'appliquer pour la représentation de la fonction communication de l'architecture distribuée et on ne peut sommer facilement et simplement les probabilités moyennes de défaillances consécutives pour aboutir à la valeur moyenne de la probabilité de défaillance PFD_{SYS} globale.

En effet, la représentation (b) de la figure 3.2 est insuffisante pour décrire les phénomènes qui se passent réellement. Ce n'est pas vraiment un diagramme de fiabilité parce que quelque soit le temps le modèle ne bouge pas. En fait, il n'est pas du tout tenu compte des défaillances réseaux qui sont des défaillances temporelles. Aussi, il y a existence d'un mode commun auquel le modèle ne fait pas allusion et qui est dû à la distribution et donc de la présence de la communication d'une part entre les capteurs et le traitement et d'autre part entre le traitement et l'actionneur.

Néanmoins, cette fonction communication peut être modélisée par un seul bloc dans le modèle fiabiliste du système afin d'avoir un modèle de référence d'un point de vue statique.

L'aspect principal de l'intelligence des systèmes d'automatisation est celui de la distribution des traitements au plus bas niveau (dit niveau 0) de la pyramide CIM (*Computer Integrated Manufacturing* : fabrication intégrée sous le contrôle de l'informatique) [SHE 94]. Cette distribution permet la répartition des tâches de contrôle des processus aux dispositifs de terrain (capteurs et actionneurs) favorisant ainsi la mise en place des autotests pour une détection rapide et un déclenchement de mesures nécessaires aux moments opportuns. La distribution est vue ainsi comme une sorte de sous-traitance des traitements par l'implantation des fonctionnalités complexes dans les dispositifs de terrain.

Il est aussi intéressant de situer la contribution de cette amélioration de pouvoir de réactivité à la fiabilité de ce type de systèmes plus complexes et disposant d'autres modes de défaillances par rapport aux systèmes classiques. [BRO 05] fait savoir que l'utilisation de transmetteurs intelligents améliore la robustesse aux défaillances de causes communes par la séparation du transducteur de l'électronique permettant au capteur d'être relié directement au processus physique avec une électronique qui se situe dans un endroit accessible.

3. Intelligence dans les systèmes instrumentés de sécurité

L'introduction de l'intelligence dans les systèmes instrumentés de sécurité se concrétise par la déportation d'une partie de la décision dans les instruments de terrain (capteurs et/ou actionneurs) au moyen de l'utilisation d'un réseau de communication typiquement un réseau de terrain.

3.1. Utilisation d'un réseau de communication

L'organisme international de normalisation ISO a défini un modèle de référence ou modèle OSI (*Open System Interconnection*) [ZIM 80]. Le modèle OSI distingue sept couches et définit leurs rôles respectifs. Les couches physique, liaison de données, réseau et transport s'occupent du transfert de données sur le réseau de communication et permettent le transfert de données d'une machine à une autre machine. Les couches session, présentation et application sont plus liées au type d'application utilisée.

3.1.1. Réseau de terrain

Les réseaux de terrain représentent, par rapport aux réseaux de communication classiques, une modification en terme d'architecture dans le but de diminuer les délais de communication des échanges d'informations entre les éléments du procédé.

L'architecture d'un réseau de terrain est réduite aux couches essentielles de l'architecture ISO de l'OSI, c'est-à-dire les couches application, liaison des données et physique.

Les principales caractéristiques que doivent satisfaire les réseaux de terrain sont : temps de transfert déterminé, contrôle de flux, faible longueur des trames, capacité à traiter/gérer des événements particuliers (type de synchronisation), génération d'un trafic périodique (ou cyclique) en plus du trafic apériodique et mise en œuvre de mécanismes particuliers permettant la vérification des contraintes temporelles moyennant un bon contrôle de l'accès au médium [BER 96].

De nombreux réseaux de terrain ont été mis sur le marché (Profibus, WorldFip, CAN, Interbus-S, …) [CIA 99], ils offrent aux équipements des systèmes automatisés la possibilité de communiquer entre eux.

Derrière les bus de terrain se profile une évolution vers Ethernet dans l'univers des automatismes.

Le réseau Ethernet est spécifié par la norme IEEE 802.3 [IEE 98], c'est un réseau dont le contrôle d'accès au medium physique (*MAC : Medium Access Control*) utilise l'algorithme du CSMA/CD (*Carrier Sense Mutiple Access / Collision Detection*). CSMA/CD est le moyen par lequel deux (ou plus) stations partagent le même support physique.

Avec l'arrivée des commutateurs (switchs) en remplacement des concentrateurs (*hubs*), Ethernet a évolué vers Ethernet commuté et il a commencé à s'intéresser aux applications temps réel.

La configuration adoptée dans un réseau Ethernet commuté est celle d'une topologie en étoile, avec un commutateur central dont les ports sont reliés à un et un seul équipement. L'interconnexion avec les autres éléments est ensuite réalisée en reliant les commutateurs entre eux. Le mode Full Duplex prévu dans la norme IEEE 802.3 permet une communication simultanée entre deux stations assurant une diminution de risque de collisions lorsque le réseau est fortement sollicité.

On appelle couramment ce type de réseau un réseau Ethernet commuté Full Duplex. Ces réseaux possèdent l'avantage de ne plus posséder d'indéterminisme quant au temps d'accès au support physique, et de ne pas entraîner de pertes de trames par collision.

Le réseau Ethernet commuté peut être ouvert ou fermé. Dans le premier cas, il peut être victime d'"attaques" extérieures (virus, piratage) mais surtout peut se poser également le problème de la qualité de service, ou de la disponibilité du réseau (commutateur saturé par exemple).

3.1.2. Réseaux de terrain relatifs à la sécurité

Pendant longtemps, les architectures d'automatismes distribués, tant dans le manufacturier que dans le secteur des procédés se sont heurtés à un obstacle majeur : leur fonction de sécurité restait câblée en fil à fil.

Les réseaux de terrain relatifs à la sécurité offrent l'indépendance de la communication liée à la sécurité et de la communication standard (cas de *Profisafe*) mais aussi leur cohabitation (cas de *ASI-Safety at work*).

Plusieurs types de réseaux relatifs à la sécurité sont implémentés dans des applications industrielles spécialisées, parmi lesquels on trouve ASI-Safety at work, Profisafe, SafetyBus [WOO 03].

Nous allons nous intéresser à décrire un réseau de terrain relatif à la sécurité qui est le réseau Safetybus p basé sur le standard CanOpen.

A l'origine le CAN (Controller Area Network) a été développé pour l'usage automobile par Bosch. La fiabilité et le coût étaient les principaux objectifs [CIA 99].

Le réseau CAN possède des fonctionnalités Multi Maîtres (multi master) pour accroître la possibilité d'assurer des temps rapides de recouvrement d'erreurs après leur détection [PAR 99]. Sur le réseau CAN, chaque message possède un identificateur qui détermine sa priorité.

Un principe d'arbitrage est effectué autorisant ainsi les messages à plus haute priorité à être transmis.

La topologie utilisée par CAN est le bus. Lorsque celui-ci est libre, n'importe quelle station peut commencer à transmettre une information. Lorsque deux nœuds tentent d'accéder simultanément au médium, l'arbitrage est gagné par celui qui dispose de la haute priorité.

CANopen est un protocole qui utilise le bus CAN. L'un des objectifs de CANopen est de supporter des systèmes temps réel [PAR 99]. En effet des tâches particulières sont attribuées aux différents intervenants impliqués (maîtres ou esclaves). Safetybus est basé sur CANopen. Il est destiné à la mise en réseau d'applications de sécurité déportées. Il nécessite l'utilisation d'un ou plusieurs automates de sécurité. Des modifications ont été apportées au niveau de la couche d'échange de données CSMD afin de rendre le protocole plus sûr. Il comporte les couches 1 et 2 suivant le modèle ISO / OSI. La couche 1 est partiellement redéfinie tandis que la couche 7 subit une révision totale. Cette nouvelle couche 7, intégrant les mesures de sécurité et le système de gestion du réseau a été ajoutée dans le SafetyBUS p. Le réseau Safetybus dispose de nouvelles fonctionnalités de contrôle de signaux intégrées, des fonctions *timer* pour la transmission des messages et des fonctionnalités de diagnostic intégrées, d'une décentralisation des modules entrées/sorties, la connexion des capteurs et actionneurs est assurée directement par le Safetybus [SAF 05].

Grâce à la séparation stricte, établie par le Safetybus p, entre la communication Fail-safe et les tâches de commande standard ainsi que la communication standard, d'importantes exigences vont être transférées à l'utilisateur. Le but est de pouvoir modifier régulièrement les programmes et les fonctions dans la partie Standard d'un automate. Dans la technique de commande de sécurité, au contraire, il faut essayer de garder le plus longtemps possible l'état enregistré [SAF 05]. Grâce à la séparation entre l'automate de fonctionnement et la partie sécurité, on obtient une liberté rétroactive. Toute modification apportée dans la partie Fail-safe doit être documentée et peut entraîner une nouvelle homologation de la technique de commande de sécurité.

Profisafe [PRO 02] est la déclinaison sécurité de Profibus. L'un des critères fondamentaux en matière de développement de Profisafe était de continuer à utiliser tels quels les composants standard de communication Profibus, dont les câbles, les circuits intégrés, le protocole DP (*Decentralized Periphery*) etc., de sorte que les applications de sécurité puissent coexister sans conflits avec les applications standards.

Profisafe définit le raccordement d'équipements à sécurité intrinsèque (arrêts d'urgence, barrières immatérielles). Le domaine particulier de la sécurité peut ainsi bénéficier des multiples atouts d'une communication ouverte sur Profibus.

Un autre réseau qui possède une extension sécuritaire est le réseau AS-I. AS-I est un bus qui travaille uniquement au niveau capteur/actionneur [CIA 99]. Le système d'interface Actionneur Capteur AS-i standard se compose d'un maître, d'un élément de réseau (bus) et d'esclaves. Le maître est l'élément de liaison entre l'hôte (automate programmable) et les périphériques. Il prend en charge suivant un protocole strict le transfert des données et la gestion du système (réception des nouveaux esclaves, consultation de la configuration). La transmission des données s'effectue de manière strictement cyclique (*polling*) selon le principe maître-esclave.

Le concept "Safety at Work" permet de raccorder directement au bus AS-I standard des éléments de sécurité. Ainsi, il est possible d'envoyer par le même câble AS-I des données d'Entrées / Sorties ayant un rapport ou non avec la sécurité. A cet effet, il existe un moniteur spécifique qui gère les esclaves dédiés à la sécurité. Les caractéristiques de sécurité exigées

sont respectées par l'envoi de données supplémentaires entre les esclaves et les moniteurs de sécurité.

3.1.3. Evaluation de la sûreté de fonctionnement d'un réseau de terrain

La présence d'un réseau de communication dans un système d'automatisation distribué fait en sorte qu'il y a interaction permanente entre le réseau et le reste des composants du système. Les aspects doivent alors être pris en compte avec un soin attentif [JUA 02].

Si les réseaux de terrains semblent être une meilleure solution pour l'amélioration de la sûreté de fonctionnement, ils peuvent être aussi un obstacle en regard de nouvelles défaillances introduites [CAU 03]. Le choix du réseau de terrain dans une application avec une architecture spécifique doit être basé sur les moyens de sûreté de fonctionnement afin de prédire, éliminer ou tolérer les fautes identifiées durant la phase de conception.

Le canal de communication est souvent modélisé comme une ligne de transmission, c'est-à-dire un élément physique induisant un retard constant, dépendant des propriétés structurelles de la ligne. Cette description devient plus complexe lorsque le système est commandé à travers un réseau de terrain utilisé par de multiples utilisateurs. Dans ce cas, le retard induit ne dépend plus seulement d'éléments physiques mais aussi et surtout des algorithmes mis en place pour la gestion du trafic sur le réseau et le codage de l'information.

Les difficultés de l'évaluation émanent des contraintes dues au réseau telles que les caractéristiques temporelles.

Les aspects relatifs aux caractéristiques temporelles se manifestent par la perte de trames ou encore une partie de cette trame, par la corruption de ces trames, ou par l'ordre de leur arrivée qui peut être différent de celui de leur émission.

3.2. Les tests dans les systèmes instrumentés de sécurité

Les normes et directives en matière de sécurité imposent de vérifier régulièrement l'état de fonctionnement des éléments constituant la chaîne de sécurité. Le niveau de SIL attribué à un SIS est calculé en prévoyant des tests périodiques sur les différents éléments qui composent le système.

Les normes mentionnent clairement les tests en ligne et hors ligne comme une condition pour maintenir le niveau de SIL pour les systèmes de sécurité.

Si toutes les défaillances étaient détectées, il ne serait pas nécessaire de vérifier périodiquement les éléments entrant dans la composition d'un SIS.

Le problème posé parfois est celui de la périodicité de ces tests et la planification des arrêts des procédés pour maintenance qui deviennent de moins en moins fréquents. En effet, il paraît déraisonnable d'interrompre délibérément la production dans un procédé pour tester une vanne qui ne sera peut-être jamais sollicitée. Du coup, dans certains cas, il faut parfois attendre six ans pour avoir l'occasion de tester une vanne d'arrêt hors ligne [GRU 98].

3.2.1. La fonction test et les inspections visuelles (hors ligne)

Le diagnostic (test en ligne) et les inspections visuelles sont des moyens très importants pour vérifier si un SIS est capable d'atteindre ses fonctions de sécurité et de révéler les défaillances qui entravent la mise en sécurité du procédé au moment où il y a une demande [LUN 07].

Le diagnostic est un moyen de détection en ligne des déviations, des dégradations et des divergences et il est souvent réalisé par du matériel et du logiciel dédiés et implémentés dans les dispositifs (par exemple, les chiens de garde).

La norme définit le test périodique comme un essai effectué pour révéler des défauts non détectés dans un système instrumenté de sécurité, de telle sorte que, au besoin, le système puisse être restauré dans sa fonctionnalité de conception.

Les défaillances détectées par les tests de diagnostic sont appelées défaillances dangereuses détectées [CEI 00]. D'autres métriques sont aussi spécifiées par la norme. La figure suivante illustre la répartition des défaillances selon la norme.

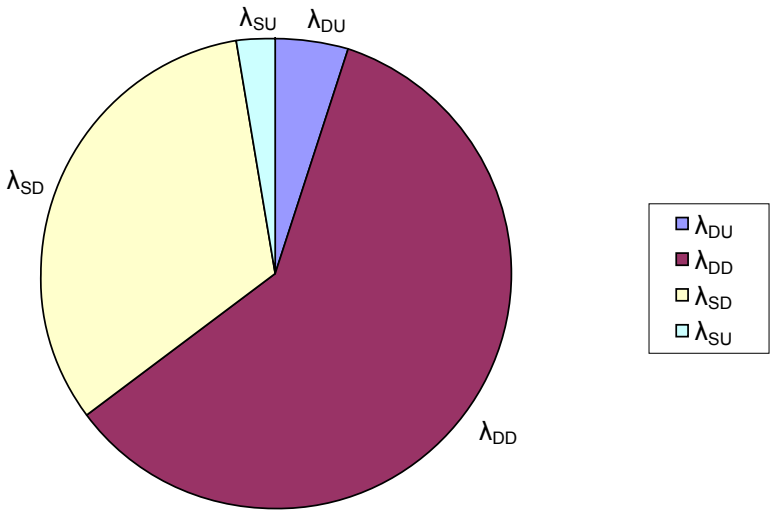


Figure 3. 3 : Proportion de défaillances selon un exemple illustré dans la norme [CEI 00]

λ_{DD} : Taux de défaillances dangereuses détectées,

λ_{DU} : Taux de défaillances dangereuses non détectées,

λ_{SD} : Taux de défaillances en sécurités détectées,

λ_{SU} : Taux de défaillances en sécurité non détectées.

La norme définit en outre, la proportion de défaillances en sécurité *SFF* (*Safe Failure Fraction*):

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

Cette métrique est un ratio de taux de défaillances et ne dépend pas du taux total de défaillances. Le résultat est un nombre entre zéro et un. Il est souhaitable d'avoir un *SFF* suffisamment important. Le *SFF* mesure la tendance de l'instrument à avoir des défaillances sûres ou détecter des défaillances dangereuses.

Le test de diagnostic souvent utilisé ne révèle pas toutes les défaillances et ne teste pas la fonction de sécurité complète.

D'après [ISA 96], les tests de diagnostic sont effectués périodiquement et automatiquement pour détecter les défauts latents cachés qui empêchent les SIS de répondre à une demande.

Il existe deux types de tests de diagnostics [LAM 02] :

- ✓ Les diagnostics de référence : comparaison par rapport à une valeur prédéterminée comme la mesure de la période (*watch dog*), le rebouclage de toutes les sorties sur une entrée,
- ✓ Les diagnostics par rapport à une opérationnelle

La norme CEI 61508 définit un taux de couverture de diagnostic pour les tests automatiques de diagnostic comme le rapport de taux de défaillances dangereuses détectées (par un test de diagnostic) sur le taux total des défaillances dangereuses (détectées et non détectées).

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{dangereuses}}$$

Ce taux de couverture de diagnostic reflète la qualité et l'étendue des tests automatiques en ligne. Sa grande valeur désigne la pertinence de traitement des défaillances détectées par leur détection. 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.

Les tests périodiques et les inspections visuelles sont réalisés alors qu'il y a arrêt de production. Ils sont destinés à révéler les défaillances non détectées par les tests en ligne. Ils sont réalisés à des intervalles réguliers. La durée de ces intervalles a une conséquence directe sur la probabilité de défaillance sur demande relative à la fonction de sécurité exécutée. Les défaillances révélées par ce type de tests sont appelées par la norme défaillances dangereuses détectées.

Dans plusieurs cas, les tests et les inspections visuelles sont exécutés manuellement. Cependant, les tests sont devenus automatiques avec les nouvelles technologies comme par exemple le test partiel de course de vanne [SUM 00b].

Les tests et les inspections comprennent généralement les six tâches suivantes [LUN 07] :

- ✓ L'ordonnancement par gestion au niveau de la maintenance. A un temps prédéfini, les tests ou les inspections sont soumis au système,
- ✓ La préparation, l'exécution et la restauration. Cette tâche relate de l'utilisation de la documentation nécessaire, de l'exécution de la procédure de test, la remise en place d'une façon adéquate des composants affectés à l'opération,
- ✓ Le report des défaillances vers le système qui gère la maintenance en mentionnant toutes les déviations et défaillances,
- ✓ L'analyse des défaillances. L'objectif de cette tâche est de comparer les performances relatives au SIS par rapport aux performances ciblées,
- ✓ L'implémentation de mesures de défense. Il est important de préparer et implémenter des moyens de corrections relatifs aux défaillances enregistrées,
- ✓ La validation et le perfectionnement continu. A des intervalles réguliers, il est important de revoir les procédures utilisées et faire des analyses à propos de l'exécution de ces procédures en regard des objectifs relatifs aux SIS consistant à maintenir leurs performances pendant l'exploitation et la maintenance.

3.2.2. L'avantage des tests dans les SIS

La tendance vers l'utilisation des instruments intelligents dans les applications de sécurité est motivée par la capacité qu'offre ce type d'instruments à être diagnostiqués en ligne mais aussi au pouvoir de validation en regard des conditions environnantes [NOB 04] [MAC 04].

Les tests périodiques assurent la détection des pannes cachées afin de maintenir la sécurité fonctionnelle prescrite.

L'impact des tests périodiques sur la fiabilité est montré dans la figure suivante :

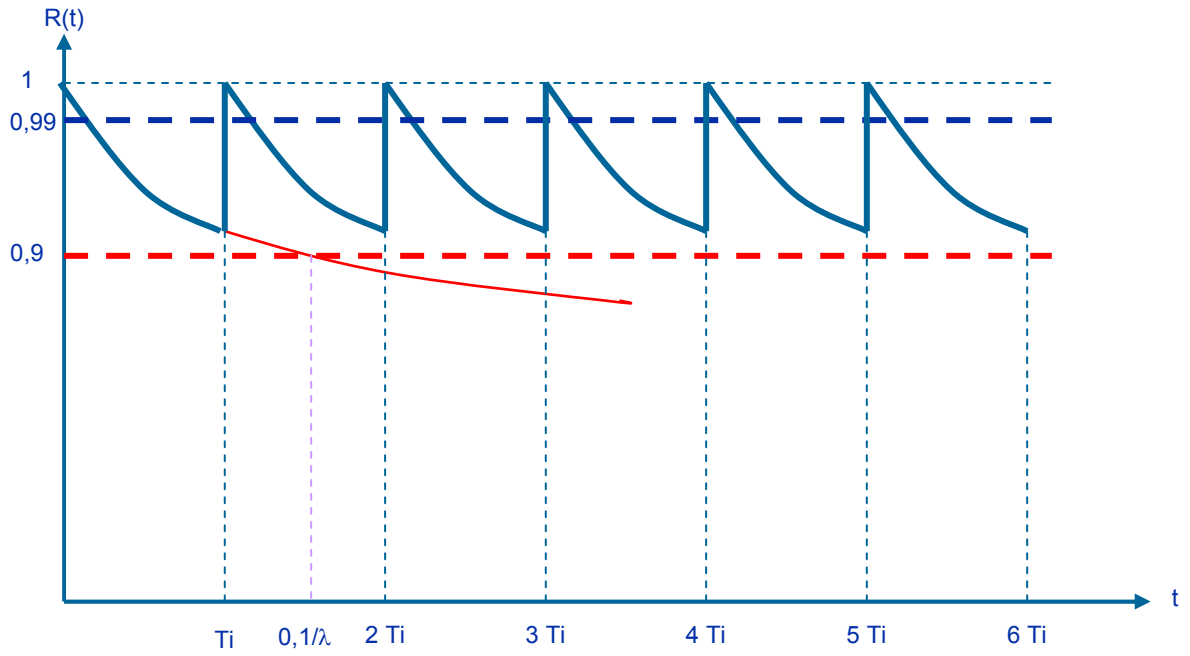


Figure 3.4 : Impact des tests périodiques sur la fiabilité

La figure 3.4 montre bien le rétablissement de la fiabilité du système après chaque test périodique et ainsi le niveau de SIL peut être maintenu comme le préconise la norme. La métrique R(t) exprime tout simplement l'inverse de la probabilité de défaillance sur demande PFD et l'on voit bien qu'en absence de tests périodiques, la valeur de R(t) se dégrade nettement et sort de la bande [0,9 0,99], par conséquent le SIL ne peut plus être maintenu à sa valeur.

Les tests dans les éléments finaux typiquement les vannes d'arrêt se concrétisent partiellement sur une partie de la course. Ces tests partiels peuvent être pratiqués à des périodes très rapprochées afin de permettre le maintien du niveau SIL au niveau initial. L'avantage de l'utilisation d'instruments intelligents est que la commande ne provient plus de l'automate programmable mais tout simplement de la vanne elle-même. Les capteurs dotés d'intelligence disposent aussi de moyens d'autotests en ligne permettant de diagnostiquer la nature des défaillances avec un taux de couverture propre à chaque instrument. Ils disposent aussi d'autres propriétés telles que la réaction au vieillissement prématuré, l'adaptation à l'usure réelle, la participation à l'intelligence globale du système…

Lorsque les dispositifs d'un système de contrôle sont distribués dans toute l'installation, il semble raisonnable d'examiner la possibilité de distribuer la détection associée et les tâches de diagnostic. Ces tâches visent à isoler les défauts de la boucle qui affectent les performances. [CHE 02] a utilisé le diagnostic distribué en mettant en évidence une certaine similitude avec

le concept de validation de [CLA 95] décrit dans le premier chapitre et qui vise à distribuer des tâches locales de détection et de diagnostic à des instruments (capteurs et actionneurs).

[WAN 00] introduit aussi le principe du diagnostic distribué en décrivant la différence qui peut exister entre un système et un système distribué. En effet, dans un système, un processeur central est nécessaire afin de recueillir tous les résultats des tests et de diagnostics sur le système. Toutefois, dans les systèmes distribués utilisant des réseaux de communication, il n'existe pas de processeur central et tous les processeurs sont utilisés séparément. Cette procédure permet le test et le diagnostic en ligne. Les tests peuvent être appliqués de manière asynchrone, c'est-à-dire un processeur peut toujours appliquer ses tests.

3.3. L'utilisation des instruments intelligents dans les SIS

Les performances globales obtenues en sécurité dépendent de tous les constituants de la boucle de sécurité y compris les instruments de terrain. Ainsi, les fonctions de sécurité sont allouées au dispositif de traitement mais aussi aux capteurs et aux actionneurs.

3.3.1. Test partiel de la course de vanne (PVST)

Les actionneurs constituent le maillon le plus faible de la boucle de sécurité [RAJ 05]. C'est pourquoi bon nombre de fabricants et chercheurs se sont penchés sur la question afin de proposer des solutions. Un cas particulier des actionneurs est celui des vannes utilisées dans les systèmes instrumentés de sécurité. Ces vannes sont considérées comme les composants les plus fragiles du fait qu'elles restent sans bouger pendant de longues périodes, et les obturateurs auront tendance à se coller.

Capteurs	Unités de traitement	Actionneurs
35 %	15 %	50 %

Tableau 3.2 : Proportion de défaillances relatives aux constituants d'un SIS [AUB 04]

Une solution proposée tant par les fabricants que les chercheurs consiste à réaliser des tests périodiques sur une partie de course de l'obturateur de la vanne ce qui est communément appelé PVST (*Partial Valve Stroke Testing* : Test Partiel de la Course de Vanne).

Le problème rencontré souvent dans les vannes est le blocage en fermeture ou en ouverture du fait qu'il s'agit de dispositifs statiques qualifiés de *dormants*. Ces éléments ne sont appelés à réagir qu'au moment où il y a une demande suite à un danger qui se présente. Malheureusement, du fait de la durée importante de la non réaction (leur mise en repos) de ces vannes, un certain nombre d'entre elles ne répond pas au moment opportun et elles restent coincées dans leur position de repos.

C'est pourquoi le PVST consiste à tester régulièrement les vannes sur un pourcentage de leur course (10 à 20%) afin de s'assurer que celles-ci ne resteront pas bloquées lorsqu'on en aura besoin. La vanne se trouve actionnée sur une partie de sa course pour tester sa fonctionnalité

sans interruption de la production. La proportion de 20 % de la course est choisie en se référant au principe de Pareto (règle des 80/20) [PAR 01], ce test à 20% permet de déceler 80% des défauts.

Le PVST a cependant des limites. Le test de course partielle ne garantit pas que la vanne fonctionnera lorsqu'elle sera sollicitée pour une fermeture complète. En effet, il se peut qu'il y ait un blocage au niveau de la nouvelle butée et donc que la vanne ne se ferme pas complètement mais uniquement à 20% de sa course.

L'élément qui détermine la position de la vanne est le positionneur de vanne. Il est doté d'intelligence. Il est monté sur des organes de réglage et détermine une position bien précise de la vanne par rapport au signal de commande (grandeur directrice élaborée par un microprocesseur). Il compare le signal de commande provenant d'un dispositif de réglage avec la course de l'organe de réglage et émet une pression d'air.

D'autres solutions alternatives au PVST consistent à utiliser une vanne de dérivation (*bypass*) autour des vannes d'arrêt ou prévoir une redondance. Ces solutions sont ou coûteuses ou potentiellement dangereuses [GRU 98]. En effet, le doublement du nombre de vannes augmente le coût de l'équipement de base, mais aussi les coûts de mains d'œuvre liés aux essais de maintenance puisque les tests périodiques portent sur un nombre plus élevé de vannes. En plus, les coûts de la tuyauterie supplémentaire pour les vannes de dérivation sont importants. Le danger peut provenir d'une vanne de dérivation qui ne peut remplacer la vanne d'arrêt au moment de test de celle-ci hors ligne.

3.3.2. Capteurs intelligents constituant de SIS

Le tableau 3.2 qui décrit la proportion des défaillances des dispositifs constituant un système instrumenté de sécurité montre bien que les dispositifs de terrain qu'ils soient capteurs ou actionneurs sont les plus vulnérables (avec un accroissement pour les actionneurs qui arrivent en premier lieu).

La question qui se pose concerne la justification de l'utilisation des capteurs intelligents comme éléments d'entrée des systèmes instrumentés de sécurité et sur leur contribution dans la dégradation ou l'amélioration des performances des SIS en matière de sécurité et de disponibilité.

[BIS 05] justifie l'utilisation des capteurs intelligents dans les applications sécuritaires par trois critères :

- ✓ La justification par rapport aux exigences au sujet du comportement des systèmes de sécurité,
- ✓ L'utilisation des normes et directives,
- ✓ La recherche des vulnérabilités connues du système.

Un ensemble d'attributs tel que la précision, le comportement à sûreté intégrée (*fail-safe*), le temps de réponse, entre autres, a pu être identifié pour un capteur intelligent. Toutes ces qualités sont exigées d'après [JON 01] dans les systèmes qui sont relatifs à des applications sécuritaires. D'ailleurs, la justification d'utilisation de capteurs intelligents fait partie d'une plus grande justification de sécurité pour un SIS par la satisfaction des contraintes et l'indépendance vis-à-vis des applications [BIS 05].

L'ensemble des fonctionnalités d'un capteur intelligent ne peut être utilisée dans des applications sécuritaires. En effet, les capteurs intelligents doivent être protégés en écriture afin d'interdire toute modification accidentelle à distance.

La crédibilité des informations fournies par le capteur doit être néanmoins améliorée. En effet, une seule information erronée peut conduire à la prise d'une mauvaise décision et mener à la défaillance d'un système avec des conséquences éventuellement désastreuses.

Le capteur intelligent se doit de délivrer une information validée afin de concourir à l'amélioration de la sécurité globale de l'application.

[PER 04] différencie la précision d'un capteur intelligent avec celle d'un capteur intelligent dans une application sécuritaire. En effet, certains capteurs intelligents relatifs à la sécurité certifiés selon la norme CEI 61508 possèdent des mécanismes de rétroaction permettant de comparer la sortie analogique avec la sortie digitale. D'autres ont placé un seuil pour le contrôle de dérive pour permettre d'améliorer la précision de la détection des défaillances dangereuses.

Le temps de réponse de sécurité est aussi différent d'après [PER 04] par rapport au temps de réponse du capteur. Le temps de réponse du capteur est la durée qui sépare le changement à l'entrée du capteur à la réponse en sa sortie. Le temps de réponse de sécurité est le temps de réponse du capteur auquel il faut ajouter le temps nécessaire pour effectuer les tests. Typiquement le temps de réponse de sécurité est de 1 à 5 secondes.

Une rétrospective paraît nécessaire pour sentir la différence qui peut exister pour l'emploi des capteurs dans les applications de sécurité. En effet, les SIS utilisent des capteurs conventionnels type capteurs TOR (tout ou rien) ou transmetteurs analogiques.

Les capteurs TOR se contentent de donner l'état de présence ou d'absence de l'information. Ce sont des capteurs qui envoient un signal binaire au moment où la grandeur physique à mesurer atteint un seuil prédéfini par l'utilisateur.

Pour les transmetteurs analogiques, la détection de la mesure provoque une variation du signal de sortie qui est transmis via la boucle 4-20 mA. Certains transmetteurs analogiques sont dotés de communication selon le protocole HART qui est superposé à la sortie analogique 4-20 mA.

Le système de communication basé sur HART (*Highway Adressable Remote Tranducer*) [CIA 99] n'est pas un réseau de terrain et le protocole n'est pas entièrement numérique, il permet la communication simultanée de données analogiques et numériques. Son intérêt est d'apporter les facilités de la communication numérique sans modifications des installations existantes, dans la mesure où il y a compatibilité avec les instruments en 4-20 mA.

Plusieurs transmetteurs analogiques qui utilisent la boucle 4-20 mA pour la détection des variables des processus, emploient le niveau de courant de la boucle 4-20 mA pour signaler des fautes internes détectées par des diagnostics automatiques dans le transmetteur [GOB 05].

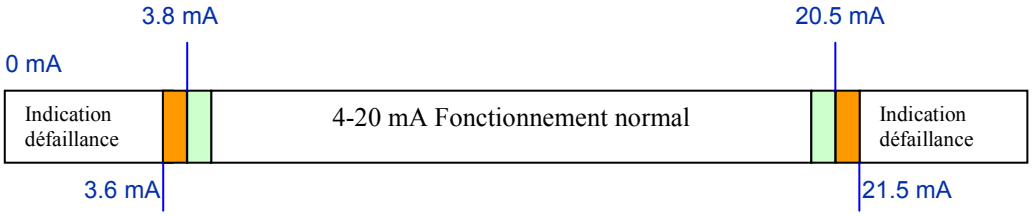


Figure 3.5 : Niveaux de courants utilisés pour l'indication des défaillances internes dans les transmetteurs [GOB 05]

L'utilisation des capteurs TOR dans les applications de sécurité pose un problème dans la mesure où ce sont des dispositifs qui vont réagir à des dépassements de seuils, et tant que ces seuils ne sont pas franchis, les fins de course de ces capteurs TOR ne vont pas être sollicitées. Ceci peut bien entendu mener à des situations dangereuses s'il y a franchissement et que le capteur TOR est en panne et ne pourra pas indiquer sa nouvelle position.

Au contraire, les transmetteurs analogiques sont mieux adaptés à ces situations par rapport aux capteurs TOR dans les applications de sécurité du fait qu'ils envoient en permanence leurs mesures à l'unité de traitement de telle façon que s'il y a interruption d'envoi de mesures, on sait qu'il y a forcément un problème au niveau de ces transmetteurs et la réaction peut être immédiate. La nature dynamique de ces transmetteurs permet facilement de dire si l'équipement fonctionne correctement.

Le problème qui peut persister avec ces transmetteurs analogiques est celui d'une part des autotests ou de la couverture des diagnostics qui sont préconisés par la norme CEI 61508 et également celui de la crédibilité des mesures envoyés par ces transmetteurs. On peut par exemple recevoir sans interruption des mesures pouvant caractériser la dynamique de ces transmetteurs mais comment quantifier le crédit que l'on peut accorder à ces mesures.

A notre avis, l'apport principal des instruments intelligents de terrain pour les applications sécuritaires va dans le sens de l'amélioration de la métrologie avec une précision accrue et une confiance allouée aux grandeurs mesurées, ce qui permettra une crédibilité sur les mesures. D'autre part, les autotests ne sont plus dirigés par l'unité centrale de traitement mais exécutés localement au plus près du procédé et le compte rendu peut être envoyé par l'utilisation de moyens de communications contemporains (réseaux de communication).

3.3.3. Le taux de déclenchement intempestif

L'autre mode de défaillance auquel les systèmes dédiés à la sécurité peuvent être confrontés est celui du déclenchement intempestif. Ce mode affecte plutôt la disponibilité que la sécurité.

Les arrêts intempestifs du système de sécurité provoqués sont parfois appelés fausses pannes ou pannes sans risque [GRU 98].

La norme CEI 61508 définit dans sa partie 4 au paragraphe 3.6.8. la défaillance en sécurité comme celle qui n'a pas la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction.

Une attention particulière doit être portée sur ce type de modes de défaillances qui ne sont pas véritablement considérées dans la norme [INA 07]. En effet, la norme ne traite que les défaillances dangereuses. Les formules données par la norme concernent uniquement ce type

de défaillances alors qu'un système instrumenté de sécurité peut subir deux modes de défaillances : les défaillances dangereuses et les défaillances en sécurité.

Ce paramètre est l'un des indicateurs fiabilistes des systèmes dédiés à la sécurité, il est souvent donné sous forme de probabilité de défaillances en sécurité PFS (*Probability of Failure to Safe*). Il est aussi exprimé par le taux d'arrêts intempestifs NTR (*Nuisance Trip Rate*) [GRU 98] exprimé en années et il représente le temps moyen entre deux déclenchements parasites.

Pour être considérée comme sûre, aucune défaillance d'un composant ni aucune condition de panne ne doit mener à un état de panne du système.

Dans un système dédié à la sécurité, les deux modes de défaillances doivent être pris en compte. La PFS doit être la plus petite possible. Là aussi, d'après [GRU 98], il faut se préoccuper des transmetteurs et des vannes qui présentent des NTR nettement moins élevés que celui d'un automate programmable.

L'évaluation des systèmes instrumentés de sécurité est concernée par ces deux aspects indissociables pour une étude relative à la sécurité mais mutuellement exclusifs.

3.4. 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 deux premiers chapitres de cette thèse ont fait l'objet de description des systèmes d'automatisation à intelligence distribuée (SAID) composés essentiellement d'instruments intelligents autour d'un réseau de terrain et des systèmes instruments de sécurité. 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 3.3 et 3.4 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 terme d'architectures et en terme 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 [MKH 07][MEK 06][REV 05] génériques des instruments intelligents se résument comme suit : ✓ l'acquisition (mesure et conditionnement) ✓ la configuration (paramétrage et réglage) ✓ la validation (traitement et prise de décision) ✓ l'actionnement ✓ la communication	L'architecture fonctionnelle d'un système instrumenté de sécurité [LUN 06] qui est composée d'un ensemble de fonctions instrumentées de sécurité est constituée de **trois** fonctionnalités de base : ✓ la **détection** (ou la mesure), ✓ la configuration est interdite l'architecture d'un SIS est figée, ✓ la **décision** ✓ l'**actionnement** ✓ la communication n'est pas réellement prise en compte dans la norme (seulement quelques recommandations)
Architecture matérielle	Les constituants des SAID sont [CON 99] [VYA 03] : ✓ plusieurs unités de traitement ✓ des composants intelligents ✓ Un réseau de communication tel qu'un réseau de terrain	Les SIS se composent [CEI 03] [ISA96] : ✓ d'unités logiques ✓ de capteurs et d'éléments 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 [CON 99]. ✓ 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 et CEI 61511. ✓ Problème d'activation/désactivation selon les besoins de mode de sécurité (batch)

Tableau 3.3 : 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. [MAC 04] relate que les auto-tests dans les instruments intelligents permettent d'accroître la fraction des défaillances sûres de ces dispositifs. Le pouvoir de validation en 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 micro-programmés 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, 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.

Système	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 [CAM 99], ✓ Rapidité de traitement, grande flexibilité [LAF 93] [DAI 03], ✓ Réduction du coût et du câblage, Simplification de la maintenance [LEE 01], ✓ Structuration hybride [RIE 02], ✓ Reconfigurations offrant un caractère dynamique [BAR 03], ✓ Coopération des composants, systèmes répartis autour d'un réseau de communication, ✓ Contrôle/Commande des processus industriels	✓ Pas de spécification sur la distribution de l'architecture dans la norme, ✓ Traitement au niveau du système logique, ✓ ✓ ✓ Systèmes statiques (dormants) [GOB 05], ✓ Systèmes centralisés, ✓ Moyens de protection du personnel ou de l'environnement [CEI 03] [CEI 00], application à de nombreuses industries de processus, Surveillance des procédés [KNE 02], Partie des couches de protection pour les industries de transformation [WIE 02],
	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 [PAG 80][VIL88]. *R(t)* = P[entité non défaillante sur [0,t]] *A(t)* = P[entité non défaillante à l'instant t] M(t) = 1-P[entité non réparée sur [0,t]] $MTTF = \int_0^\infty R(t)dt$ [PAG 80] $MTTR = \int_0^\infty [1 - M(t)]dt$	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. *PFD(t) = 1-R(t)-PFS(t)* [GOB 98] *PFD(t) = 1-A(t)* [SMI 04] $PFD_{avg}=1/RRF$ [SUM98] *RFF* : Facteur de réduction de risque, PFD_{avg} : Probabilité moyenne de défaillance dangereuse. La norme [CEI00] 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. $PFD_{avg} = \frac{1}{T}\int_0^T PFD(t)dt$ [ISA96]
Evaluation de la sûreté de fonctionnement	Il existe des méthodes diverses pour l'évaluation de la Sdf de ce type de systèmes : ✓ approche dynamique [BAR 03] ✓ approche statique [CON 99]	La norme propose un certain nombre d'équations mathématiques pour la détermination de la $PFD_{avg}=1/RRF$ [SUM98]. L'évaluation est faite avec la technique des blocs diagrammes de fiabilité. D'autres techniques sont aussi répandues telle que l'approche markovienne [GOB 98][ZHA03].

Tableau 3.4 : Aspects relatifs à la sûreté de fonctionnement des SAID et des SIS

4. Méthodologie d'évaluation des systèmes instrumentés de sécurité à intelligence distribuée

4.1. Modélisation fonctionnelle et dysfonctionnelle

La modélisation de systèmes en vue d'une analyse de sûreté de fonctionnement doit comprendre tant la modélisation fonctionnelle que la modélisation dysfonctionnelle. La modélisation fonctionnelle est subordonnée à une analyse fonctionnelle du système qui utilise ces fonctions ainsi que leur organisation hiérarchique tandis que la modélisation dysfonctionnelle se rapporte généralement aux aspects de la sûreté de fonctionnement des systèmes, celle-ci (Annexe 1) étant souvent définie comme étant la science des défaillances. La modélisation fonctionnelle et dysfonctionnelle a pour objectif l'évaluation des performances en fonctionnement normal et en fonctionnement anormal.

A l'issue des travaux précédents [MKH 06a] [MKH 06b], la modélisation et l'analyse de la sûreté de fonctionnement d'instruments intelligents ont été élaborées avec un objectif d'améliorer les compréhensions du modèle de SAID. Les techniques de modélisation statiques permettent une validation du modèle sans tenir compte des aspects temporels. Les performances globales pour l'évaluation de ce type de systèmes pour des applications relatives à la sécurité doivent être déterminées avec une approche dynamique de modélisation tenant compte entre autres du caractère hybride de ce type de systèmes. En effet, les systèmes automatisés à intelligence distribuée (SAID) sont des systèmes hybrides disposant d'une dynamique continue et d'une dynamique discrète liée à la commande numérique et à l'existence d'événements discrets (défaillances, dépassements de seuils). Un système hybride est un système qui nécessite dans sa description la prise en compte de sa dynamique continue et de sa dynamique discrète. La dynamique continue est représentée par des variables continues, la dynamique discrète représente les changements d'états dus à l'occurrence d'événements. Ces deux aspects rendent la modélisation hybride indispensable [MED 06].

Les méthodes les plus adaptées à la modélisation et à l'analyse des systèmes dynamiques hybrides sont les modèles états transitions tels que les graphes d'états (les graphes de Markov et les automates) et les approches basées sur les réseaux de Petri [GRI 03] [SCH 04] [VIL 06].

Les méthodes de modélisation peuvent être classées selon deux aspects : l'aspect dysfonctionnel qui permet de décrire les défaillances et les réparations ainsi que le comportement du système en présence de dysfonctionnements, l'aspect fonctionnel qui s'intéresse au comportement des systèmes.

La séparation entre ces deux aspects est la plus grande cause de l'inefficacité des méthodes classiques de sûreté de fonctionnement concernant la fiabilité dynamique. Ces deux aspects doivent être intégrés dans un même modèle de fiabilité en respectant leur interaction [MKH 08b] [MED 06] [SCH 04].

4.1.1. Modélisation de l'aspect fonctionnel

Les automates font partie des moyens de modélisation des systèmes à événements discrets et sont l'un des formalismes états-transitions utilisés pour la description de ces systèmes.

Le point faible de ce formalisme est l'explosion combinatoire du nombre d'états du graphe. Pour éviter ce problème, dans le cas de la modélisation des systèmes complexes pouvant être découpés en sous-systèmes, il est possible de construire un modèle d'automate pour chacun d'eux et de les composer ensuite pour élaborer l'automate correspondant au système global.

Un autre formalisme très utilisé dans la modélisation fonctionnelle des systèmes à événements discrets et dans les études de sûreté de fonctionnement des systèmes dynamiques est celui des réseaux de Petri (Annexe 2). Ils sont caractérisés par une évolution asynchrone dans laquelle les transitions des composantes parallèles sont franchies les unes après les autres, et par une représentation explicite des synchronisations. Plusieurs extensions des réseaux de Petri ont été élaborées pour répondre à la modélisation des problèmes spécifiques. L'un des points forts des réseaux de Petri par rapport aux autres formalismes repose sur des fondements théoriques qui leur permettent de vérifier les propriétés générales d'un modèle (vivant, sans blocage ou borné, etc.,) ainsi que l'accessibilité de certains marquages.

4.1.2. Modélisation de l'aspect dysfonctionnel

La méthode des graphes de Markov est utilisée pour analyser et évaluer la sûreté de fonctionnement des systèmes réparables. La construction d'un graphe de Markov consiste à identifier les différents états du système (défaillants ou non défaillants) et à chercher comment passer d'un état à un autre lors d'un dysfonctionnement ou d'une réparation.

Les graphes de Markov souffrent de l'explosion du nombre des états [MED 06], car le processus de modélisation implique l'énumération de tous les états possibles et de toutes les transitions entre ces états. L'utilisation des réseaux de Petri stochastiques s'avère une alternative pour surmonter ce problème.

Les réseaux de Petri stochastiques [DAV 97] sont obtenus par l'association de durées de franchissement aléatoires aux transitions. Une extension nommée "réseaux de Petri stochastiques généralisés" existe permettant ainsi de prendre en compte les transitions immédiates sans délai.

4.1.3. Modélisation fonctionnelle et dysfonctionnelle à travers le langage Altarica

Le langage Altarica [GRI 98] a été crée par le Laboratoire Bordelais de Recherche Informatique (LaBRI) ; il permet de décrire à la fois le comportement d'un système dans le cas nominal et en présence de défaillances. C'est un langage formel simple, à la fois hiérarchique et compositionnel. Sa sémantique et sa syntaxe clairement définies lui permettent d'être couplé à différents outils de fiabilité et de validation comme Aralia [VIN 04], MocaRP ou encore de *model-checking*.

Le développement de modèles Altarica est supporté par Cecilia OCAS (Outil de Conception et d'Analyse Système) workshop de Dassault Aviation qui fournit un éditeur graphique de modèles et un gestionnaire de composants. De plus, cet outil intègre des fonctions de simulation interactive et de génération d'arbre de défaillance.

AltaRica est fondé sur la notion d'automate à contraintes. Chaque composant du système est appelé nœud (`node`). Un nœud possède un nom, des variables de deux types, celles d'état, internes et non visibles de l'extérieur, et celles de flux qui représentent l'interface du composant avec son environnement. Les valeurs que prennent ces variables expriment leur état de fonctionnement. Des transitions de la forme [garde, événement, mise à jour] décrivent les changements d'états sous l'effet d'événements, suivant certaines conditions, et avec des conséquences sur la valeur des variables d'état.

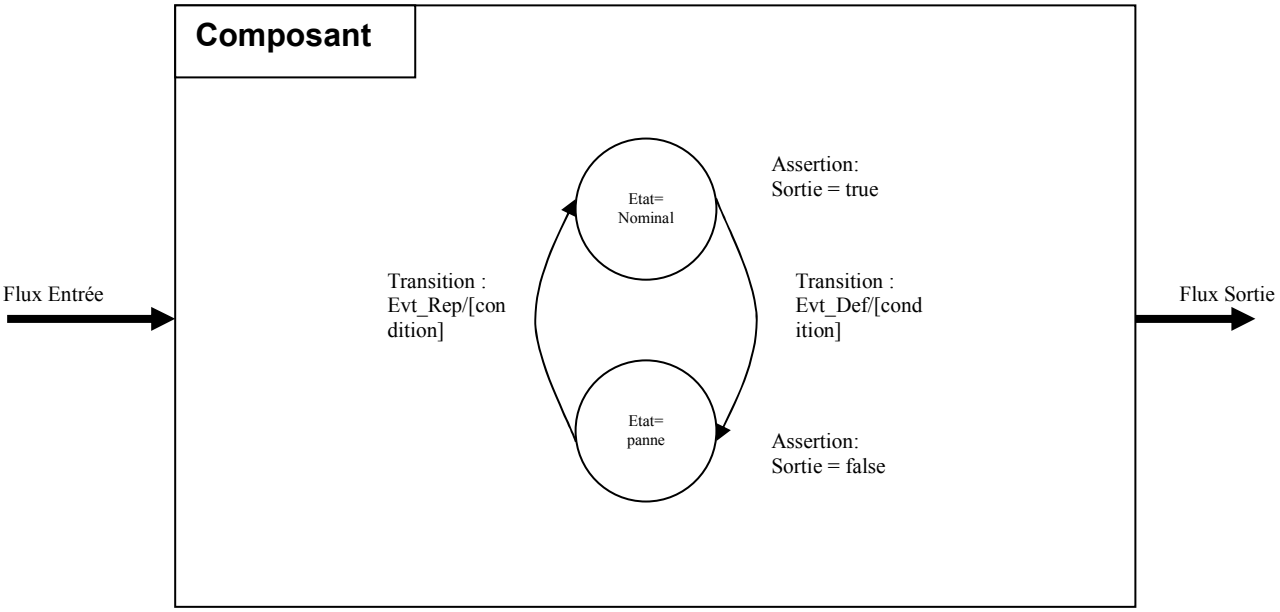


Figure 3.6 : Représentation d'un composant sous forme d'un automate

Les flux de sortie sont évalués en fonction de l'état actuel, et éventuellement en fonction des flux d'entrée par des assertions.

Les transitions définissent le passage d'un état à un autre. Une transition est franchie sur occurrence d'un événement et éventuellement en fonction de conditions portant sur les valeurs des flux d'entrée.

Ces concepts sont illustrés par l'exemple suivant. Le composant `mesure_p` a une variable d'entrée nommée `m_p` qui indique la présence d'une grandeur à l'entrée du composant et une variable de sortie `m1` qui indique la présence d'une mesure en sortie. La variable état indique l'état du composant, sa valeur est égale à `nominal` lorsqu'aucune défaillance ne s'est produite et à `hs` lorsque le composant ne peut plus transmettre de mesure. L'événement `panne` décrit une défaillance qui fait passer le composant dans l'état `hs`. La transition associée à cet événement ne peut se déclencher que si le composant est dans l'état nominal. L'assertion signifie que la valeur de la mesure en sortie est égale à la valeur de la grandeur en entrée si le composant est dans l'état nominal et sinon il n'y a pas de mesure en sortie.

```
node mesure_p
   state
    etat :{nominal,hs} ;
   flow
    m_p : bool : in ;
    m1 : bool : out;
   event
    panne;
   trans
    etat=nominal|-panne->etat:=hs;
   assert
     if  (etat=nominal)&  m1=  true  then  m_p=true
else m_p=false;
   init
     etat:=nominal;
edon
```

Figure 3.7 : Description de modélisation en code Altarica

Dans un modèle de système, les instances de nœud Altarica sont interconnectées par des assertions qui relient les flux d'entrée d'un composant avec les flux de sortie d'autres composants.

Le langage Altarica permet de décrire les comportements fonctionnel/dysfonctionnel de composants dans un formalisme à états/transitions. Il offre la possibilité de décrire formellement des comportements [MKH 07]. Sa faiblesse est qu'il n'intègre pas la notion de temps et la description de comportements dynamiques.

4.2. Analyse fonctionnelle et dysfonctionnelle

4.2.1. Analyse fonctionnelle

Une analyse fonctionnelle, en général, précède une étude de sûreté de fonctionnement. Une première analyse fonctionnelle permet de définir avec précision les limites matérielles du système étudié, 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.

4.2.1.1. La simulation

La simulation est une solution pour mener une vérification formelle des systèmes. Cette approche a pour avantage de pouvoir traiter des systèmes hybrides incorporant les aspects discrets et continus. Les performances temporelles de systèmes modélisés peuvent être mesurées. Cette approche ne garantit pas l'absence d'erreurs dans le modèle établi et ne permet pas de considérer toutes les évolutions.

4.2.1.2. Le Model Checking

La vérification de modèle ou le "*model checking*" [SCH 99] est une technique de vérification formelle qui est développée afin de permettre une vérification automatique et exhaustive de systèmes. Elle s'applique à une large classe de systèmes : protocoles de communication, réseaux téléphoniques, industrie manufacturière, systèmes embarqués, etc.

Cette technique est basée sur une description du système sous forme d'un automate. La génération consiste à générer des états possibles, d'examiner tous ces états, et d'identifier ceux qui sont en contradiction avec la propriété vérifiée.

La modélisation du système est basée sur des formalismes à états/transitions (réseaux de Petri, Altarica…), et les propriétés sont exprimées à l'aide de formules de logique temporelle (LTL…).

4.2.2. Analyse dysfonctionnelle

Les études de sécurité des systèmes sont souvent basées sur une analyse qualitative ayant pour objectif la détermination des scénarios aboutissant à l'occurrence de l'état redouté, suivie d'une analyse quantitative pour estimer la probabilité de leur apparition.

4.2.2.1. Limites des méthodes classiques

Les méthodes classiques de la sûreté de fonctionnement, comme celles présentées dans l'annexe 1 sont statiques. Ces méthodes basées sur la logique booléenne pour représenter le système étudié sont adaptées à des systèmes à configuration statique, c'est-à-dire des systèmes dont les relations fonctionnelles entre leurs composants restent figées.

Dans le cadre de nos travaux, la prise en compte d'aspects dynamiques dans les systèmes est essentielle. Cet aspect n'est pas pris en compte par les méthodes classiques de sûreté de fonctionnement ce qui les rend inappropriées pour ce type de systèmes. Par exemple la méthode des Arbres de Défaillance ne tient pas compte de l'ordre d'apparition des événements dans un scénario. En effet, une séquence d'événements peut conduire à un événement redouté alors que les mêmes événements se produisant dans un ordre différent ou à des dates différentes peuvent l'éviter. Le temps séparant deux événements n'est pas pris en compte dans la méthode des Arbres de Défaillance, les reconfigurations ne peuvent donc pas être représentées. Les défaillances temporaires ne sont pas non plus prises en compte. Plusieurs extensions des méthodes classiques ont été proposées afin d'élargir leurs champ d'application.

A titre d'exemple, le caractère intermittent des défaillances relatives à un réseau de communication les rendent difficilement modélisables par ce type de méthodes. En effet, il n'est pas facile d'intégrer la défaillance de transmission d'un réseau dans une étude [BAR 03]. L'autre problème réside dans le fait que les défaillances du réseau ne se produisent pas de la même façon et un événement peut être fatal dans un scénario et ne le pas l'être pendant un autre scénario.

Ces méthodes restent combinatoires et incapables de prendre en compte les changements d'états et les reconfigurations dans les scénarios redoutés.

4.2.2.2 Simulation de Monte Carlo

La simulation de Monte Carlo est une méthode numérique basée sur le tirage de nombres aléatoire [KER 02]. Elle permet d'estimer l'espérance mathématique d'une variable aléatoire qui est une fonction de plusieurs paramètres. Elle permet également d'estimer toute quantité, déterministe ou stochastique, dont la valeur a pu être associée à l'espérance mathématique d'une variable aléatoire qui n'est pas directement liée à la physique du problème étudié. Le principe consiste à étudier l'évolution d'un système en simulant un modèle générique représentant le comportement du système au cours d'un scénario (ou histoire).

La quantification de la grandeur recherchée (fiabilité ou probabilité d'apparition d'un événement redouté) est basée sur l'étude d'un certain nombre de scénarios différents, permettant d'extraire des résultats statistiques.

L'avantage de ce type d'approche est l'insensibilité par rapport à la complexité et la taille des systèmes modélisés [SCH 04].

Le temps de calcul reste un inconvénient pour cette méthode. En effet, dans le cas de modèles régis par des événements rares (cas typique des applications sécuritaires), la durée d'une histoire peut être excessivement longue et de plus un nombre non négligeable d'histoires est demandé pour voir apparaître l'événement redouté. De nombreuses techniques d'accélération de la simulation permettent de réduire ces temps de calcul. Elles sont basées sur la diminution de la complexité du modèle ou par la réduction du nombre de scénarios à simuler favorisant ainsi l'apparition des événements rares [GAR 98].

4.3. Description de la méthodologie

La méthodologie utilisée pour l'étude des systèmes instrumentés de sécurité 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.

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 [JUA 95]. 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 [MAL 94].

La modélisation est traitée sous la forme d'une approche stochastique utilisant les SAN (*Stochastic Activity Network*). Les SAN sont un formalisme de modélisation puissant et sont une extension des réseaux de Petri stochastiques [MOV 84]. Le haut niveau de constructions de modèles est offert par les "portes d'entrée" et les "portes de sortie" qui permettent des commandes spécifiques dans l'exécution du réseau et permettent aussi des constructions hiérarchiques pour le modèle. Les modèles composés sont basés sur des sous-modèles plus simples qui peuvent être développés indépendamment et joints à d'autres sous-modèles. L'outil utilisé pour les SAN est Möbius [DEA 02].

Dans cette méthodologie, parallèlement aux modèles fonctionnels, les modèles dysfonctionnels sont développés en même temps en exprimant les différents modes de défaillances relatifs aux différents composants. Ainsi, les modèles fonctionnels et dysfonctionnels seront intégrés dans un seul modèle.

La jonction des différents composants permet la construction de tous les sous-modèles et constitue l'étape ultime de la modélisation.

L'étape suivante consiste à spécifier les critères d'évaluation de la sûreté de fonctionnement. Les performances de sécurité ou de disponibilité s'expriment par la probabilité de se trouver dans un état dangereux (PFD) ou dans un état de repli intempestif (PFS). Cette quantification est rendue possible par la connaissance du taux de défaillance, du taux de couverture de chaque composant, ainsi que de l'architecture du système.

Les modèles sont ensuite analysés par simulation de Monte Carlo.

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.

5. Modèles de base des constituants des SISID

L'approche que nous proposons consiste à élaborer un modèle de base en réseaux de Petri sur lequel s'appuiera l'analyse quantitative qui permettra de déterminer les performances en terme de sécurité des systèmes instrumentés de sécurité à intelligence distribuée (SISID). Le modèle est composé d'une partie fonctionnelle spécifiant le comportement du système et

d'une partie dysfonctionnelle dans laquelle est représentée l'occurrence de défaillances qui peuvent affecter le système et le mettre en état de panne.

L'architecture fonctionnelle est indépendante de l'architecture matérielle. Les composants de l'architecture matérielle susceptibles de tomber en panne sont le capteur, l'automate et l'actionneur.

L'interaction entre la partie fonctionnelle et la partie dysfonctionnelle est ensuite incorporée pour traduire le comportement global du système en présence de défaillances.

Le formalisme des réseaux de Petri se prête bien à la modélisation comportementale de ce type de système. Ce formalisme offre la possibilité d'intégrer les défaillances, support d'une analyse quantitative.

5.1. Modèle d'un capteur défaillant

Dans le modèle d'un capteur défaillant à base de réseau de Petri stochastique, le changement d'état d'un état de fonctionnement normal à un état de panne est assujetti au franchissement d'une transition stochastique. Par hypothèse, des distributions de loi exponentielle sont associées aux transitions stochastiques.

L'interaction entre le modèle fonctionnel et le modèle dysfonctionnel est régie par des transitions immédiates (δ).

Un modèle de capteur défaillant est présenté en figure 3.8. Dans ce modèle, la place P1 représente l'opération effectuée par le capteur (mesure par exemple). L'état du capteur est représenté par les places OK et KO représentant respectivement l'état de marche et l'état de panne. La partie fonctionnelle est décrite par les places P1, P2 et la transition T1. Les actions et opérations qui y sont associées sont relatives aux spécificités du capteur.

La place D représente un danger potentiel, cette place est marquée s'il y a occurrence de la défaillance par franchissement de la transition stochastique. A ce moment, on retire le jeton de la partie fonctionnelle et le marquage simultané des places OK et P1 permet le franchissement de la transition immédiate et le capteur se trouve dans un état de dysfonctionnement.

Sur cet exemple simple, l'étude de performances concernant la sûreté de fonctionnement consiste en une mesure quantitative de la probabilité d'être à un instant t dans la place D [SCH 04].

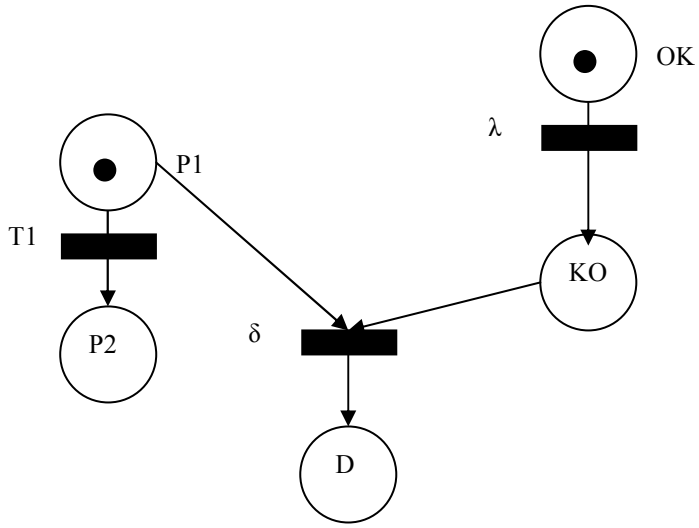


Figure 3.8 : Modèle d'un capteur défaillant

5.2. Modélisation du système complet

Le modèle complet est traité dans un premier temps sans redondance et sans introduction d'intelligence dans les dispositifs de terrain qui sont le capteur et l'actionneur.

Dans ce modèle (figure 3.9), deux parties sont bien distinguées : la partie fonctionnelle et la partie dysfonctionnelle. Le réseau de Petri composé des places P1, P2, P3, P4, P5, P6 et P7 modélise l'architecture fonctionnelle de l'automate. A ces places, sont associées des actions ou opérations non décrites ici. Des événements sont associés aux transitions T1, T2, T3, T4, T5, T6 et T7 dont les franchissements permettent à la fonction de passer d'une opération à une autre.

La place OK représente l'état de marche de l'automate. Le franchissement de la transition T8 traduit l'occurrence d'une défaillance non détectée. Cette transition est associée à un taux de défaillance λ_{aut} relatif à l'automate. Le marquage de la place P5 (autotest de l'automate) valide la transition immédiate et les défaillances se partagent en défaillances détectées par le test de diagnostic ou non détectées et ceci suivant un taux de couverture de diagnostic CD. Le marquage de la place P9 est synonyme de la situation de l'automate dans un état sûr qu'il peut quitter après restauration à laquelle on attribue une durée déterministe appelée durée de restauration.

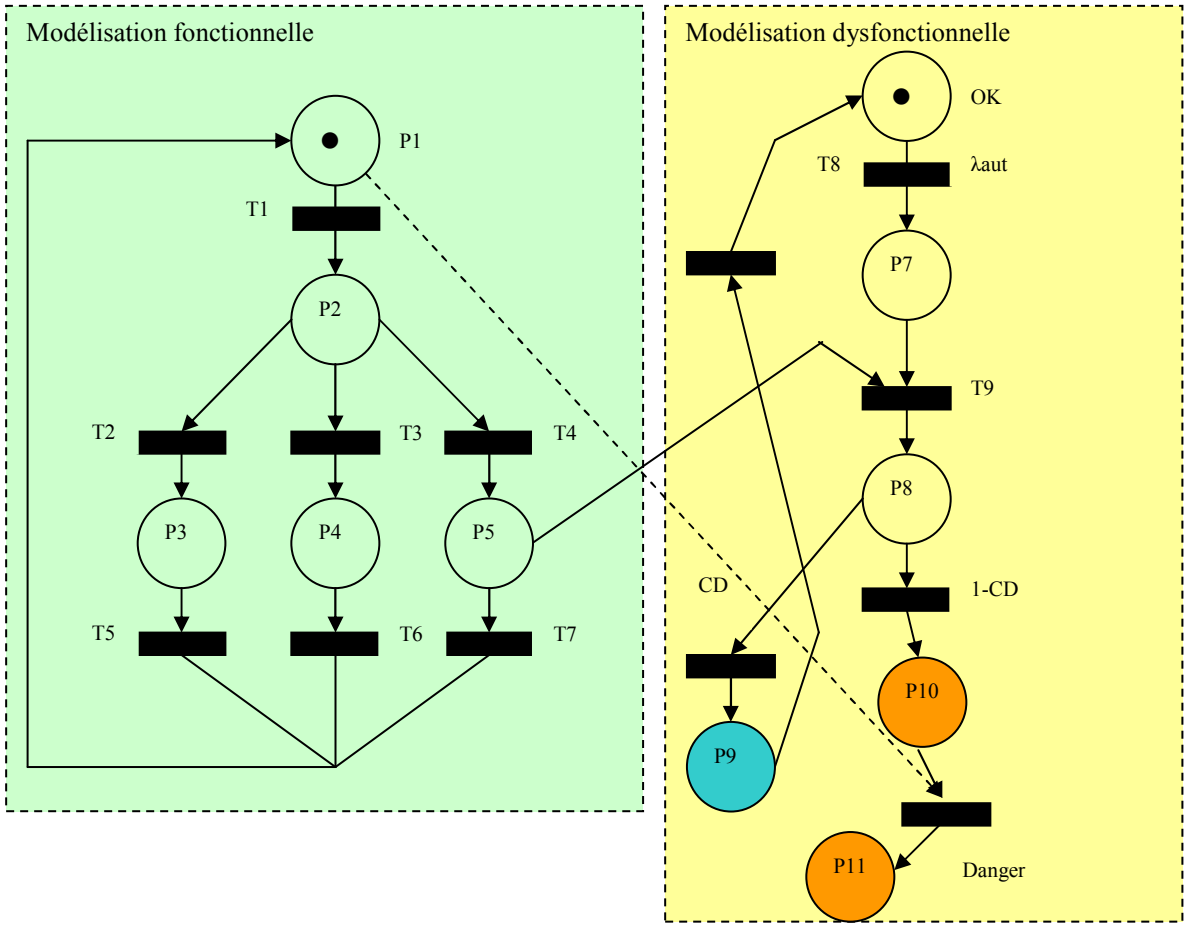


Figure 3.9 : Modélisation fonctionnelle/dysfonctionnelle de l'automate

Sur une défaillance de l'automate, la marque du réseau de Petri relatif à la partie fonctionnelle est récupérée afin de bloquer son évolution et un jeton est mis dans la place P11 (Danger) pour traduire un état de panne de l'automate. Le jeton doit être retirer de la partie fonctionnelle là où il se trouve si la place P10 est marquée. Un mécanisme de récupération de jeton est effectué sur toutes les places de la partie fonctionnelle.

Dans la figure 3.9, la partie fonctionnelle est décrite par l'ensemble des places et des transitions allant de P1 à P7 respectivement de T1 à T7. La présence du jeton dans la partie gauche reflète le bon fonctionnement de l'automate et tout dysfonctionnement entraîne systématiquement un marquage nul dans toutes les places de cette partie. 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.

La politique de test est décrite par le réseau de la figure 3.10. Dans cette figure, trois places Tc (test capteur), Tv (test actionneur) et Ta (test automate) sont ajoutées au modèle fonctionnel. La présence d'un jeton dans l'une de ces places traduit l'entité qui subit le test de diagnostic de la part de l'automate qui dispose d'une gestion centralisée des autotests des différents dispositifs avec des taux de couverture de diagnostic propres à chaque dispositif.

Dans cet exemple, le jeton se trouve initialement dans la place Tc relative au test du capteur. Ensuite le jeton est récupéré par la place P1 et se trouve de nouveau dans la place P2 après

franchissement de la transition déterministe T1 (Temporisation) et récupéré par la place Tv (test actionneur). Après franchissement de la transition T3, cette fois-ci, c'est la place Ta (test automate) qui récupère le jeton et cycliquement et suivant les périodes synchronisées par la temporisation, tous les dispositifs peuvent être testés et le cycle peut recommencer à nouveau.

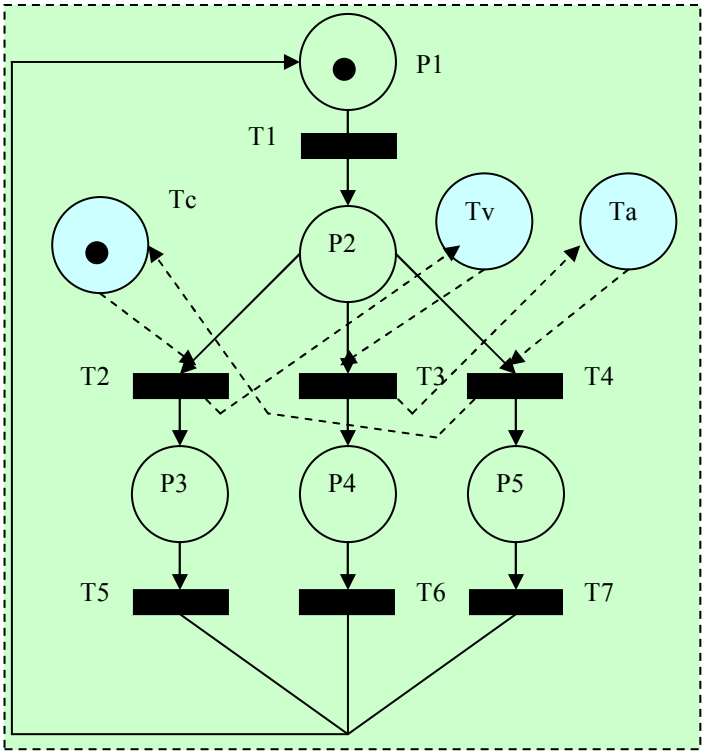


Figure 3.10 : Politique de test de l'automate

Les modèles du capteur et de l'actionneur sont identiques. Les transitions stochastiques traduisent l'occurrence de défaillances dans le cas où elles sont franchies.

Le modèle du capteur est donné dans la figure 3.11.

La place Tc attend un ordre de test qui provient de l'automate, le capteur dans l'état de marche OK passe dans l'état de défaillances non détectées DND et suite à la présence de jeton dans la place Tc qui est une place partagée avec le modèle de l'automate, les défaillances seront non détectées ou révélées avec un taux de couverture de diagnostic DC compris entre 0 et 100%. Une restauration du système est possible lorsque la place "Sur" est marquée reflétant ainsi le mode de défaillances sûres du capteur. Ceci avec une durée de restauration SD.

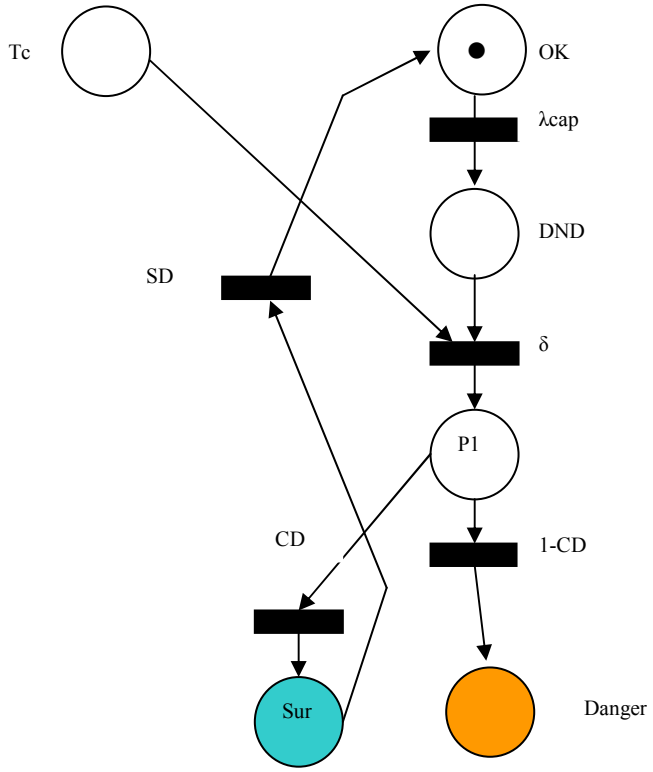


Figure 3.11 : Modèle du capteur.

5.3. Prise en compte de la redondance de quelques dispositifs

Dans ce modèle, la redondance de dispositifs de terrain (capteurs et actionneurs) est réalisée à des fins de tolérance aux fautes et pour l'amélioration des indicateurs de performances de la sûreté de fonctionnement.

Il s'agit d'utiliser une redondance matérielle active de type 1oo2. Les deux capteurs fonctionnent simultanément et la défaillance de l'un mène vers un état dégradé. Les deux actionneurs aussi sont tous les deux prêts à être actionnés et toute défaillance de l'un n'entraîne pas forcément la défaillance du système. Bien entendu, il s'agit de défaillances dangereuses, par contre toute défaillance sûre entraîne forcément l'arrêt du système.

La figure 3.12 illustre le modèle d'un capteur avec une redondance active 1oo2 :

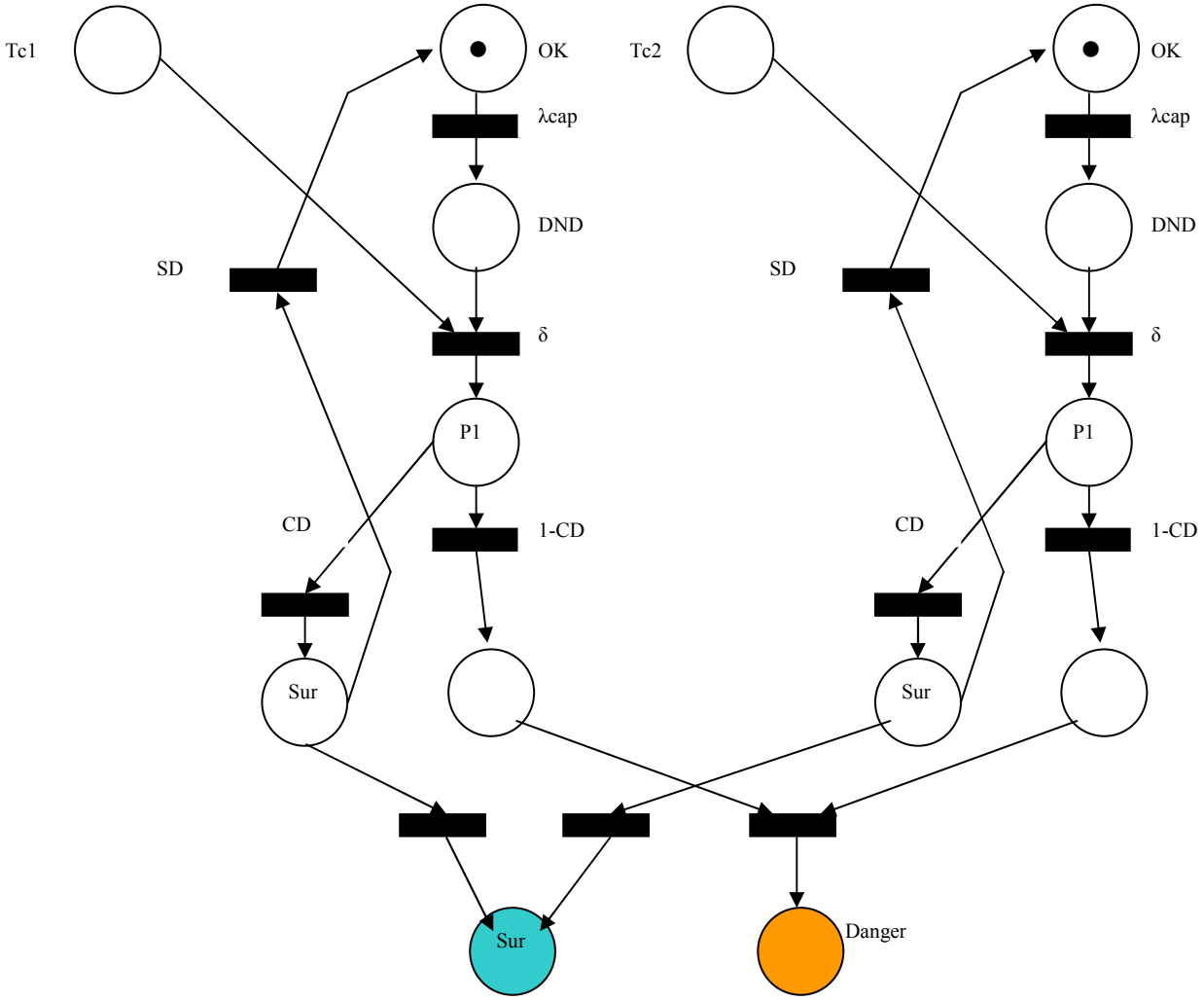


Figure 3.12 : Capteur avec redondance active 1oo2

Il faut noter que les places Tc1 et Tc2 ne sont pas identiques. En effet, le modèle fonctionnel de l'automate va subir quelques changements afin de prendre en compte les autotests du second capteur et du second actionneur.

5.4. Modèle d'un instrument intelligent

Dans ce modèle, contrairement au modèle classique, les autotests sont gérés localement et les différentes fonctionnalités sont traitées. Le modèle comprend une partie fonctionnelle et une partie dysfonctionnelle. La partie fonctionnelle décrit les opérations effectuées par l'instrument lorsqu'il est dans un état normal tandis que la partie dysfonctionnelle construite à l'aide de réseaux de Petri stochastiques représente des défaillances et permet d'effectuer les mesures de performance relatives à la sûreté de fonctionnement.

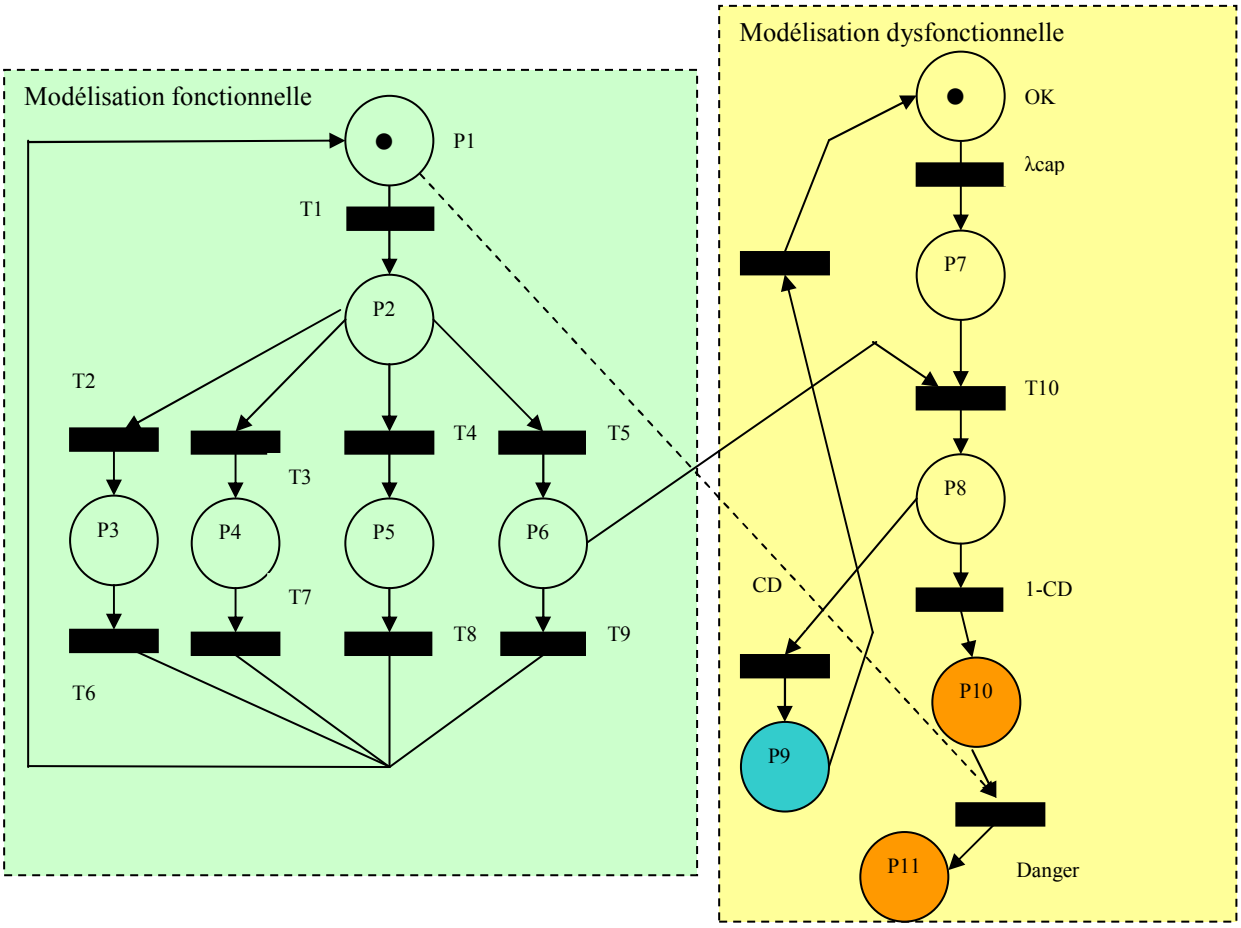


Figure 3.13 : Modèle d'un instrument intelligent

La partie fonctionnelle représente l'ensemble des fonctionnalités de l'architecture fonctionnelle d'un instrument intelligent à l'exception de la configuration. En effet, celle-ci ne peut être autorisée dans un contexte sécuritaire [MAC 04] puisque les informations qui concernent les paramètres et les réglages sont figées.

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. Les opérations associées aux places ne sont pas détaillées et elles couvrent les fonctionnalités propres de l'instrument intelligent. L'interaction entre les modèles fonctionnel et dysfonctionnel est représentée à l'aide de transitions immédiates.

Selon la nature du dispositif, les fonctionnalités vont différer. Les places allant de P3 à P6 vont décrire soit un capteur intelligent ou un actionneur intelligent.

Le modèle présenté en figure 3.13 est un modèle générique dans lequel le marquage n'est pas autorisé non plus dans la partie fonctionnelle lorsqu'un dysfonctionnement a lieu dans l'instrument concerné.

Notons que pour le modèle décrit auparavant (figure 3.13), le niveau d'intelligence incorporé dans les différents dispositifs est le niveau 2 (cf., chapitre 1). En effet, les procédures d'autotests et de diagnostic délocalisées au niveau des capteurs et actionneurs procurent de l'intelligence à ces dispositifs mais pas dans le sens le plus large (niveau 3). Dans le chapitre

4, la contribution de ce niveau d'intelligence vis-à-vis du niveau de sécurité sera élucidée quantitativement.

Le niveau d'intelligence le plus élevé (niveau 3) d'après notre classification requiert une coopération au niveau système entre les différents dispositifs de sécurité. Autres l'autotest et le diagnostic embarqué, des procédures de validation et prise de décision sont implantées en vue de l'amélioration de la sûreté de fonctionnement du système global. Le diagnostic distribué peut être aussi employé dans le cas où le système dispose d'architecture répartie favorisant le dialogue et l'échange d'informations entre les différents éléments de sécurité. Un exemple dans le chapitre 4 met en évidence quelques aspects de ce niveau d'intelligence.

6. Conclusion

La notion de sécurité intelligente est sujette à équivoque, et il ne suffit pas de disposer de moyens de calculs aussi sophistiqués dans les dispositifs qui constituent les systèmes instrumentés de sécurité pour qualifier ces systèmes de *"smart SIS"*. Encore faut-il que ces dispositifs s'accréditent de fonctionnalités inhérentes aux instruments intelligents.

A notre sens, l'intelligence se matérialise par l'existence de moyens de communication et de pouvoir d'octroi d'une crédibilité accrue aux informations au niveau des dispositifs de terrain qui se trouvent au plus près des processus physiques et ils disposent d'une certaine autonomie de gestion.

L'incorporation de l'intelligence dans les SIS mène vers cette sécurité intelligence manifestée par des SISID (*Systèmes Instrumentés de Sécurité à Intelligence Distribuée*) dont la méthodologie d'évaluation est proposée à la fin de ce chapitre. Cette méthodologie est basée essentiellement sur une structuration hiérarchique et modulaire. En effet un ensemble de modèles est présenté afin d'illustrer l'approche utilisée. Ces modèles peuvent être imbriqués pour décrire convenablement les systèmes modélisés. La vérification et l'analyse sont traitées par les réseaux de Petri stochastiques.

L'approche que nous proposons consiste à élaborer des modèles en réseaux de Petri stochastiques composés de partie fonctionnelle spécifiant le comportement des dispositifs et de partie dysfonctionnelle formalisant l'occurrence de défaillances de composants susceptibles de tomber en panne. Cette dernière partie permet d'effectuer les mesures de performances en termes de sécurité. Les deux parties sont ensuite intégrées pour reproduire le comportement global du système en présence de défaillances.

Les réseaux de Petri stochastiques sont très bien placés pour répondre à nos besoins de modélisation. Le franchissement d'une transition stochastique permet de représenter le changement de l'état d'un dispositif vers un état de défaillance. Nous supposons que les transitions stochastiques sont associées à des distributions de loi exponentielle.

L'utilisation du formalisme basé sur les réseaux de Petri permet l'inclusion de fonctionnalités de l'instrument intelligent dans la partie fonctionnelle de celui-ci à l'exception de la fonctionnalité configuration. L'intégration de ces fonctionnalités donne de l'autonomie de gestion locale, et par l'interaction avec la partie dysfonctionnelle, elle va avoir de l'influence sur les performances en sécurité.

Chapitre 4 : Mise en œuvre de l'évaluation de la sûreté de fonctionnement des SISID

Mise en œuvre de l'évaluation de la sûreté de fonctionnement des SISID

1. Introduction

Dans ce chapitre, la modélisation et l'évaluation des performances relatives à la sûreté de fonctionnement sont traitées avec des structures qui disposent d'intelligence dans les instruments composant les SIS. Dans un premier temps, nous proposons à titre de référence l'étude d'un système sans intelligence.

La méthodologie pour l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité à intelligence distribuée est mise en œuvre à travers la modélisation d'un système SIS sans redondance auquel nous introduisons des instruments intelligents et un réseau de communication. Une autre application concerne un exemple de procédé constitué d'un réservoir sous pression contenant un liquide inflammable volatil avec l'instrumentation associée. Les systèmes de sécurité concernés sont ceux qui obéissent aux directives décrites au chapitre 2 concernant les systèmes instrumentés de sécurité qui ne peuvent d'après la norme de sécurité CEI 61508 être critiques en introduisant eux mêmes des dangers potentiels aux processus concernés par la sécurité. Ce sont donc des systèmes qui réagissent à des demandes d'activation de la fonction de sécurité suite à des situations dangereuses induites par le procédé de fabrication.

Les taux de défaillance pour chaque composant sont supposés connus à priori, les évaluations vont concerner les interactions entre les différents composants du système. L'estimation du taux de défaillance global du système est assurée par la détermination des performances en sécurité et en se basant entre autres sur les taux de défaillances individuels des différents composants. Les métriques utilisées pour l'évaluation de la sûreté de fonctionnement des SISID se rapportent aux deux modes de défaillances cités par la norme : le mode de défaillance dangereux et le mode de défaillance en sécurité.

2. Approche de modélisation avec les réseaux d'activité stochastiques (SAN) et simulation de Monte Carlo

L'introduction de différentes variantes de réseau de Petri vise l'amélioration de la compréhension des modèles et l'augmentation du pouvoir de modélisation. C'est ainsi que ces réseaux de Petri ont évolué progressivement et plusieurs extensions ont été présentées pour répondre à des besoins spécifiques.

Parmi ces extensions, nous pouvons citer les réseaux de Petri stochastiques généralisés (RdPSG). Ce type de réseaux associe des transitions immédiates en plus des transitions temporisées. Une autre extension des RdP sont les *Stochastic Activity Networks* (SANs) qui ont été introduits par [MOV 84]. Ce formalisme de modélisation puissant est une extension des réseaux de Petri stochastiques; il dispose de fonctions de validation des transitions et de fonctions permettant le changement de marquage après le franchissement des transitions. Ceci se fait à travers des portes d'entrées et des portes de sorties.

2.1. Réseaux d'activités stochastiques

Les SAN (Stochastic Activity Network) sont une généralisation des réseaux de Petri stochastiques [MOV 84]. Les modèles offrent la possibilité de la concurrence, tolérance aux fautes et la représentation d'états dégradés dans un simple modèle. Les SAN sont plus flexibles que beaucoup d'autres extensions de RdP telles que les SPN et les GSPN (respectivement, les réseaux de Petri stochastiques et les réseaux de Petri stochastiques généralisés) [AZG 05]. Leur flexibilité est manifestée par leur conservation de toutes les capacités de modélisation des réseaux de Petri stochastiques par le biais d'activités stochastiques et les avantages des réseaux de Petri colorés par les structures associées à des places spécifiques appelées "*extended places*".

La structure des SAN est composée de places, de portes d'entrée (***Input Gates***), de portes de sorties (***Output Gates***) et d'activités. Les activités sont similaires aux transitions pour les RdP. Elles sont de deux types : temporisées ou instantanées. Les activités temporelles "*timed*" représentent les actions du système modélisé dont la durée a un impact sur la performance du système. Les activités instantanées "*Instantaneous Activity*" représentent les activités du système dont l'occurrence est immédiate. Les portes d'entrée et de sortie contrôlent la validation des activités et assurent des comparaisons ou tests (portes d'entrée) et des affectations (portes de sorties). Ces portent définissent aussi le marquage lorsque l'activité est achevée.

Une porte d'entrée dispose d'une sortie unique et de plusieurs entrées en quantité limitée. Elle représente un lien entre ces places et l'activité unique liée à la sortie de la porte.

Une porte de sortie dispose d'une entrée unique et de plusieurs sorties en quantité limitée. Elle caractérise le lien entre une activité unique en amont et les places en aval de la porte.

Les modèles SAN sont utilisés pour l'évaluation de systèmes appartenant à un large domaine et ils sont supportés par des outils de modélisation tels que UltraSAN [SAN 95] et Möbius [DEA 02].

Un des objectifs des SAN concerne l'évaluation des performances et de la sûreté de fonctionnement. L'évaluation de ces performances de la sûreté de fonctionnement est effectuée par la définition d'un ensemble de mesures dans le modèle.

Le développement de nos modèles est réalisé par l'outil Möbius qui est un support pour l'utilisation des SAN. Cet outil a montré sa puissance pour la modélisation et l'évaluation de la sûreté de fonctionnement de systèmes à événements discrets [AZG 05] [TAI 04], ceci a été concrétisé dans les travaux qui concernent la fiabilité des systèmes commandés en réseau en présence de fautes transitoires menés par [GHO 08].

2.2. La modélisation par l'outil Möbius

Le choix de cet outil a été motivé par le pouvoir d'expression facilitant ainsi la modélisation, sa conception hiérarchique qui permet la réutilisation de différents composants placés dans une bibliothèque et sa disposition de fonctions de récompense qui permettent d'élaborer l'évaluation des paramètres.

Möbius est un outil qui permet de modéliser le comportement des systèmes complexes. La première version est apparue en 2001 comme successeur de l'outil populaire et réussi d'UltraSAN. Bien que Möbius ait été à l'origine développé pour étudier la fiabilité, la disponibilité, et la performance des systèmes informatiques et systèmes liés par un réseau, son utilisation a augmenté rapidement. Il est maintenant employé pour une large gamme de systèmes à événement discret.

La large gamme de l'utilisation est rendue possible en raison de la flexibilité et de la puissance de l'outil Möbius. Ces qualités sont le fruit de son appui des formalismes multiples de modélisation à niveau élevé (réseaux de Petri, arbres de défaillances) et des techniques multiples de solutions permettant d'obtenir des estimations sur les variables recherchées (solutions numériques exactes ou solutions par simulation).

L'outil Möbius est conçu pour l'utilisation des réseaux de Petri stochastiques généralisés mais aussi dans le cas des réseaux de Petri colorés par l'introduction des structures permettant la prise en compte des jetons colorés. Cet outil est bien structuré et permet la modélisation hiérarchique et l'utilisation des entiers et des réels dans la composition des jetons. La programmation se fait en C++.

La solution calculée pour une variable de récompense s'appelle un résultat. Puisque la variable de récompense est une variable aléatoire, le résultat est exprimé comme la caractéristique d'une variable aléatoire. Ceci peut être, par exemple, la moyenne ou la variance. Le résultat peut également être l'intervalle de confiance.

Les résultats estimant les variables recherchées peuvent être donnés par un calcul numérique exact ou bien par simulation. Cette dernière est utilisée pour tous les modèles conçus dans Möbius.

De plus, *Möbius* est un outil particulièrement adapté aux simulations de Monte Carlo sur la base d'une simulation à événements discrets.

2.3. Simulation de Monte Carlo

Lorsque les activités disposent de lois de probabilités avec des taux de transitions qui ne sont pas constants, une solution de simulation peut être obtenue généralement et remplace ainsi la solution analytique qui reste restrictive aux cas où les taux de transitions sont constants.

La simulation de Monte Carlo se place comme une alternative dans les cas où des solutions analytiques ne sont pas réalisables. Le couplage de cette simulation de Monte Carlo avec les réseaux de Petri offre de la souplesse d'utilisation et un grand pouvoir de modélisation.

D'une manière générale, une simulation de Monte Carlo consiste à construire un modèle représentatif du comportement du système et à analyser l'évolution de ce dernier, à partir d'un grand nombre d'expériences. A chaque expérience, le comportement du modèle simulé est différent ; ces différences sont explicitement liées à la nature stochastique des processus relatifs à chaque entité du système.

On simule ainsi le comportement fonctionnel et dysfonctionnel du système en suivant son évolution sur une durée préfixée T qui constitue ce qu'on appelle une histoire (expérience). On réitère un grand nombre de fois N une telle histoire en partant chaque fois des mêmes conditions initiales et en conservant en mémoire les données numériques obtenues (présence ou absence de jeton(s) dans telle ou telle place…). Au terme de ces N histoires, on exploite d'une manière statistique l'ensemble des données accumulées pour déterminer les estimations désirées.

La quantification des probabilités cherchées est basée sur l'étude de plusieurs scénarios différents qui permettent d'avoir au final des résultats statistiques.

L'estimation de la probabilité d'un événement dangereux peut être effectuée par l'utilisation d'un estimateur binaire associé à cette probabilité qui permet une incrémentation d'une unité d'un compteur pour chaque histoire. L'estimation de la probabilité est déduite par le rapport entre le nombre d'histoires où il y a occurrence de l'événement dangereux et le nombre total des histoires [LAB 02].

Dans le cadre de la détermination des performances en terme de sécurité pour des systèmes instrumentés de sécurité, la procédure suivie dans la simulation consiste à obtenir dans un premier temps pour chaque expérience réalisée un ensemble de valeurs caractérisant les paramètres de défaillances dangereuses et défaillances sûres. Dans un second temps, la valeur moyenne de chacun de ces paramètres pour l'ensemble des histoires est estimée. Le nombre d'expériences doit être suffisamment grand pour obtenir des résultats d'un niveau de confiance acceptable.

3. Modèle d'un SIS classique à architecture 1oo1

3.1. Architecture 1oo1 d'un SIS

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.

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 [CEI 00].

Dans le cas de l'architecture 1oo1, toute défaillance dangereuse entraîne la défaillance du système. Une défaillance sûre se traduit par la mise dans une position de repli prédéfinie ou par une exécution intempestive de la fonction de sécurité.

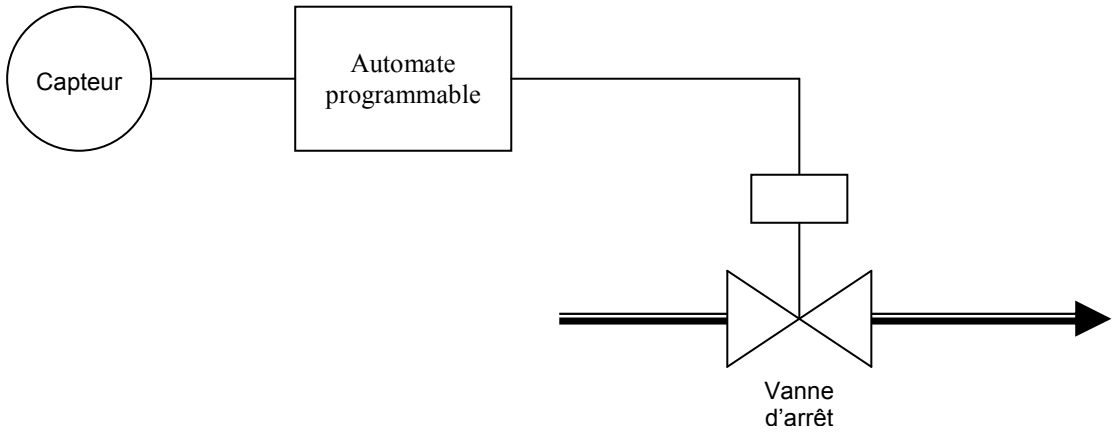


Figure 4.1 : Système instrumenté de sécurité (Architecture 1oo1)

3.2. Modèle SAN du SIS

Compte tenu du mode de fonctionnement du canal et des hypothèses émises dans la norme, un modèle SAN est conçu sans utiliser la hiérarchie dans la composition. La figure 4.2 montre une description du modèle d'un SIS à architecture 1oo1 sous Möbius.

Pour pouvoir assurer son fonctionnement, le SIS est composé d' :

- un capteur qui mesure l'état du processus,
- une unité logique qui exécute la fonction de sécurité (automate programmable par exemple),
- un élément final qui met en œuvre l'action physique nécessaire pour obtenir un état de sécurité.

Différentes défaillances peuvent apparaître sur les composants. Ces défaillances sont qualifiées par la norme CEI 61511 de deux types :

- défaillances dangereuses, qui ont la potentialité de mettre le système instrumenté de sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction,
- défaillances en sécurité, qui n'ont pas la potentialité de mettre le système instrumenté de sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction.

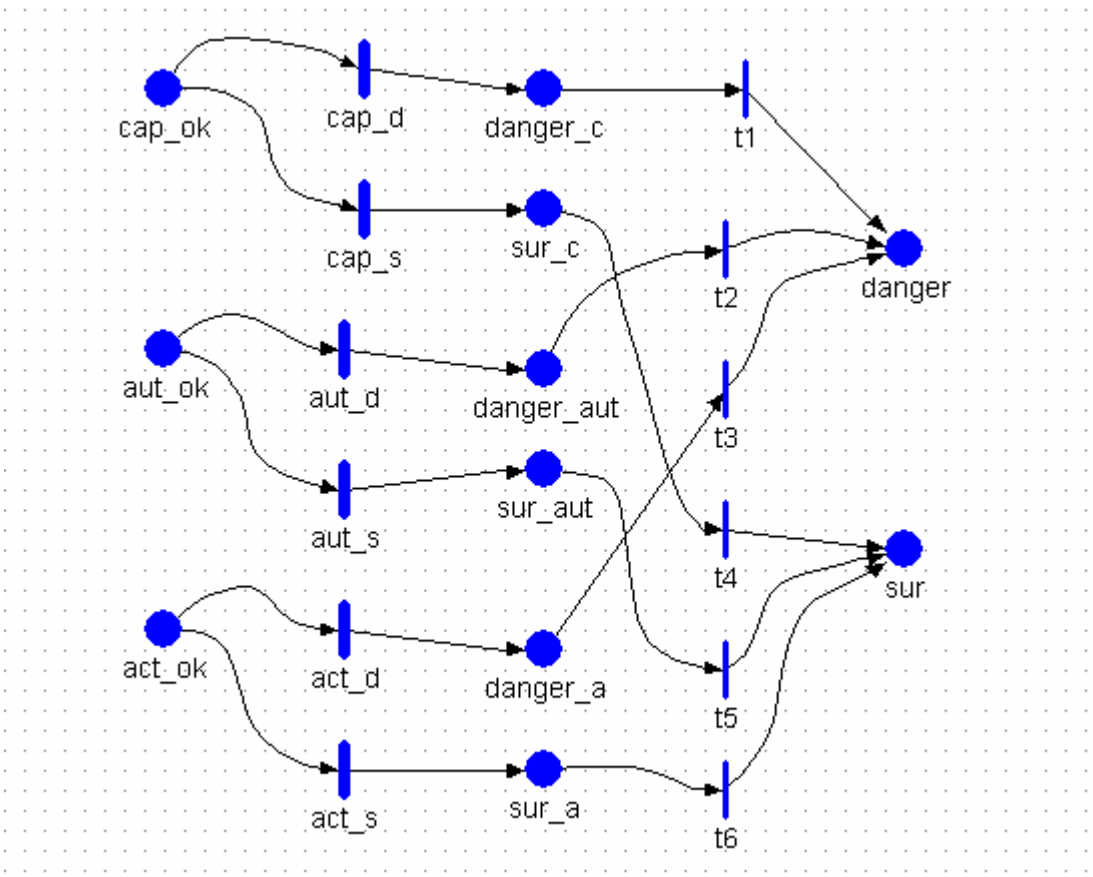


Figure 4.2 : Modèle SAN d'un SIS à architecture 1oo1

Pour ce modèle simple, chaque composant (capteur, automate, actionneur) peut se trouver dans l'un ou l'autre des deux modes de défaillances possibles identifiés auparavant : les défaillances dangereuses ou les défaillances sûres. Ces modes de défaillances sont bien entendu décrits dans les normes relatives de sécurité et reflètent l'intérêt que portent ces normes vis-à-vis des performances en sécurité. En effet la considération de ces modes de défaillances est synonyme de la prise en compte des aspects de la sûreté de fonctionnement. Quand on sait que la non réaction à une situation dangereuse se manifeste comme une indisponibilité de la fonction de sécurité ou une défiabilité du système de sécurité alors qu'un déclenchement intempestif affecte automatiquement la disponibilité.

Chaque composant dispose d'un taux de défaillances constant et les lois de probabilité sont exponentielles. Les places ***cap_ok***, ***aut_ok*** et ***act_ok*** représentent le bon fonctionnement des différents composants du SIS et donc l'état normal. L'état dangereux du SIS est représenté par la place ***danger*** qui sera marquée une fois s'il y a présence d'un marquage sur l'une des places ***danger_c***, ***danger_aut*** ou ***danger_a***. L'état sûr du SIS est représenté par la place ***sur***. Cette place sera marquée une fois qu'il y a présence d'un marquage sur l'une des places ***sur_c***, ***sur_aut*** ou ***sur_a***. Les transitions instantanées ***t1*** à ***t6*** sont de durées nulles et elles sont aussitôt franchies dès la présence de jetons dans les places en amont de ces transitions. La probabilité d'exister dans un état dangereux, respectivement dans un état sûr, est assujettie à la présence d'au moins un jeton dans la place ***danger***, respectivement dans la place ***sur***.

3.3. Evaluation des performances du SIS classique

Le SIS modélisé est utilisé pour réaliser une fonction instrumentée de sécurité (SIF) dans l'hypothèse de la demande faible.

Les taux de défaillances des composants sont déduits de la table 1 extraite de [GOB 05] suivante :

Composant	Taux de défaillances (par heure)	Pourcentage des défaillances sûres (**S%**)
Capteur	6.10^{-06}	40 %
Unité de Traitement	2.10^{-05}	70 %
Elément final	9.10^{-06}	58.3 %

Table 4.1 : Données relatives aux constituants du SIS

Le tableau 2 récapitule les différents paramètres utilisés pour le traitement de notre modèle. Ces paramètres se rapportent aux taux de défaillances dangereuses du capteur, taux de défaillances dangereuses de l'automate, taux de défaillances dangereuses de l'actionneur, taux de défaillances sûres du capteur, taux de défaillances sûres de l'automate et taux de défaillance sûres de l'actionneur.

Composant	Taux de défaillances dangereuses (λ_D)	Taux de défaillances sûres (λ_S)
Capteur	$3{,}6.10^{-6}$	$2{,}4.10^{-6}$
Unité de Traitement	6.10^{-6}	$1{,}4.10^{-5}$
Elément final	$3{,}75.10^{-6}$	$5{,}25.10^{-6}$

Tableau 4.2 : Taux de défaillances dangereuses et sûres

On prend pour durée T la valeur de 8760 heures qui correspond à un an. Cette durée correspond à la période entre deux tests notée *Ti* par la norme.

Les résultats obtenus seront comparés en regard de la norme.

Les résultats regroupés au tableau 4.3 concernent les probabilités de défaillances dangereuses et en sécurité.

	Méthode / Durée	Norme	SAN (Möbius)	Sim tree
PFD	*4380*	$5{,}8473.10^{-2}$	$5{,}526.10^{-2}$	$5{,}6796.10^{-2}$
	5000	$6{,}675.10^{-2}$	$6{,}4277.10^{-2}$	$6{,}4571.10^{-2}$
	8760	$1{,}1694.10^{-1}$	$1{,}0851.10^{-1}$	$1{,}1037.10^{-1}$
	10000	$1{,}335.10^{-1}$	$1{,}2031.10^{-1}$	$1{,}2497.10^{-1}$
PFS	*4380*	$9{,}4827.10^{-2}$	$9{,}0867.10^{-2}$	$9{,}047.10^{-2}$
	5000	$1{,}0825.10^{-1}$	$1{,}0532.10^{-1}$	$1{,}026.10^{-1}$
	8760	$1{,}8965.10^{-1}$	$1{,}6958.10^{-1}$	$1{,}7275.10^{-1}$
	10000	$2{,}165.10^{-1}$	$1{,}9065.10^{-1}$	$1{,}9467.10^{-1}$

Tableau 4.3 : Les différents résultats relatifs à l'architecture 1oo1

Les résultats qui concernent la norme sont obtenus par l'utilisation et l'application des formules préconisées par la CEI 61508 (voir le § 8 du chapitre 2 pour le cas du système 1oo1). Certes ces relations sont données sans explications ou justifications et elles induisent plus d'interrogations, voire de critiques, que de solutions satisfaisantes [INA 05]. L'objectif est de vérifier ces formules malgré la simplicité de l'exemple afin de se faire une opinion critique sur la norme.

La colonne portant le nom "Sim tree" est relative aux résultats obtenus par l'utilisation d'un outil de simulation des arbres de défaillances. La modélisation et ainsi la simulation nous ont permis de déterminer les probabilités relatives au système 1oo1 pour différentes durées en plus d'une analyse de l'aspect quantitatif par la génération de coupes minimales (la coupe minimale est la combinaison des événements de base entraînant l'événement redouté).

Le modèle du système 1oo1 simulé par Möbius est celui représenté en figure 4.2. Dans ce modèle, la détermination des probabilités de défaillances dangereuses et en sécurité passe par le calcul du nombre de franchissements des transitions qui mènent vers les places qui représentent la PFD et la PFS.

On constate que la norme est conservative, puisqu'elle donne des résultats légèrement pessimistes. La différence qui existe dans ces résultats représente l'approximation utilisée par la norme dans l'utilisation des équations simplifiées. En effet, dans l'hypothèse des événements rares relatifs aux systèmes de sécurité, les taux de défaillances sont très faibles de telle sorte que les lois exponentielles peuvent être approximées à un ordre un à des portions de droite en négligeant les termes d'ordre supérieurs [CEI 00] [GOB 98].

La figure 3 donne les probabilités de défaillances dangereuses avec des intervalles entre les deux tests *Ti* = 8760 heures.

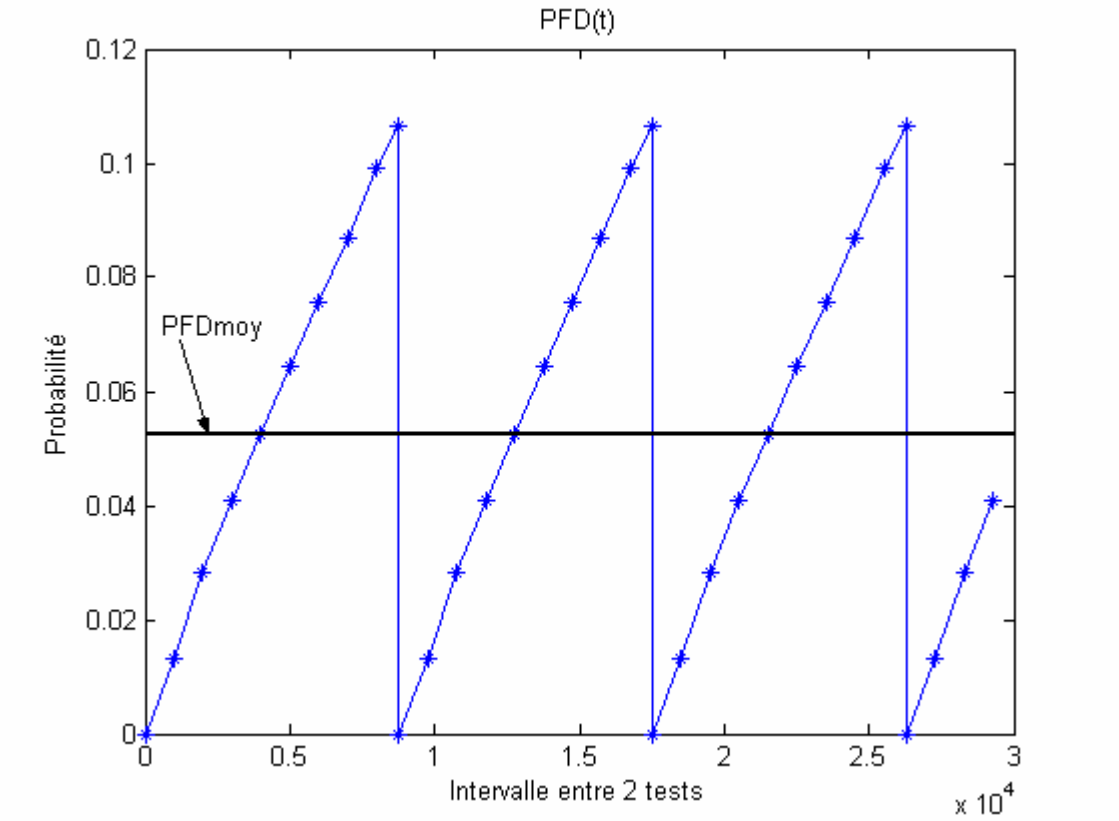


Figure 4.3 : Probabilité de défaillance dangereuse et intervalles de tests

La probabilité de défaillance dangereuse PFD(t) est un paramètre qui évolue dans le temps, la détermination de sa valeur moyenne PFD_{avg} sur une durée particulière permet d'avoir un paramètre constant qui reflète en quelque sorte la qualité du système. Cette durée n'est ni tout à fait un temps de mission ni une durée de vie mais plutôt un intervalle entre deux tests consécutifs. Il se peut d'ailleurs que la fonction de sécurité n'ait jamais été sollicitée pendant cet intervalle. Le système qui réalise la fonction de sécurité est considéré comme neuf après ce test. D'où les performances retrouvées (cf. figure 4.3) pour le système entre deux tests consécutifs.

La figure précédente est élaborée à partir des hypothèses formulées dans le chapitre 3 (voir paragraphe § 4.3). Le système instrumenté de sécurité est inactif pendant les durées d'inspection périodique et pendant l'opération de maintenance. La figure 4.3 montre le passage brutal à zéro du paramètre PFD(t) qui justifie ses hypothèses. En réalité, certains systèmes industriels restent opérationnels même pendant les tests périodiques évitant ainsi l'indisponibilité de la fonction de sécurité pendant l'exécution de ces tests. La relation qui donne la probabilité de défaillance sur demande devient plus complexe puisque d'autres paramètres agissent sur cette indisponibilité tels que la durée des tests…[SIG 07]

La valeur moyenne de la probabilité de défaillance dangereuse est représentée par la ligne horizontale dans la figure précédente. Elle est égale à $PFD_{moy} = 5{,}661.10^{-2}$. Cette valeur correspond à un SIL 1 selon le tableau 2.3 du chapitre 2. Dans notre exemple, avec un intervalle entre deux tests égal à un an, le niveau de SIL 1 reste garanti alors que si l'intervalle

entre deux tests devient plus important, le niveau de SIL peut ne plus être garanti momentanément et le système instrumenté de sécurité ne sera plus conforme aux normes de sécurité qui n'autorisent pas de niveau de SIL en deçà du SIL 1. Il faut donc s'assurer que la PFD(t) instantanée reste dans les limites du SIL requis en évitant de dépasser les frontières de SILs adjacents. De ce fait, on peut conclure que la PFD_{moy} ne saurait à elle seule pouvoir décrire le comportement de l'indisponibilité d'un SIS à exécuter une fonction de sécurité. Et pour que la représentation soit complète, il faut prendre en compte également l'évolution de la PFD(t) instantanée et s'assurer qu'à tout moment, cette indisponibilité reste équivalente au SIL requis à l'application.

La répartition en pourcentage du niveau de SIL pendant toute la durée entre deux tests est illustrée dans la figure 4.4 suivante :

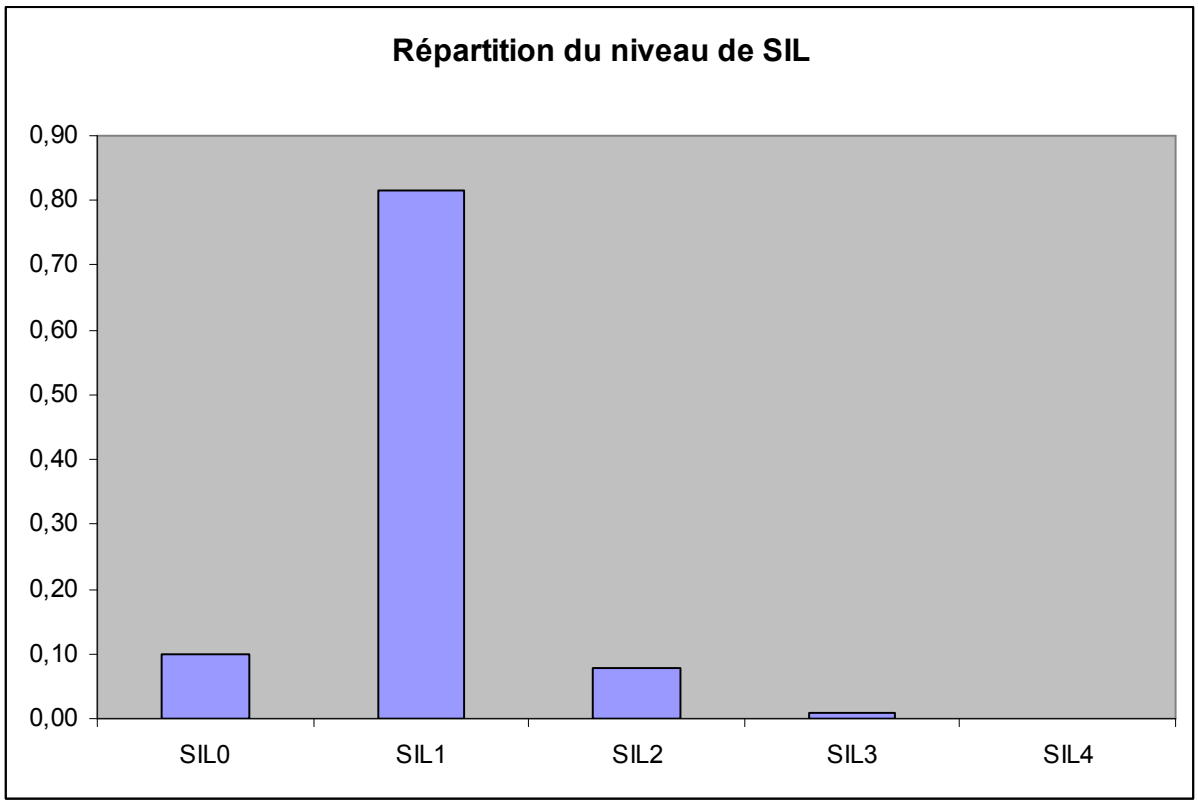


Figure 4.4 : Répartition du niveau de SIL

Cette figure montre que le SIS qui dispose d'un niveau de SIL égal à 1 (cf. figure 4.3) passe 9.9% dans la zone correspondante à SIL 0 où la norme ne peut plus être appliquée. Le SIS passe plus d'un mois pendant les tests d'intervalle avec un SIL 0. Le SIS demeure dans la zone SIL 1 pendant 81.5 % et le reste du temps est réparti entre les zones correspondantes aux SIL 2 et au SIL 3. D'ailleurs, lorsqu'un SIS est conçu pour un niveau de SIL, il peut disposer d'un niveau de SIL supérieur mais pas le contraire. Pour la zone qui correspond au niveau de SIL 4, le SIS passe 0,085 %, ce qui est très négligeable. Il faut noter que les applications courantes n'atteignent jamais ce niveau de SIL.

Notre système consacre la plupart du temps dans la zone SIL 1 et près de 10% de la mission en temps en SIL 0, ce qui est loin d'être négligeable et peut être dangereux. De plus, si ce système passe aussi plus de 7% de sa mission dans la zone SIL3, qui correspond à une zone de risque faible, ces moments passés dans cette zone ne compensent pas les risques de se

trouver en zone SIL 0. Avec le système testé périodiquement, quand le seuil d'une mauvaise zone SIL est empiété, le système reste dans cette zone jusqu'au prochain test périodique et cela peut être pour un long délai lorsque les composants sont testés tous les 10 ans, par exemple.

Notons que le passage dans la zone SIL 0 correspond au franchissement par la PFD(t) instantanée de la valeur 0,1 (cf. tableau 2.3). C'est-à-dire qu'il faut rester au deçà de cette valeur frontalière pour demeurer dans la zone SIL où la norme peut être appliquée. Le système SIS dans le cas où il atteint un SIL non conforme se trouve sans usage possible dans une application de sécurité conformément à la norme.

Le MTTF pour ce système est de 8,83 années. Seules les défaillances dangereuses sont considérées pour son élaboration. En effet, il existe aussi le MTTFS [GOB 05] qui est relatif aux défaillances sûres.

4. Evaluation dynamique des Systèmes Instrumentés de Sécurité à Intelligence Distribuée

4.1. Structure 1oo1 D

Introduisons tout d'abord la structure 1oo1 D dans laquelle le canal comporte une voie comme le montre la figure 4.5 :

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).

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.

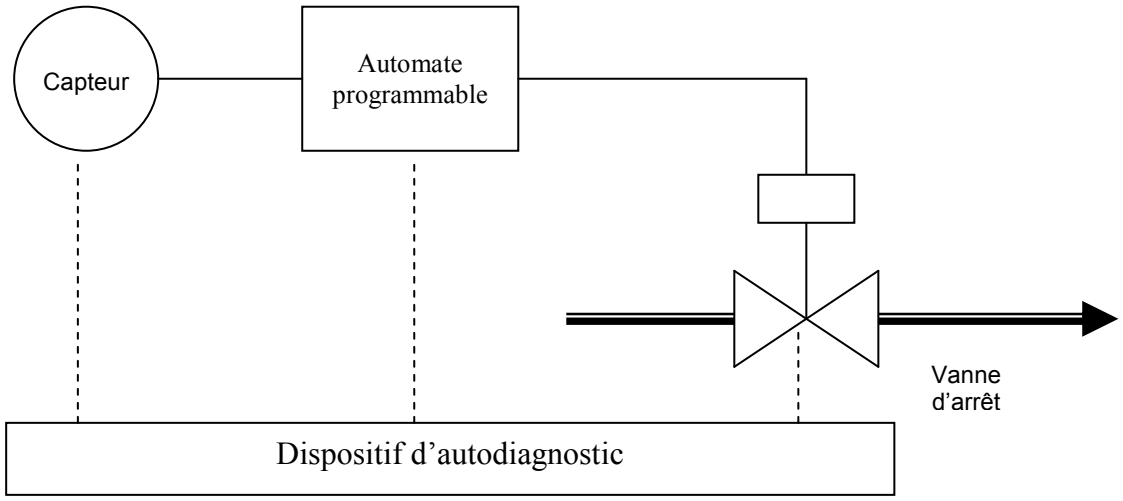


Figure 4.5 : Schéma de la structure 1oo1D

Le diagnostic permet la conversion de défaillances dangereuses détectées en défaillances sûres [GOB 05].

4.1.1. Modèles des composants

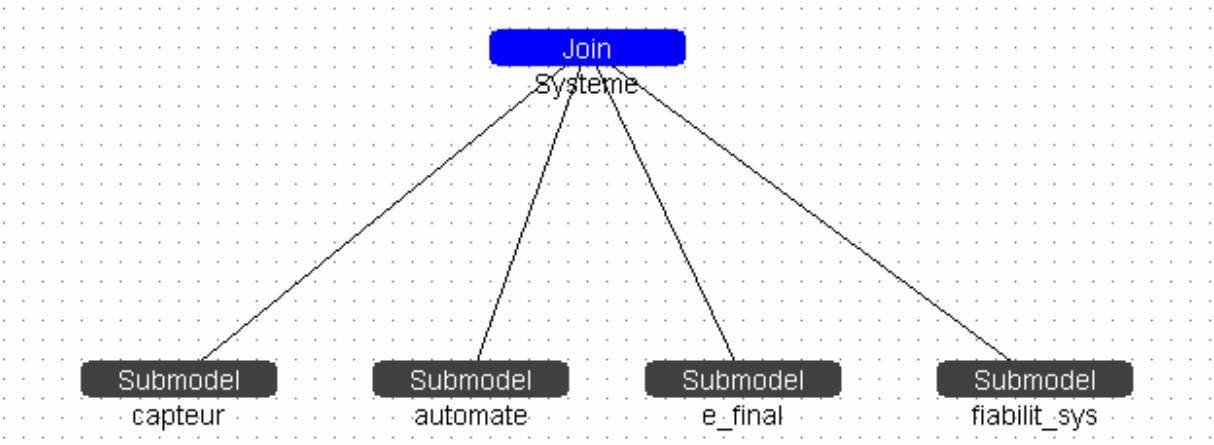


Figure 4.6 : Conception hiérarchique et composition des sous-systèmes

Dans cette partie, une description globale du modèle SAN est illustrée et les modèles de plusieurs composants du système sont présents. Le modèle est conçu d'une manière hiérarchique et sa composition est présentée sur la figure 4.6.

Cette étape permet l'interconnexion entre les différents sous-systèmes via des places partagées.

4.1.1.1. Modèle du capteur

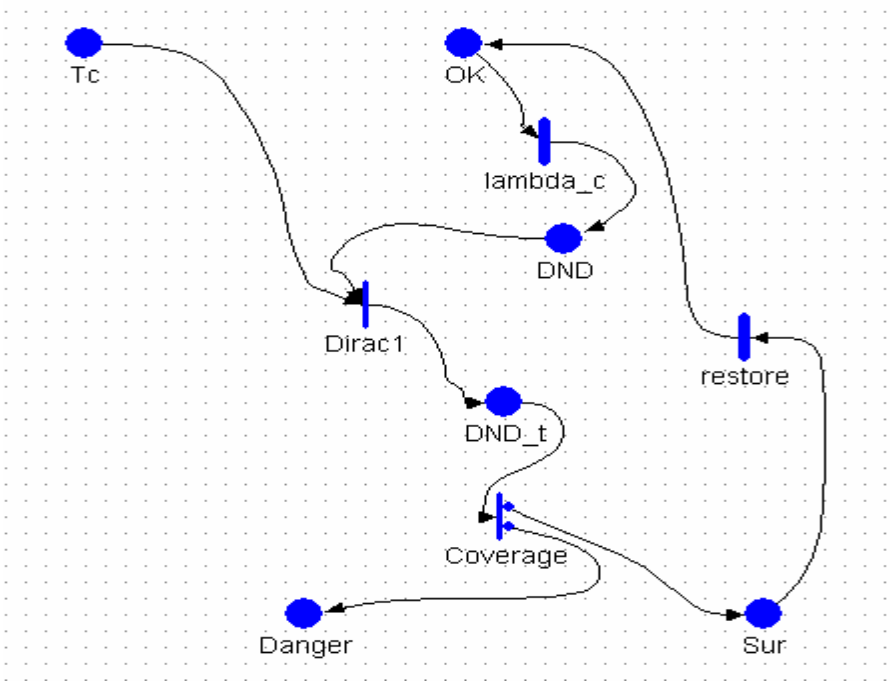


Figure 4.7 : Modèle du capteur (structure 1oo1D)

Dans le modèle du capteur de la figure 4.7, un certain nombre de défaillances sont exprimées. Il s'agit des défaillances sûres (place ***Sur***) et défaillances dangereuses (place ***Danger***). Un taux de couverture de diagnostic DC est alloué au capteur (***Coverage***). Ce taux de couverture exprime le rapport entre le taux de défaillances détectées et le taux de défaillances totales. Après l'occurrence d'une défaillance sûre, il y a possibilité de restaurer le système par le franchissement de la transition déterministe (***restore***) dont la durée est égale au temps nécessaire à la restauration complète du système après un déclenchement intempestif par exemple. La présence d'une marque dans la place ***Tc*** autorise un autotest du capteur géré par l'automate. Les défaillances non détectées ***DND*** peuvent être qualifiées de sûres ou de dangereuses suite à l'exécution de l'autotest.

4.1.1.2. Modèle de l'automate

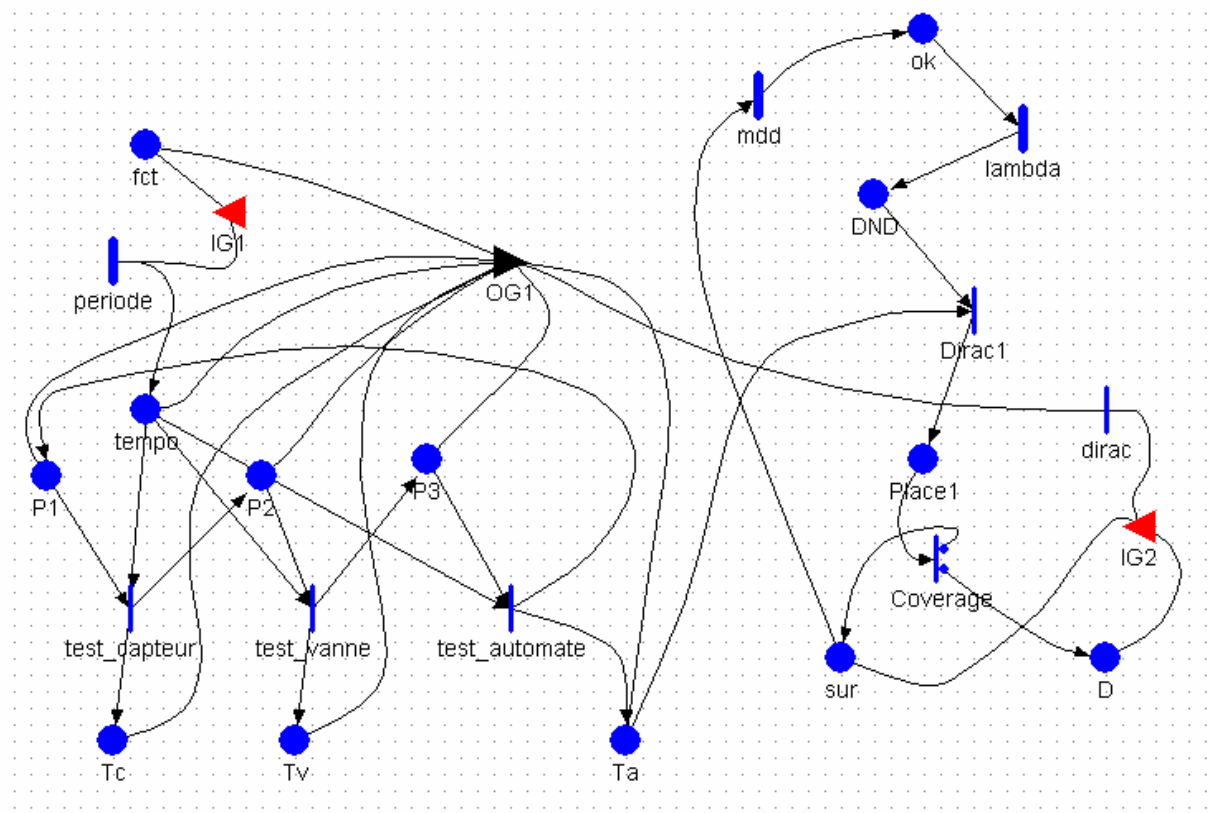


Figure 4.8 : Modèle de l'automate (structure 1oo1D)

Le modèle de l'automate de la figure 4.8 montre une disposition de deux parties, l'une fonctionnelle et l'autre dysfonctionnelle. Dans la partie fonctionnelle (à gauche), les cycles de l'automate sont exécutés par une horloge périodique (***periode***). 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***). Cette politique n'est pas la seule possible à être exécutée par l'automate et d'autres politiques peuvent être éventuellement implantées. 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. L'automate peut être également restauré en cas de défaillance sûre et il dispose également d'un taux de couverture de diagnostic qui lui est propre.

Le modèle de l'actionneur ressemble à celui du capteur, cette fois-ci, la présence d'une marque dans la place (***Tv***) de l'automate autorise des autotests de l'actionneur. Cette place est partagée avec une autre place du modèle de l'actionneur. La présence d'un jeton dans cette place permet après l'exécution du test la répartition des défaillances non détectées.

4.2. Introduction du réseau de communication dans la structure 1oo1D

L'introduction des réseaux dans les applications distribuées offre de la flexibilité mais introduit aussi quelques problèmes nouveaux. Les délais, la perte de trames, les retards éventuellement non bornés, la gigue…[CAU 04].

Dans cette partie, nous allons nous intéresser à un modèle de système 1oo1D avec un réseau de terrain type CAN.

Il faut préciser que vis-à-vis des travaux que nous menons, le réseau de communication est un moyen utilisé par les fonctions qui octroient de l'intelligence aux instruments. C'est pourquoi, il a été introduit sans se préoccuper de sa sensibilité aux perturbations et sans considération des effets de la perte des messages.

4.2.1. Modélisation du réseau de terrain sous Möbius

Cette partie est consacrée au modèle du système avec un réseau de communication (*CAN: Control Area Network*) et ensuite nous allons également introduire des instruments intelligents au lieu d'instruments traditionnels. Dans cette étude, nous nous concentrons sur le réseau CAN même si ce type d'études peut être étendu à d'autres types de réseaux de communication.

L'ensemble des composants est relié par un réseau de communication qui est défini comme un medium par lequel transitent des trames contenant des données du système. Tous les composants sont représentés comme des systèmes échantillonnés avec Te comme période d'échantillonnage. Cette période d'échantillonnage est constante et elle est la même pour tous les composants. Sa valeur est de 0.5 unité de temps. Tous les composants sont échantillonnés avec cette période d'échantillonnage et le réseau de communication est un système réagissant aux événements discrets.

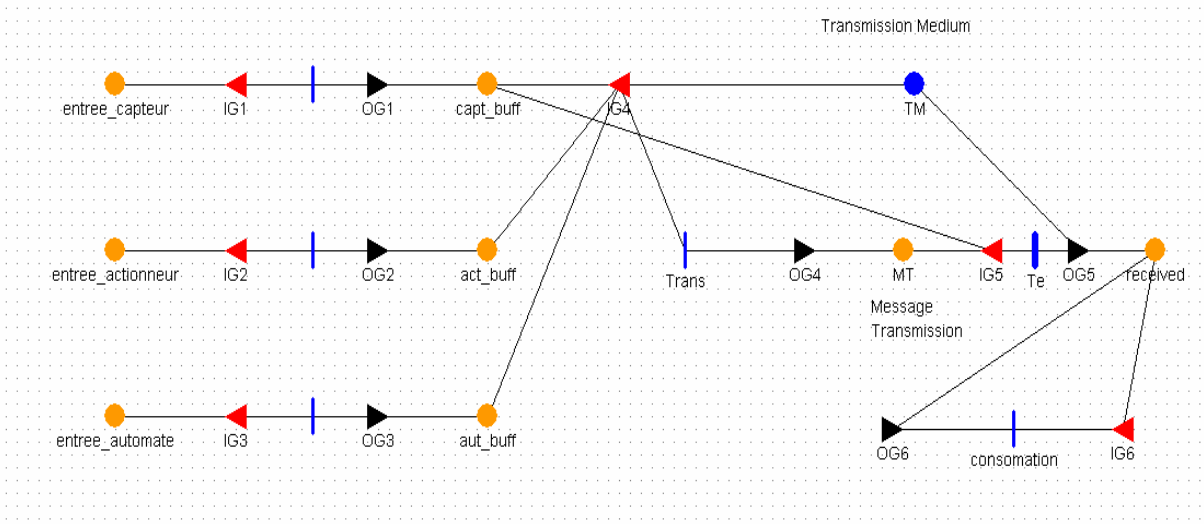


Figure 4.9 : Modèle du réseau de terrain avec l'outil Möbius

La modélisation du réseau de communication représente le modèle le fonctionnement d'un réseau CAN (Controller Area Network) [GHO 08]. Le réseau est constitué dans cet exemple de trois stations émettrices qui vont pouvoir envoyer des messages (trames) sur un médium partagé (canal de transmission). Les messages envoyés sont placés dans des places tampons (***buffer***) qui sont des places étendues, les messages ensuite attendent la libération du canal pour être transmis vers leur destination. La manière d'accéder au canal est celle d'une transmission basée sur des niveaux de priorité des messages. Ceci signifie que chaque abonné

sera affecté d'une priorité lui permettant ou non d'envoyer ces caractéristiques via le canal, pour éviter les collisions sur le canal.

Le medium (canal) est affecté d'un retard représentant le délai de transmission des messages. Le message en sortie du canal est prêt à être envoyé et il est disponible dans la place *"received"*.

Lorsque le bus est libre, n'importe quel émetteur qui dispose de son propre identificateur peut commencer à transmettre une information sur le canal. Lorsque deux nœuds tentent d'accéder simultanément au medium, le nœud qui dispose de la plus haute priorité gagne l'arbitrage et accède au bus, son information est envoyée sans perte de temps alors que le nœud affecté d'une priorité moindre attend la libération du medium pour émettre.

Nous avons procédé à vérifier des valeurs de la période d'échantillonnage autres que Te=0,5.

Te	0,5	1	5	8
PFD	$7{,}7.10^{-2}$	$7{,}33.10^{-2}$	$7{,}08.10^{-2}$	$7{,}03.10^{-2}$
PFS	$2{,}1.10^{-1}$	$2{,}078.10^{-1}$	$2{,}05.10^{-1}$	$1{,}995.10^{-1}$

Tableau 4.4 : Performances en sécurité en fonction de la période d'échantillonnage

D'une façon générale, la probabilité des défaillances dangereuses a diminué ainsi que la probabilité de défaillances sûres. Ceci est dû au fait que les informations qui concernent les défaillances ne sont envoyées que pendant des instants discrets et non pas en continu. Les performances sont en effet très sensibles aux périodes d'échantillonnages des différents dispositifs. Et de ce fait, les instants de révélations dépendent largement des périodes d'échantillonnages, ce qui provoque donc ce changement des valeurs de ces deux métriques.

Le réseau de communication garantit les délais de transmission inférieurs à la période d'échantillonnage. C'est le seul composant dans le système qui travaille d'une manière événementielle. Le délai de transmission est constant. Il faut noter que l'accent n'est pas mis sur l'influence des retards ni celui de la perte ou de l'altération des trames.

L'introduction du réseau a pour conséquence quelques modifications dans les modèles de base des constituants de la boucle de sécurité afin de tenir compte des mécanismes de transmission de données via le réseau. A titre d'illustration, le modèle de l'automate communicant est montré dans le sous paragraphe suivant.

4.2.2. Modèles échantillonnés des composants

4.2.2.1. Modèle de l'automate

Le modèle de l'automate décrit par la figure 4.10 est un dispositif communicant, il dispose d'une intelligence locale (et centrale vis-à-vis de la boucle de commande considérée) lui permettant entre autres de gérer les autotests dans les dispositifs de terrain en envoyant des ordres par voie de communication par réseau.

L'automate, qui est doté d'une capacité de communication, envoie ses messages périodiquement. A chaque période d'échantillonnage (transition ***periode_aut*** dans la figure 4.10), l'automate est disposé à envoyer des informations sur le réseau.

En effet, tous les dispositifs (capteur, actionneur) disposent d'une période d'échantillonnage et ils sont considérés comme des systèmes échantillonnés.

Dans l'étude menée, le réseau de communication garantit un délai exprimant le retard affecté aux messages inférieurs aux périodes d'échantillonnage de tous les dispositifs.

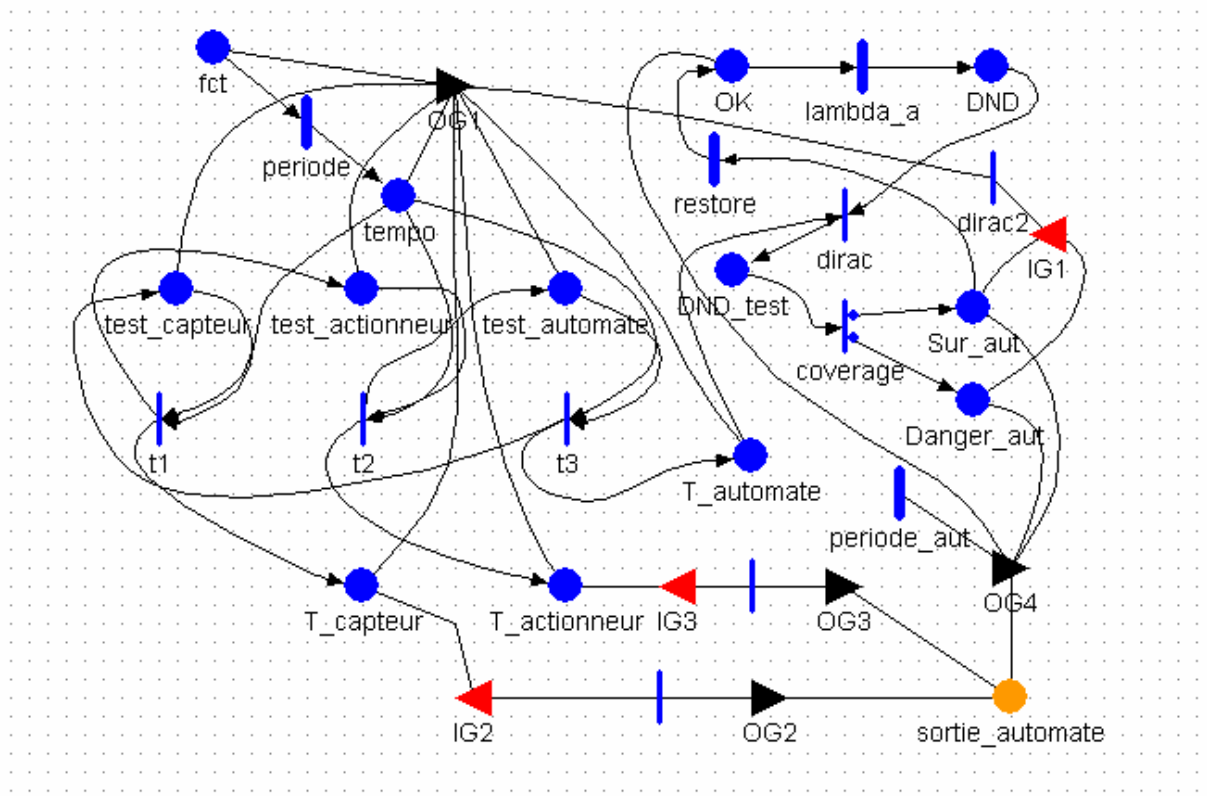


Figure 4.10 : Modèle de l'automate communicant

La place colorée ***sortie_automate*** est une place partagée avec la place ***entree_automate*** de la figure 4.9 qui correspond à la description du réseau de communication. Cette place contient les informations prêtes à être envoyées par le réseau aux différents interlocuteurs. Cette place dispose d'un jeton de type coloré appelé ***trame*** qui est relatif à un ensemble d'attributs qui sont ***etat***, ***valeur***, ***emetteur*** et ***dispo***. Ces attributs sont communs entre toutes les places qui sont en relation avec le réseau pour les opérations d'émission et de réception des messages. Ils expriment en effet la nature de l'émetteur de l'information (capteur ou autres), son état, l'affectation d'une valeur pour différencier les destinataires des autotests et la disposition à émettre dans le réseau.

4.3. Introduction des instruments intelligents dans la structure 1oo1D

4.3.1. Modèle de capteur intelligent

Dans le modèle, l'ordre de test n'est plus transmis via le réseau de communication par l'automate et la fonctionnalité relative au test ainsi que les autres fonctionnalités du capteur intelligent sont traitées localement. Les modules de test peuvent être sollicités soit lorsque c'est nécessaire, soit cycliquement, soit en permanence suivant un principe de surveillance active [NOI 95]. Dans notre modèle, le capteur intelligent dispose cycliquement selon les instants d'une période d'autotests. Les autres fonctionnalités sont aussi synchronisées par cette période.

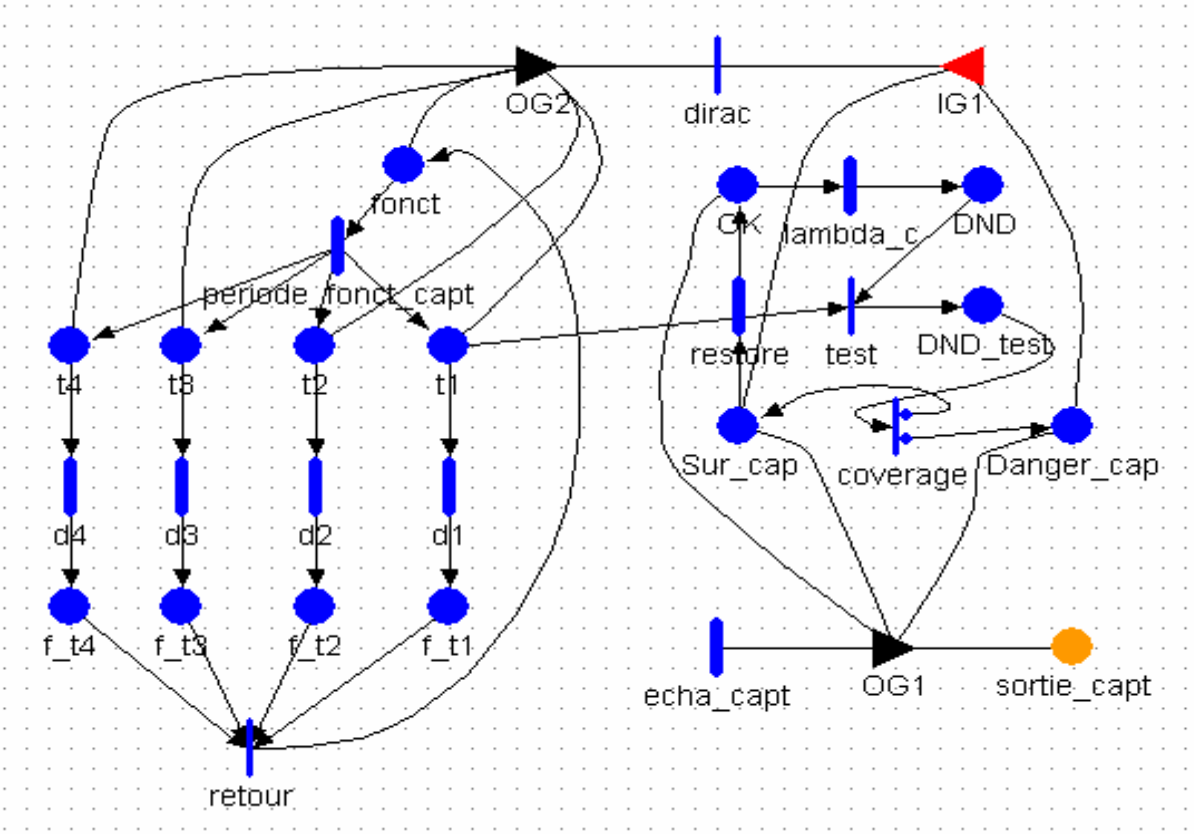


Figure 4.11 : Modèle de capteur intelligent

Le modèle du capteur de la figure 4.11 montre une disposition de deux parties, l'une fonctionnelle et l'autre dysfonctionnelle. Dans la partie fonctionnelle (à gauche), les cycles du capteur sont exécutés par une horloge périodique (***periode_fonct_capt***). Les autotests internes sont gérés localement suivant une politique de test qui consiste à allouer une durée de test du capteur (transition ***d1***). La partie réservée aux autotests est constituée entre autres des places ***t1*** (début tâche 1) et ***f_t1*** (fin tâche 1). 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. Les opérations associées aux autres places de la partie fonctionnelle ne sont pas détaillées et elles couvrent le reste des fonctionnalités propres au capteur intelligent. L'interaction entre les modèles fonctionnel et dysfonctionnel est représentée à l'aide de transitions immédiates.

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

capteur peut être également restauré en cas de défaillance sûre et il dispose également d'un taux de couverture de diagnostic qui lui est propre. Dans le modèle présenté en figure 4.11, un certain nombre de défaillances sont exprimées. Il s'agit des défaillances sûres (place ***Sur_cap***) et défaillances dangereuses (place ***Danger_cap***). Un taux de couverture de diagnostic DC est alloué au capteur (***coverage***). Ce taux de couverture exprime le rapport entre le taux de défaillances détectées et le taux de défaillances totales. Après l'occurrence d'une défaillance sûre, il y a possibilité de restaurer le système par le franchissement de la transition déterministe (***restore***) dont la durée est égale au temps nécessaire à la restauration complète du système après un déclenchement intempestif par exemple. La présence d'une marque dans la place ***t1*** 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. La place ***sortie_cap*** assure l'envoi des informations via réseau après le franchissement de la transition ***echa_capt*** dont la durée représente la période d'échantillonnage du capteur.

Le modèle de l'actionneur ne diffère pas beaucoup de celui du capteur intelligent et les parties dysfonctionnelles sont similaires. Il faut noter que les différents modèles, du capteur, de l'actionneur ou de l'automate, sont des modèles échantillonnés et que les informations sont envoyées au réseau de communication périodiquement.

Différentes performances peuvent être évaluées sur ce modèle.

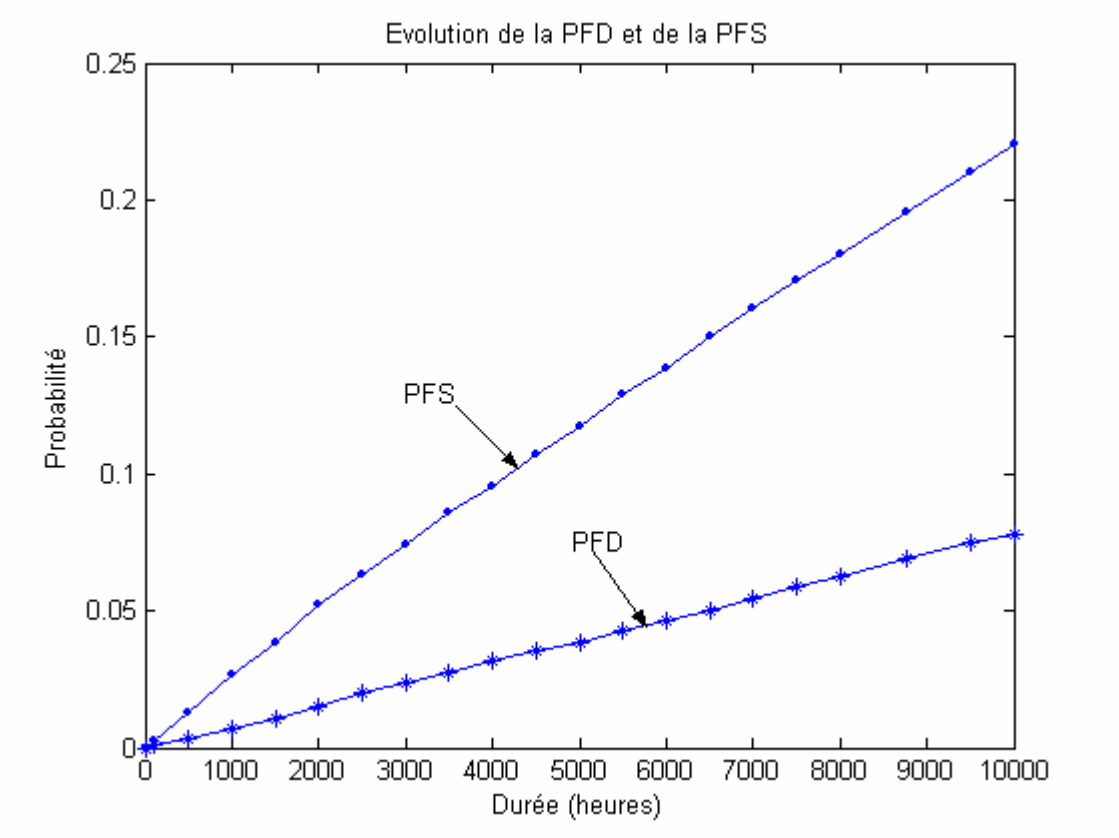


Figure 4.12 : Evolution des deux métriques en fonction du temps

La figure 4.12 montre l'évolution 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 paramètres du modèle sont :

lambda_actionneur	9.0E-6
lambda_automate	2.0E-5
lambda_capteur	6.0E-6
delai	1.0E-5
echantillonage_actionneur	0.5
echantillonage_aut	0.5
echantillonage_capteur	0.5
CD_actionneur	0.75
CD_automate	0.75
CD_capteur	0.75
p1	2
p2	3
p3	1
periode_fonct_actionneur	1.0
periode_fonct_capteur	1.0
periode_test_automate	1.0
restore_actionneur	24.0
restore_automate	24.0
restore_capteur	24.0
retard_reseau	0.01

Les taux de défaillances des composants et le taux de restauration proviennent de [GOB 05]. Les autres paramètres cités ci-dessus concernent des identificateurs propres aux dispositifs (***p1***, ***p2***, ***p3***) qui prennent des valeurs entières respectivement ***2***, ***3*** et ***1***. Le retard relatif au réseau (***0.01***) est maintenu inférieur à la période d'échantillonnage (***0.5***). Le taux de couverture de diagnostic est pris égal à ***75 %*** (ni faible ni moyen selon la norme).

La figure 4.12 montre les performances en sécurité d'un système instrumenté de sécurité à intelligence distribuée. L'évolution des deux métriques qui décrivent les performances en sécurité du système étudié montrent une nette diminution de la probabilité de défaillance dangereuse et une augmentation de la probabilité de défaillances sûres. Une illustration est faite sur le tableau 4.5 suivant :

	Durée (heures)	SIS	SISID
PFD	*1000*	$1{,}34.10^{-2}$	$0{,}73.10^{-2}$
	5000	6,37.10-2	3,85.10-2
	8760	$1{,}05.10^{-1}$	$0{,}689.10^{-1}$
	10000	$1{,}17.10^{-1}$	$0{,}781.10^{-1}$
PFS	*1000*	$2{,}27.10^{-2}$	$2{,}66.10^{-2}$
	5000	$1{,}026.10^{-1}$	$1{,}18.10^{-1}$
	8760	$1{,}71.10^{-1}$	$1{,}95.10^{-1}$
	10000	$1{,}926.10^{-1}$	$2{,}20.10^{-1}$

Tableau 4.5 : Comparaison des performances du SIS et du SISID

En effet, plus on a un taux élevé de détection par les moyens d'autotests intégrés, plus le taux de défaillances dangereuses s'affaiblit et le taux de défaillances sûres augmente car des défaillances dangereuses se transforment en défaillances sûres. Nous relevons donc une diminution de la valeur de la PFD et une augmentation de la valeur de la PFS par rapport aux valeurs du système SIS classique. La somme des deux métriques reste quasi constante. Le motif de cette évolution est tout simplement la possibilité d'accomplir des tâches localement (autotests) par les dispositifs de terrain.

L'intégration directe de la procédure de test dans les dispositifs de terrain (capteur et actionneur) autorise le renseignement sur l'état de ces dispositifs sans l'ordre centralisé auparavant dans l'élément de décision logique qui est l'automate dans notre exemple. Ce changement de stratégie procure des révélations sur les états des dispositifs au fur et à mesure de leur apparition.

Maintenant, nous allons nous intéresser à la répartition du niveau de SIL pour le système SISID.

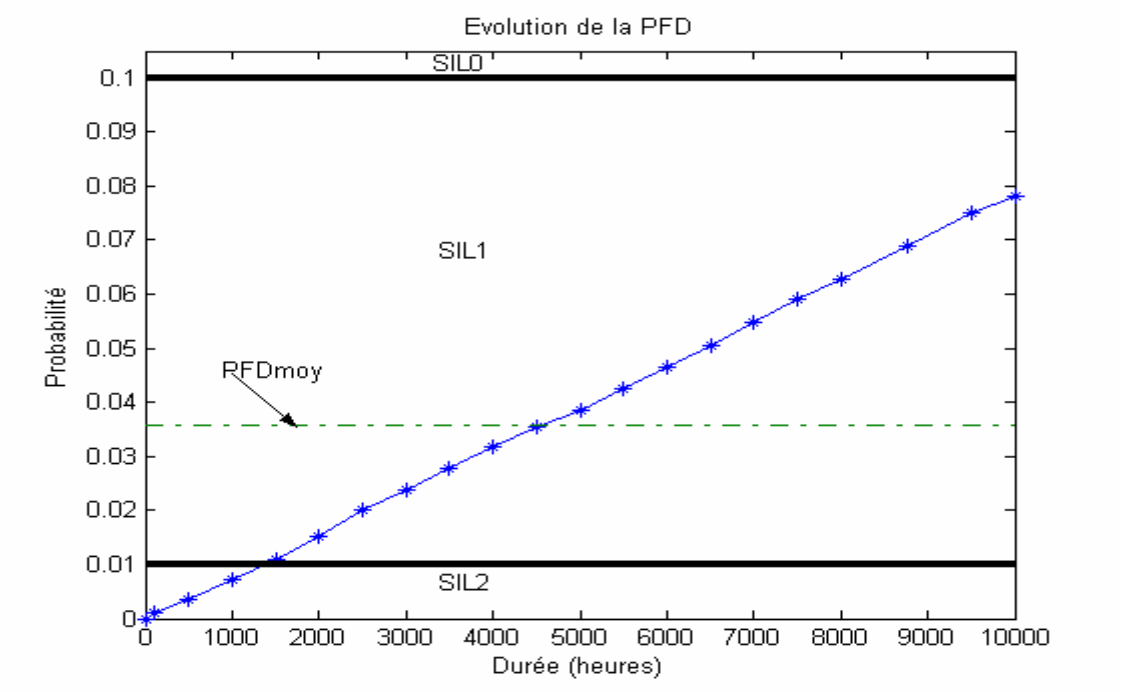


Figure 4.13a : PFD(t) et niveau de SIL

La figure 4.13a montre l'évolution de la PFD(t) pour un SISID dans une échelle linéaire. Nous constatons que contrairement au SIS classique, la zone SIL 0 (absence de SIL) n'est jamais franchie et en majorité, le système se trouve dans la zone SIL 1. La probabilité de défaillance dangereuse moyenne PFD_{moy} est aussi mentionnée et elle a une valeur de $3{,}589.10^{-2}$ ce qui correspond à un système de niveau SIL 1. Pour faire apparaître les autres niveaux de SIL, nous passons à une échelle semi-logarithmique (cf. Figure 4.13b).

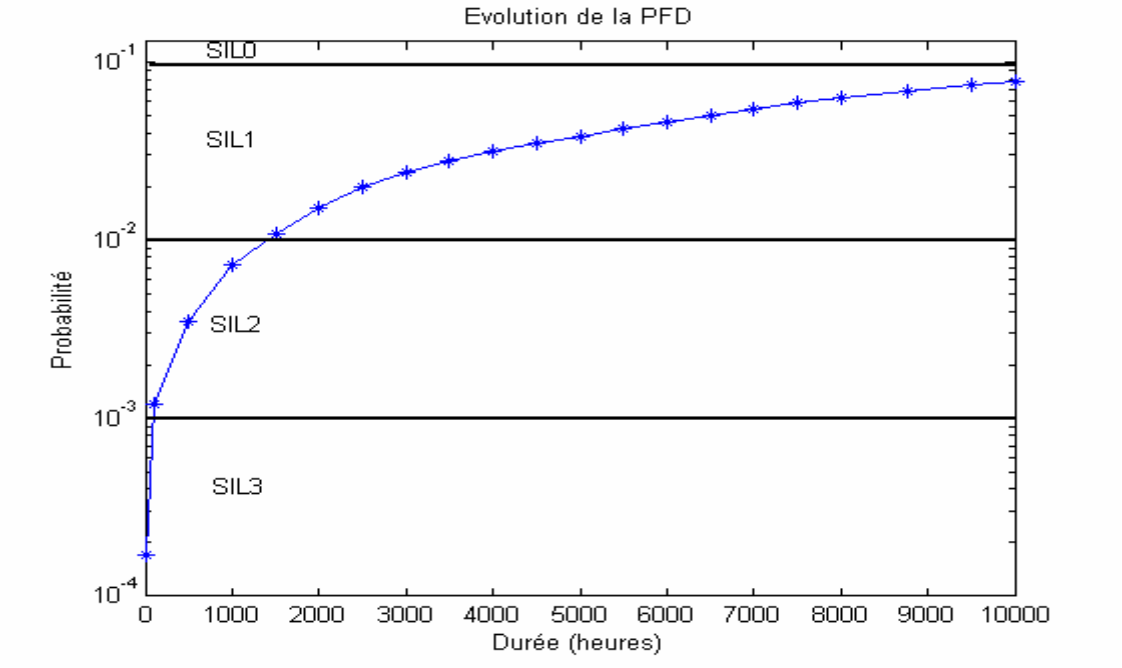


Figure 4.13b : PFD(t) et niveau de SIL

On s'aperçoit clairement d'après cette illustration des zones de SIL franchies par le système.

Le pourcentage des différents niveaux de SIL est réparti dans la figure 4.14 suivante :

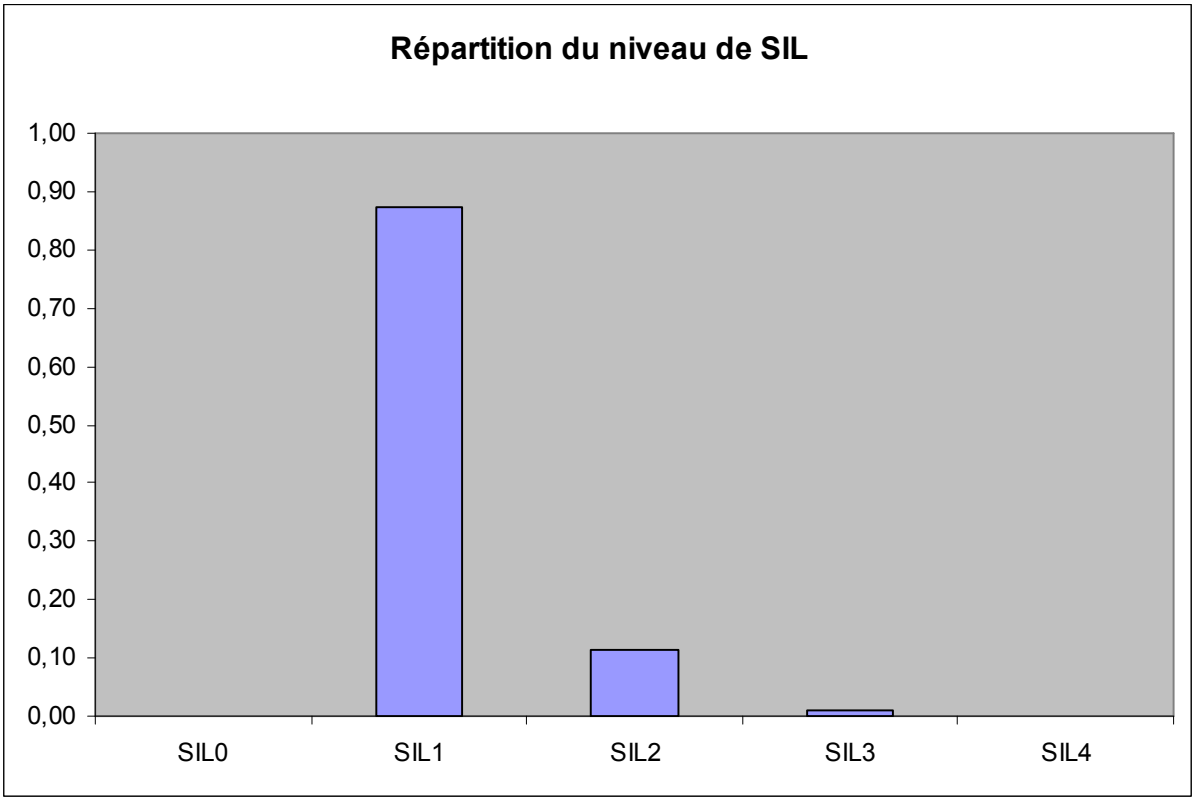


Figure 4.14 : Répartition du niveau de SIL pour un SISID

Cette figure montre que le SISID qui dispose d'un niveau de SIL égal à 1 passe 100% dans des zones correspondantes à un des niveaux de SIL supérieurs au niveau SIL 0 où la norme ne peut plus être appliquée. Le SIS demeure dans la zone SIL 1 pendant un peu plus de 87 % et le reste du temps est réparti entre les zones correspondantes aux SIL 2 (11.5%) et au SIL 3 (1.1%). Le SISID a permis au système qui était non conforme à la norme dans 9.9% des cas (cf. SIS) de se conformer totalement à 100% à cette norme de sécurité.

Le MTTF pour le SISID est de 14,54 années. Nous observons une nette amélioration de cette métrique qui qualifie la fiabilité du système.

4.4. Indicateur de performance

Afin d'examiner les résultats et les effets de l'intégration des niveaux d'intelligence dans les systèmes de sécurité, nous introduisons des indicateurs de performance. Un indicateur de performance nous aide à comprendre l'impact que subit la modification d'un paramètre tel que la PFD du système. Nous proposons pour le calcul de l'indicateur de performance la relation suivante:

$$IP_{PFD} = \frac{(PFD_{moy})_{SISID}}{(PFD_{moy} + PFS_{moy})_{SIS}}$$

Nous avons introduit dans cette relation les valeurs moyennes plutôt que les valeurs instantanées pour avoir une estimation globale de ce taux en restant conforme à la norme qui préconise pour les performances en sécurité les valeurs moyennes. Notons que concernant les défaillances sûres, l'indicateur peut s'exprimer de la façon suivante :

$$IP_{PFS} = \frac{(PFS_{moy})_{SISID}}{(PFD_{moy} + PFS_{moy})_{SIS}}$$

Le calcul de ces deux indicateurs nous donne les valeurs suivantes:

$IP_{PFD} = 0.245$ et $IP_{PFS} = 0.71$

Ces valeurs correspondent donc à l'introduction d'une intelligence niveau 2 tel que cela était décrit au chapitre 1.

4.5. Conclusion

L'intérêt de cette étude porte sur la détermination des performances en sécurité du système en régime dynamique. Elle permet d'obtenir une comparaison quantitative des comportements des systèmes. Ainsi, elle permet de comparer les différents architectures de SIS disposant ou non de moyens d'autodiagnostics qui sont gérés localement ou d'une manière centralisée.

Un résultat important 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.

Cette étude nous a permis d'approcher la problématique de la prise en compte de l'intelligence, telle qu'elle a été définie dans le chapitre 1, dans la conception des SIS. En effet, l'exemple traité nous a permis de déterminer le niveau de SIL relatif à chaque système et de voir que l'apport de l'intelligence permet de couvrir les zones de niveaux de SIL exigés par la norme pour un SIS qui disposait d'un niveau de SIL 1 mais qui ne pouvait pas être maintenu pendant toute la durée entre deux tests d'intervalle.

L'augmentation de la valeur de la PFS provoque une perte financière causée par le système de sécurité en raison de déclenchements intempestifs. Ceci nous rappelle qu'en sûreté de fonctionnement, le compromis sécurité/disponibilité demeure même avec l'adjonction d'éléments intelligents dans la boucle de sécurité.

L'introduction des indicateurs de performances a permis de mieux situer la contribution de l'intelligence introduite dans le système de sécurité vis-à-vis des performances globales de sécurité.

5. Exemple d'un réservoir sous pression équipé d'un système de sécurité

5.1. Description

Considérons l'exemple suivant (figure 4.15) emprunté à [GOB 01] et modifié par le remplacement des instruments classiques par des instruments intelligents. Dans cet exemple, un procédé est constitué d'un réservoir sous pression contenant un liquide inflammable volatil avec l'instrumentation associée. Le système de protection disponible est un système instrumenté de sécurité constitué de deux capteurs de pression qui relèvent en continu la valeur de la pression et ils sont contrôlés par un automate programmable qui commande aussi le fonctionnement des vannes qui sont normalement ouvertes.

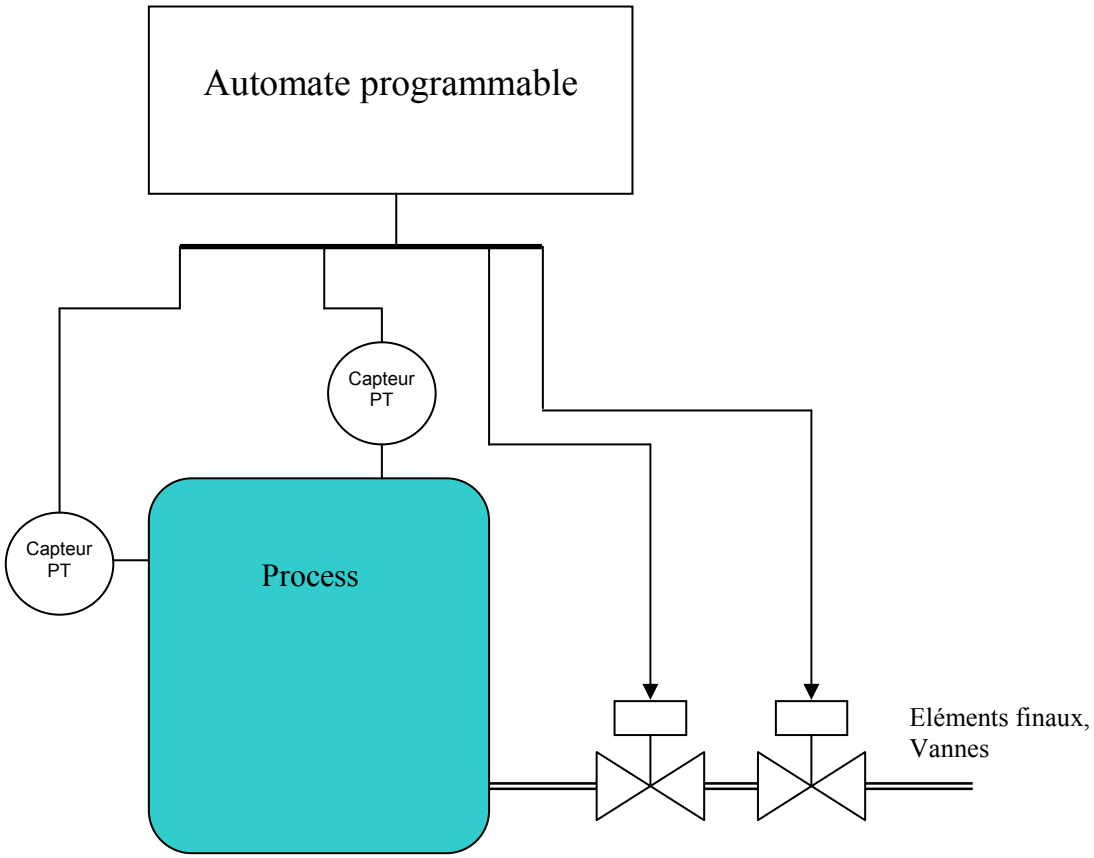


Figure 4.15 : Réservoir sous pression équipé de système de sécurité

Une condition d'excès de pression peut provoquer un rejet de produit inflammable dans l'environnement. Il s'agit d'un événement initiateur qui peut se transformer en un scénario d'événement dangereux selon la réponse des systèmes de protection disponibles.

D'autres événements initiateurs pouvant provoquer un rejet de gaz dans l'environnement pourraient inclure les fuites du matériel du procédé, la rupture de la tuyauterie, et des événements externes tels qu'un incendie. Pour cet exemple, seule la condition d'excès de pression est étudiée.

Le système instrumenté de sécurité a pour finalité, en cas de sollicitation, de fermer les deux vannes qui sont en redondance 1oo2. Ainsi, il faudrait la défaillance dangereuse des deux vannes pour qu'un signal d'alarme valide ne soit pas traité correctement.

Le système de sécurité n'est pas capable d'induire une situation dangereuse de lui-même. Le pire des cas qui peut se produire est une panne dangereuse, c'est-à-dire que le système ne peut effectuer sa fonction de sécurité prévue.

Les deux capteurs sont des transmetteurs intelligents de pression et sont également en redondance 1oo2. Des tests périodiques en ligne sont effectués par les deux transmetteurs. Une information concernant la comparaison des signaux de sortie des deux capteurs est effectuée et renvoyée à l'automate programmable.

Deux modes de défaillances peuvent affecter les différents types de composants. Il s'agit des défaillances sûres et des défaillances dangereuses.

5.2. Modèle des composants

La période d'échantillonnage est affectée au modèle du process (réservoir sous pression) et de ce fait tous les autres composants réagissent à des événements discrets.

La description globale du modèle sous Möbius est donnée et les modèles des composants du SIS sont montrés. Le modèle est conçu d'une façon hiérarchique et sa composition est donnée en figure 4.16.

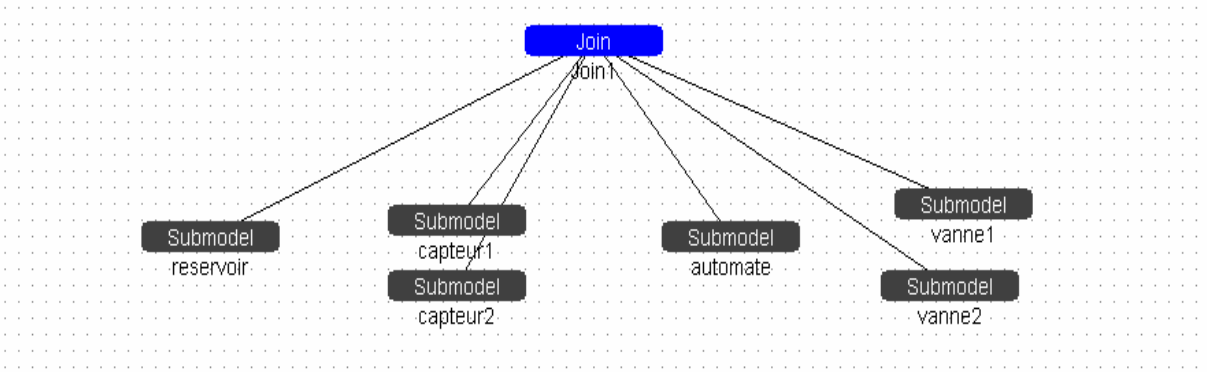


Figure 4.16 : Conception hiérarchique du process équipé du système de sécurité

5.2.1. Modèle du process

Le process (réservoir) et modélisé par un système échantillonné. Il est connecté aux capteurs à l'aide de la place "***vers_capteur***" qui est une place partagée. La place "***process***" contient un jeton de type *float* (réel) qui correspond à l'état normal du fonctionnement du réservoir et donc à la pression nominale.

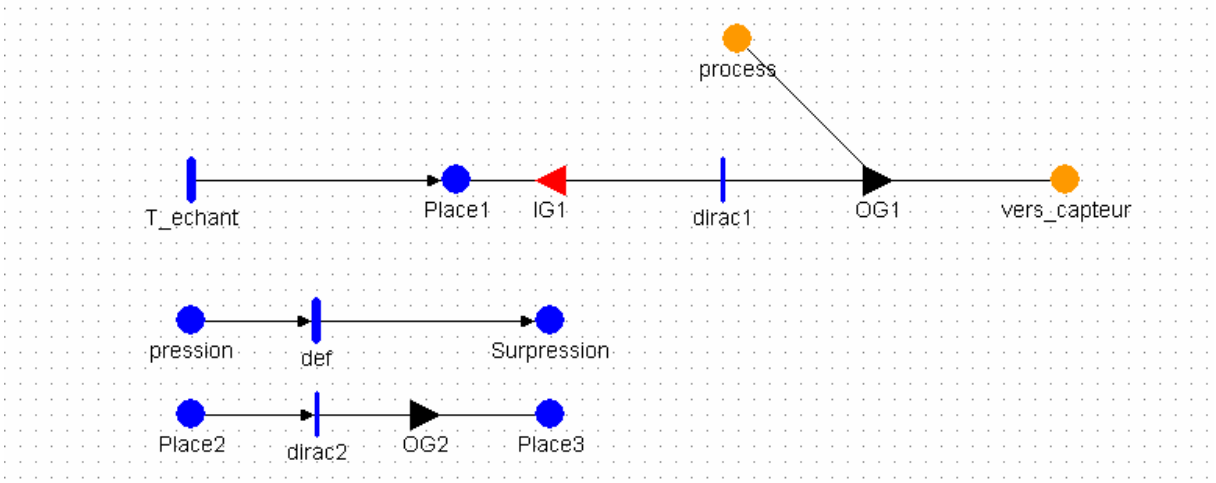


Figure 4.17 : Modèle SAN du réservoir

Pour le franchissement de la transition instantanée "***dirac1***", la porte d'entrée ***IG1*** permet le test sur la présence d'un jeton dans la "***Place1***". Le jeton apparaît dans cette place seulement aux instants k*Te (k = 0, 1, 2, 3, …), il est temporisé par la période d'échantillonnage (transition "***T_echat***"). Cette présence de jeton est synonyme de la possibilité de l'exécution de l'algorithme présent dans la porte de sortie OG1. En effet, la non occurrence de l'effet dangereux dans le réservoir qui prend la forme d'une surpression entraîne un fonctionnement normal et l'attribution de la marque de la place "***process***" à la place partagée "***vers_capteur***". En cas de surpression (présence d'un jeton dans la place "***surpression***"), la pression ne varie pas instantanément et elle va varier selon un système du premier ordre décrit par les équations suivantes :

$$x(k+1) = 0.99x(k) + 0.135u(k)$$
$$x(k) = x(k+1)$$

où *x(k+1)* et *x(k)* sont des variables internes du système et *u(k)* est une entrée. Après chaque simulation, les valeurs de *x(k+1)* et *x(k)* sont réinitialisées par la présence d'un jeton dans la "***Place2***".

La transition "***def***" dispose d'une distribution de loi exponentielle et le taux affecté à cette transition est calculée dans l'hypothèse de la faible demande.

Le système va évoluer aux instants k*Te (k=0,1, 2, 3, …). Cette évolution est observée dans la figure 4.18 avec l'adjonction d'une surpression.

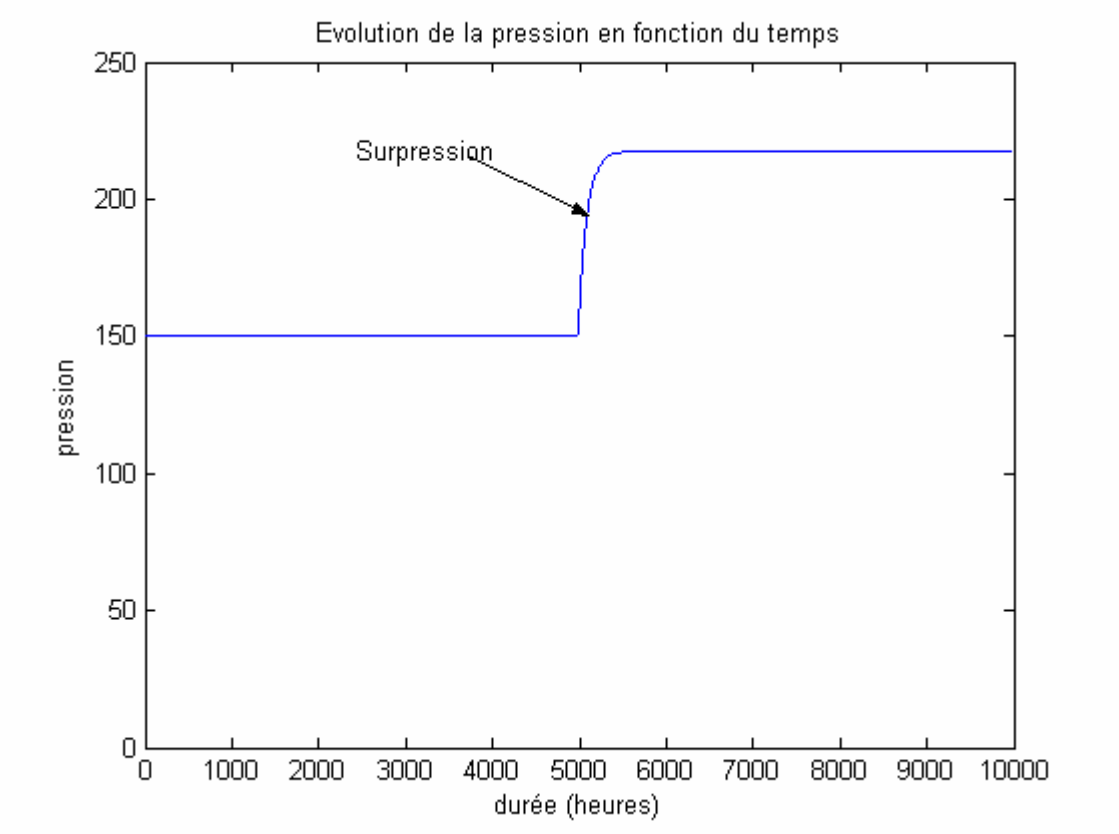


Figure 4.18 : Evolution de la pression dans le réservoir

Cette figure montre l'évolution de la pression dans le process (réservoir). On constate que la valeur nominale de la pression est de 150 et que l'événement dangereux a lieu dans cet exemple vers la date t = 4984 heures. Ce n'est évidemment pas la seule date à laquelle peut survenir cette surpression, en effet, d'autres simulations permettront d'avoir des dates autres que celle-là.

Aussitôt la surpression arrivée, la demande d'activation de la fonction de sécurité est déclenchée. Les deux vannes en redondance 1oo2 vont pouvoir assurer la mise en état sûr du process en cas de leur bon fonctionnement.

5.2.2. Modèle du capteur

Dans le modèle du capteur (figure 4.19), il y a cohabitation entre la partie fonctionnelle et la partie dysfonctionnelle. Les deux modes de défaillances qui affectent ce composant sont représentés dans la partie dysfonctionnelle par les places "***capt1_danger***" et "***capt1_sur***". Ces places caractérisent respectivement les défaillances dangereuses et les défaillances sûres. La transition "***def_capt1***" est tirée au moment de l'avènement de la défaillance qui suit une distribution exponentielle et qui est suivi d'une possibilité de couverture de diagnostic pour permettre de répartir les défaillances dans les deux modes existants. Le tir de la transition déterministe "***restore***" permet la restauration du composant vers l'état de fonctionnement normal représenté par la place "***capteur1_OK***".

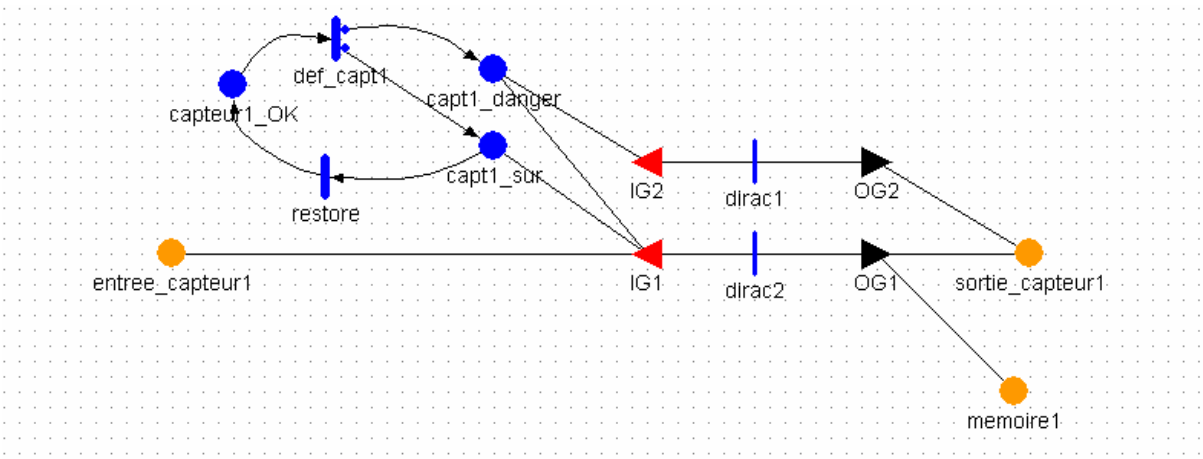


Figure 4.19: Modèle du capteur

La place "***entree_capteur1***" qui est une place partagée avec le modèle du réservoir dispose de la valeur de la mesure. A chaque période d'échantillonnage, une nouvelle mesure est établie et préparée pour l'envoi à condition que le capteur ne soit pas dans une situation de défaillance dangereuse. Les messages sont donc envoyés périodiquement. La défaillance dangereuse ne modifie pas la capacité de communication du capteur. Elle arrête uniquement la prise de mesures.

Pour le cas des défaillances sûres, la procédure utilisée (cf. chapitre1) est basée sur l'utilisation de modèles et elle consiste en la génération de résidus par la reconstruction de la sortie et sa comparaison avec la sortie mesurée et ensuite l'étape de la validation consiste en la prise de décision vis-à-vis de ce modèle qui ne donne qu'une approximation du comportement réel.

Ainsi, les résidus élaborés seront stockés dans la place "***memoire1***" et le contenu de cette place sera utilisé au moment où le capteur quitte son état de fonctionnement normal et se trouve en état de défaillances sûres.

5.2.3. Modèle de l'automate

La partie dysfonctionnelle est similaire pour tous les composants (capteurs, automate, actionneurs). Ce sont les traitements qui vont différer d'un composant à un autre suivant qu'on est dans cette situation ou une autre.

L'automate reçoit en son entrée les deux mesures qui proviennent des deux capteurs redondants. Les places "***entree1_automate***" et "***entree2_automate***" sont partagées avec les places de sorties de deux capteurs ("***sortie_capteur1***" pour le premier capteur dans la figure précédente par exemple). Au cas de la disponibilité d'au moins un des deux capteurs et du bon fonctionnement de l'automate, celui-ci va pouvoir élaborer un ordre (franchissement de la transition instantanée "***ordre***") et le transmettre aux deux actionneurs qui sont en redondance 1oo2. L'ordre transmis est soit ne rien faire lorsque la pression mesurée par les capteurs est nominale ou agir par la fermeture des actionneurs au cas où il y a une surpression.

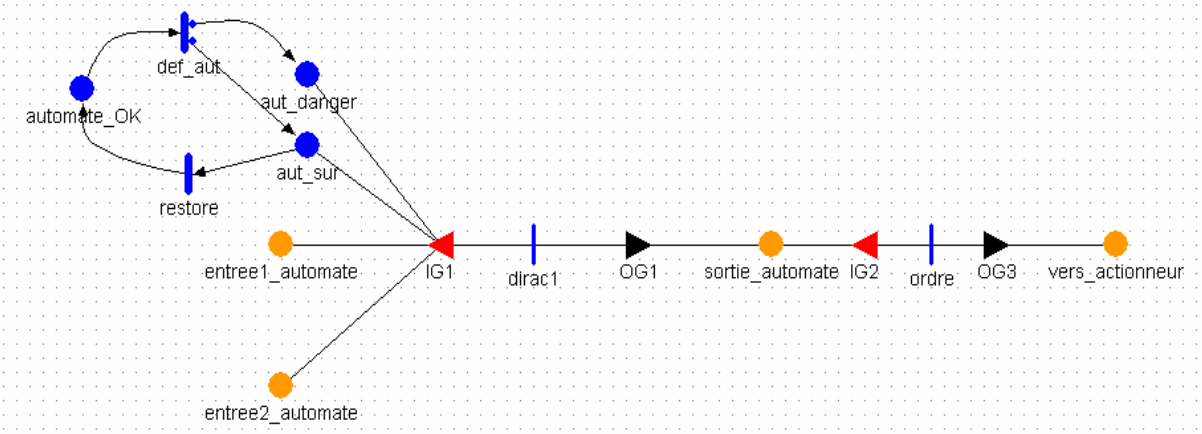


Figure 4.20 : Modèle de l'automate

5.2.4. Modèle de l'actionneur

L'autorisation de l'actionnement des actionneurs est assujettie à leur bon fonctionnement. En cas de défaillance, l'ordre émanant de l'automate ne peut aboutir.

Les actionneurs dans les applications relatives à la sécurité sont considérés comme des composants dormants. C'est pourquoi, la seule fois où ils vont être mis en actionnement est le cas de la surpression et l'apparition de l'événement dangereux dans le réservoir. Dans ce cas la place "***Place2***" sera marquée par un jeton qui va permettre le franchissement de la transition "***depression***" synonyme du retour à un état de sécurité.

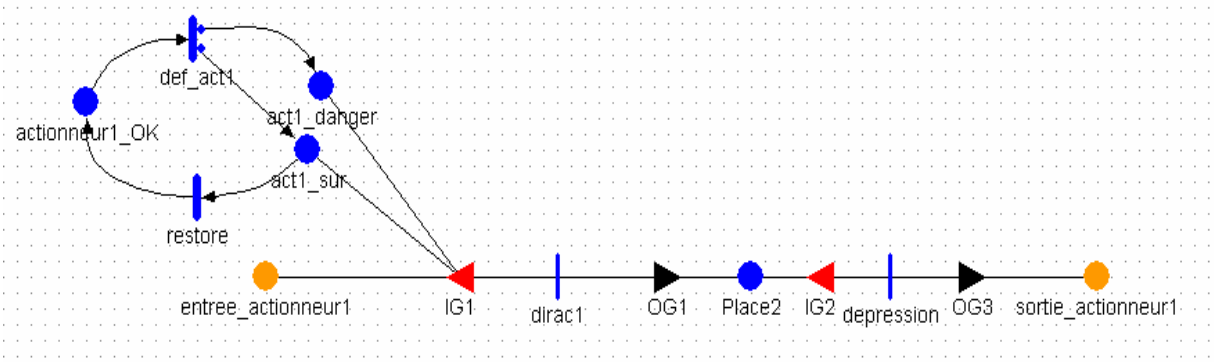


Figure 4.21 : Modèle de l'actionneur

Après interaction entre les différents composants du système global, celui-ci peut se trouver dans quatre états possibles.

5.3. Définition des états

Le système peut se trouver dans quatre types d'états :

- un état normal

- un état normal dégradé
- un état de défaillances sûres
- un état dangereux

5.3.1. Etat 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.

5.3.2. 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.

5.3.3. Etat de défaillances sûres

Dans l'état sûr, la sécurité est assurée pour le système. Cet état peut faire suite à l'apparition d'un événement dangereux (surpression dans le 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.

5.3.4. Etat dangereux

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.

La figure 4.22 regroupe les différents états du système ainsi que les transitions entre ces états.

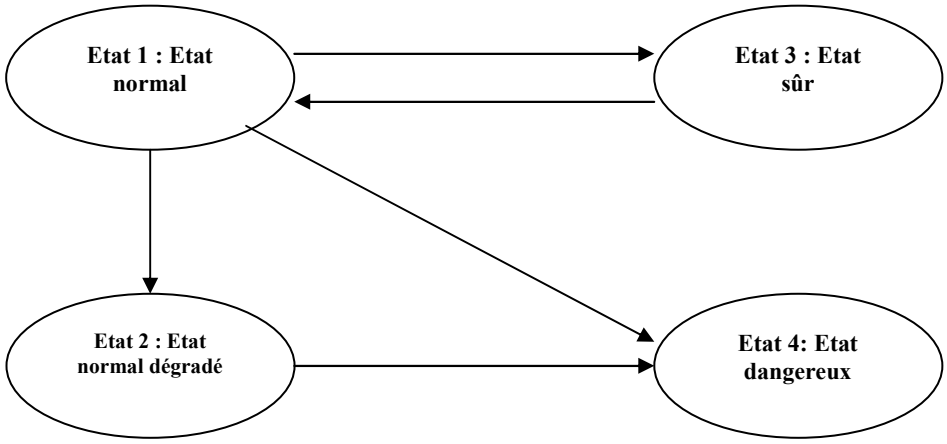


Figure 22 : Etats du système et transitions entre états

5.4. Fonctionnalité de validation au niveau des capteurs

La validation telle qu'elle a été décrite dans le chapitre 1 est reprise dans la modélisation des capteurs.

Le tableau 4.6 illustre le mécanisme de compensation élaboré au niveau des capteurs redondants et la logique de décision entreprise :

Capteur 1	Capteur 2	**état**
OK	OK	**1**
OK	Danger	**2**
OK	Sur	**1**
Sur	OK	**1**
Sur	Danger	**2**
Sur	Sur	**3**
Danger	OK	**2**
Danger	Danger	**4**
Danger	Sur	**2**

Tableau 4.6 : Etats des capteurs redondants

En effet, le module de reconstruction de la sortie incorporé dans les deux capteurs va permettre en cas de défauts de générer un résidu et la valeur de sortie sera substituée, ce qui permet la continuité du service. La logique de décision permet en fonction des états des deux

capteurs et par l'intermédiaire de la possibilité de la compensation de placer les deux capteurs dans un état correspondant conformément au tableau 4.6.

5.5. Performances en sécurité du système à réservoir de pression

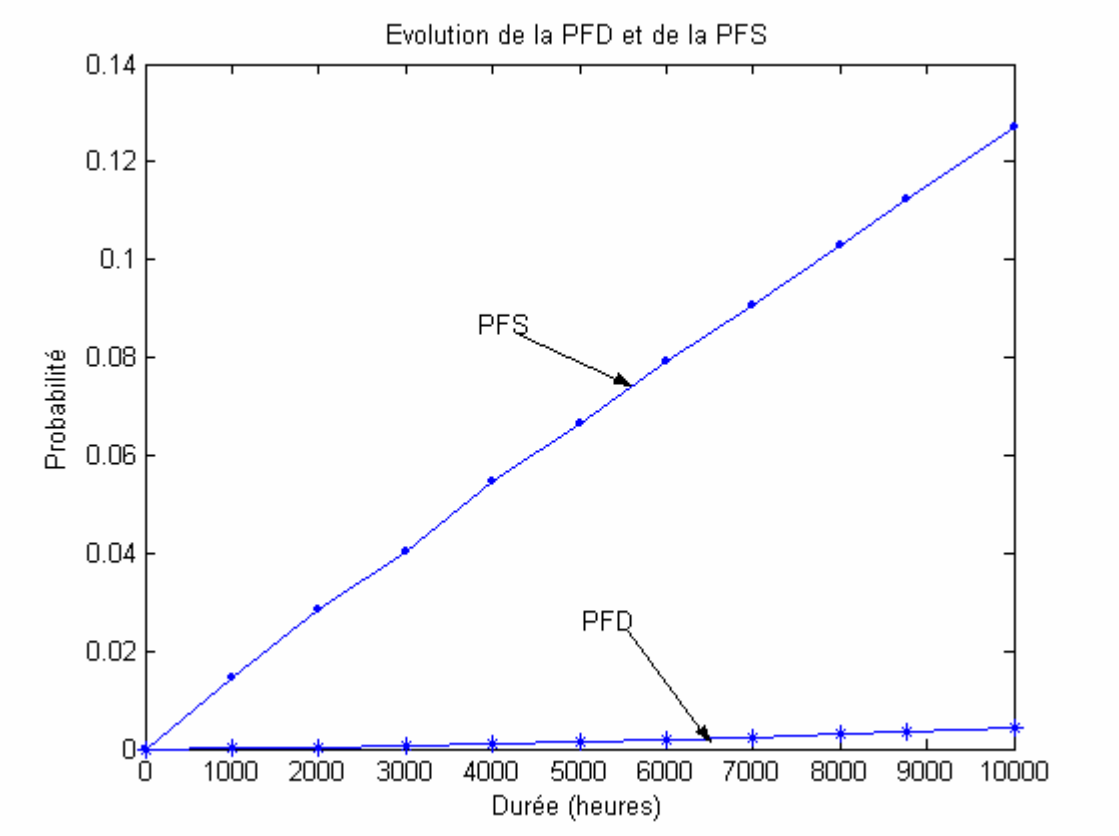


Figure 4.23 : PFD et PFS du système à réservoir

La figure 4.23 montre l'évolution 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 paramètres du modèle sont :

lambda_actionneur	float	9.0E-6
lambda_automate	float	8.10^{-7}
lambda_capteur	float	6.10^{-6}
lambda_demande	float	1.5E-4
capti	float	0
captimoin1	float	0
cd_capteur	float	0.75
cd_actionneur	float	0.75

cd_automate	float	0.75
periode_echantillonage	float	0.5
sd_capteur	float	24.0
sd_actionneur	float	24.0
sd_automate	float	24.0
ti	float	0
timoin1	float	0
residu	float	0
xk	float	0
xkplus1	float	0
ps1	int	0
ps2	int	0
plc	int	0
q	int	0
qu	int	0

Le taux de défaillance qui concerne l'événement dangereux dans le réservoir est choisi conformément à la clause 3.5.12. de la partie 4 de la norme qui stipule que l'on est en mode de faible demande : *lorsque la fréquence des demandes de fonctionnement sur un système relatif à la sécurité est plus grande que une par an et au plus égale à deux fois la fréquence des tests périodiques*.

Ceci se traduit par une fréquence comprise dans l'intervalle suivant :

$$1{,}141.10^{-4} < \textbf{\textit{lambda\_demande}} < 2{,}283.10^{-4}$$

La fonction traitement peut être plus au moins complexe. Elle peut se résumer à acquérir une grandeur mesurée par un capteur et à l'indiquer. Elle peut également récolter plusieurs informations émanant de plusieurs capteurs et en faire un traitement à partir d'une fonction combinatoire. Les unités de traitement peuvent être classées en deux catégories suivant leur technologie :

- ✓ Les technologies câblées, à base de composants logiques élémentaires (relais), liés entre eux électriquement,
- ✓ Les technologies programmées, à base d'automates programmables (API), de systèmes numériques de contrôle commande (SNCC), ou de cartes électroniques à microprocesseurs.

Dans la fonction instrumentée de sécurité relative au système étudié, la logique utilisée pour la fonction traitement est réduite aux composants câblés de telle façon à réaliser des fonctions logiques contrairement aux dispositifs de terrain qui disposent eux d'une intelligence locale.

Les technologies à relais sont considérés comme un bon choix pour la logique de traitement lorsque le nombre d'entrée/sorties est faible (moins de 6) et les modifications futures dans la logique de traitement sont hautement improbables [GOB 05].

Il faut attirer l'intention sur le fait que l'utilisation de cette logique câblée n'est pas suffisante pour assurer de meilleures performances en sécurité mais ceci est compensé par la cohabitation avec cette logique câblée d'instruments intelligents capables de compenser le manque laissé par les automates programmables. Ceux ci sont généralement composés d'une architecture particulière utilisant plusieurs microprocesseurs couplés à des circuits d'entrée et de sortie via des modules spécifiques. Cette panoplie de circuiterie fait en sorte que les automates programmables disposent de taux de défaillances additionnels et de nouveaux modes de défaillances.

[ISA 84] donne une relation qui illustre ces propos :

$$\lambda_{PLC} = n_{IC} \times \lambda_{IC} + n \times \lambda_{IP} + \lambda_{MP} + m \times \lambda_{OP} + m_{OC} \times \lambda_{OC}$$

où

n_{IC} : nombre des canaux d'entrées (*Input Channels*),

n : nombre des modules d'entrée (*Input modules*),

m : nombres des modules de sorties (*output modules*),

MP : processeur principal (*Main Processor*),

m_{OC} : nombre des canaux de sortie (*output Channels*).

Le taux de défaillance global d'un automate programmable est plus grand par rapport à celui d'une logique câblée à relais.

La valeur citée parmi les paramètres ci-dessus s'apparente à celle du taux de défaillance d'un système à logique câblée. Le taux est égal à 8.10^{-7} [GOB 05] tandis que pour l'automate utilisé pour le système classique comportant le niveau 0, en ce qui concerne l'intelligence dans les instruments, celui là dispose d'un taux de 2.10^{-5} (voir table 4.1).

Les autres paramètres cités ci-dessus sont utilisés pour la détermination du résidu pour la reconstruction de la sortie en cas de défauts dans le capteur (***capti***, ***captimoin1***, ***ti***, ***timoin1***, ***residu***) ou comme variables internes décrivant le fonctionnement dans quelques dispositifs (***xk***, ***xkplus1***) ou comme identificateurs propres aux dispositifs (***ps1***, ***ps2***, ***plc***).

La figure 4.23 montre les performances en sécurité d'un système instrumenté de sécurité à réservoir de pression. L'évolution des deux métriques qui décrivent les performances en sécurité du système étudié montrent une nette diminution de la probabilité de défaillances sûres et une augmentation de la probabilité de défaillances sûres. Une illustration est faite sur le tableau 4.7 suivant :

	Durée (heures)	SIS normal (niveau 0)	SIS avec validation (niveau 3)
PFD	*1000*	5.10^{-3}	2.10^{-4}
	5000	$2{,}25.10^{-2}$	$1{,}4.10^{-3}$
	8760	$4{,}13.10^{-2}$	$3{,}4.10^{-3}$
	10000	$4{,}79.10^{-2}$	$4{,}2.10^{-3}$
PFS	*1000*	$2{,}79.10^{-2}$	$1{,}46.10^{-2}$
	5000	$1{,}351.10^{-1}$	$6{,}64.10^{-2}$
	8760	$2{,}221.10^{-1}$	$1{,}123.10^{-1}$
	10000	$2{,}513.10^{-1}$	$1{,}273.10^{-1}$

Tableau 4.7 : Comparaison des performances en sécurité

L'adjonction de la fonctionnalité validation telle qu'elle a été décrite auparavant a contribué à l'amélioration des performances en sécurité d'une façon significative. En effet, la probabilité de défaillances dangereuses a nettement diminué alors que la probabilité de défaillances sûres a sensiblement diminué par rapport aux valeurs relatives à un SIS classique. Notons que ces probabilités correspondent respectivement à la présence dans les états 4 et 3 décrits dans la figure 4.24. Nous relevons donc une forte diminution de la valeur de la PFD due essentiellement à la transformation de quelques cas dangereux induisant le système dans un état dégradé (2). D'ailleurs, la probabilité de siéger dans cet état est passée de $2{,}87510^{-2}$ pour le SIS normal à $7{,}03.10^{-2}$ lorsqu'il y a validations dans les deux capteurs. Ceci montre clairement que la présence du système dans cet état quasi normal (état dégradé) s'est accrue en affectant aussi la probabilité des défaillances dangereuses. La nette diminution de la valeur de la PFS par rapport aux valeurs du système SIS classique a pour motif la prise en compte dans les capteurs de pression des valeurs octroyées par le modèle qui décrit la fonctionnalité de la validation. En effet, en présence de défaillances sûres, la continuité du service peut être assurée. L'impact est pressenti globalement dans le système de sécurité.

La valeur moyenne de l'indisponibilité de la fonction de sécurité donnée par la PFD_{moy} pour une durée de simulation de 10000 heures qui correspond à un intervalle entre deux tests périodiques est de $1{,}707.10^{-3}$. Le système est par conséquent dans un état correspondant au SIL 2. Pour le système normal (niveau 0), la valeur moyenne de l'indisponibilité de la fonction de sécurité $PFD_{moy} = 2{,}33.10^{-2}$, ce qui correspond à un système SIL 1. Nous constatons que le niveau de SIL a changé et il est amélioré du fait qu'il est passé du niveau 1 au niveau 2. Ce résultat illustre bien la contribution des instruments intelligents dans les boucles de sécurité.

La figure 4.24 montre l'évolution des deux métriques (PFD et PFS) et illustre les chutes de leurs valeurs lorsque nous sommes passés d'un système classique à un système SISID.

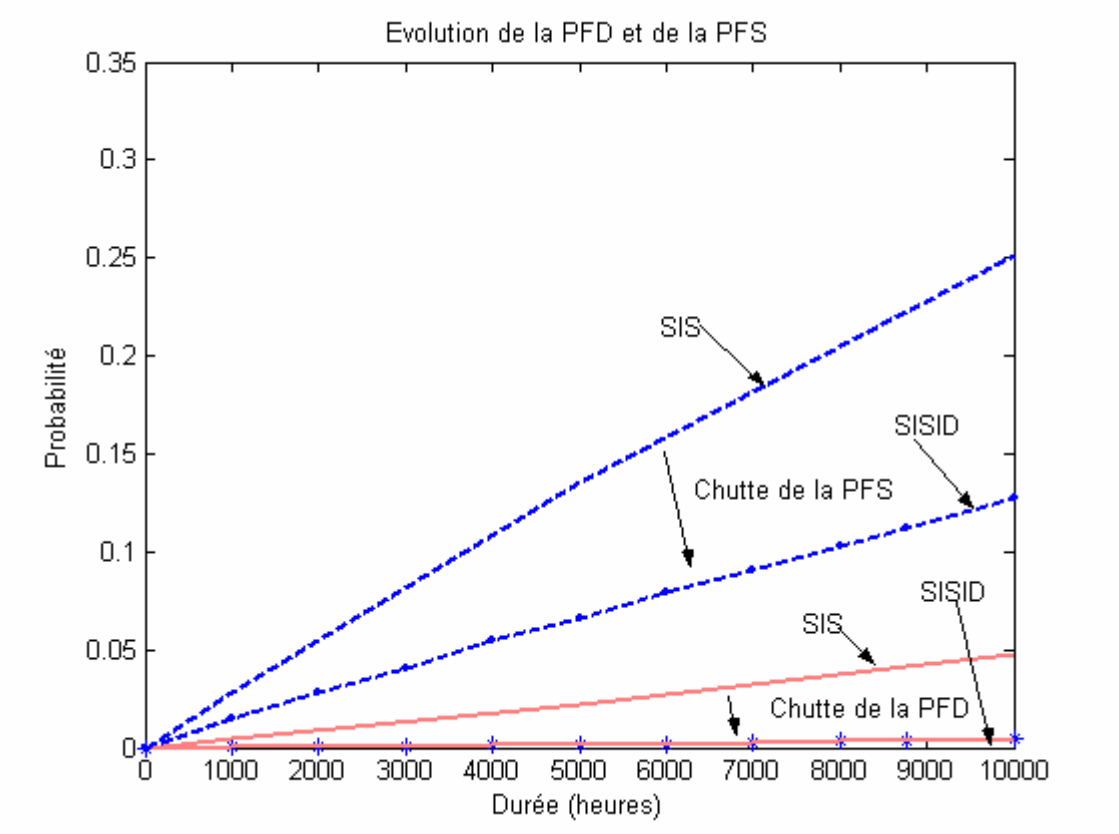


Figure 4.24 : Chute des deux métriques

Le tableau 4.8 donne les pourcentages de temps passé dans les différentes zones SIL. Ce tableau montre qu'il existe une cohérence apparente entre la valeur de la PFD_{moy} et le temps passé dans les différentes zones SIL.

SIL	Pourcentage de temps passé dans les zones SIL (%)
SIL0	0
SIL1	0
SIL2	70,73
SIL3	26,35
SIL4	2,92

Tableau 4.8 : Pourcentage de temps passé dans les zones SIL

5.6. Indicateurs de performances

De la même façon, nous reprenons les deux indicateurs de performances IP_{PFD} et IP_{PFS} décrits auparavant pour faire la correspondance entre les niveaux d'intelligence et les performances en sécurité.

Le calcul de ces deux indicateurs nous donne les valeurs suivantes : IP_{PFD} = 0.011 et IP_{PFS} = 0.432.

Ces valeurs correspondent donc à l'introduction d'une intelligence niveau 3 tel que cela était décrit au chapitre 1.

Nous constatons que le niveau 3 d'intelligence a de l'influence directe sur les performances en sécurité. L'amélioration est nettement aperçue dans les valeurs des indicateurs de performances qui se trouvent diminués.

5.7. Conclusion

Malgré la nette diminution de la valeur de la PFS, l'influence sur le SIL du système est faible car le niveau d'intégrité de sécurité qui décrit en quelques sorte la qualité d'un système de sécurité ne se mesure que par la probabilité de défaillances dangereuses. Sa notion est en quelque sorte une mesure de la confiance avec laquelle le système peut s'attendre à exécuter la fonction de sécurité. Or, ceci est très restrictif, et ce point là est l'une des faiblesses de la norme CEI 61508 qui accorde un niveau de confiance aux systèmes disposant d'un niveau de SIL élevé sans se préoccuper du taux de défaillances sûres.

Dans la suite, nous allons inclure des défaillances possibles des modules qui assurent le diagnostic pour voir l'impact de ce mode de défaillance additionnel sur les performances en sécurité du système.

6. Inclusion des défaillances de la fonctionnalité validation dans le modèle dysfonctionnel du capteur

Dans cette partie, nous allons introduire la défaillance possible du modèle qui reconstruit la sortie. En effet, une défaillance dans le circuit de diagnostic ne possède pas un impact immédiat sur le bon fonctionnement d'un capteur. Le capteur va continuer à fonctionner normalement. Toutefois, un défaut de diagnostic dans le circuit du capteur permet de créer une situation potentiellement dangereuse sur avènement d'une deuxième faute, la défaillance du diagnostic va être incluse dans l'analyse de la PFD moyenne.

6.1. Description des états du capteur

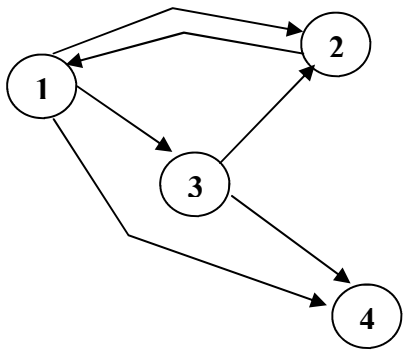


Figure 4.25 : Différents états du capteur de pression

Les états 1, 2 et 4 représentent respectivement l'état de bon fonctionnement du capteur, l'état de défaillances sûres et l'état de défaillances dangereuses. Ces états sont communs au capteur décrit dans le modèle du système de sécurité utilisé pour le réservoir de pression. L'état nouveau est l'état 3 qui se comporte comme un état dégradé au niveau du capteur qualifiant la défaillance de l'élément qui assurait la redondance fonctionnelle.

6.2. Modèle SAN du capteur

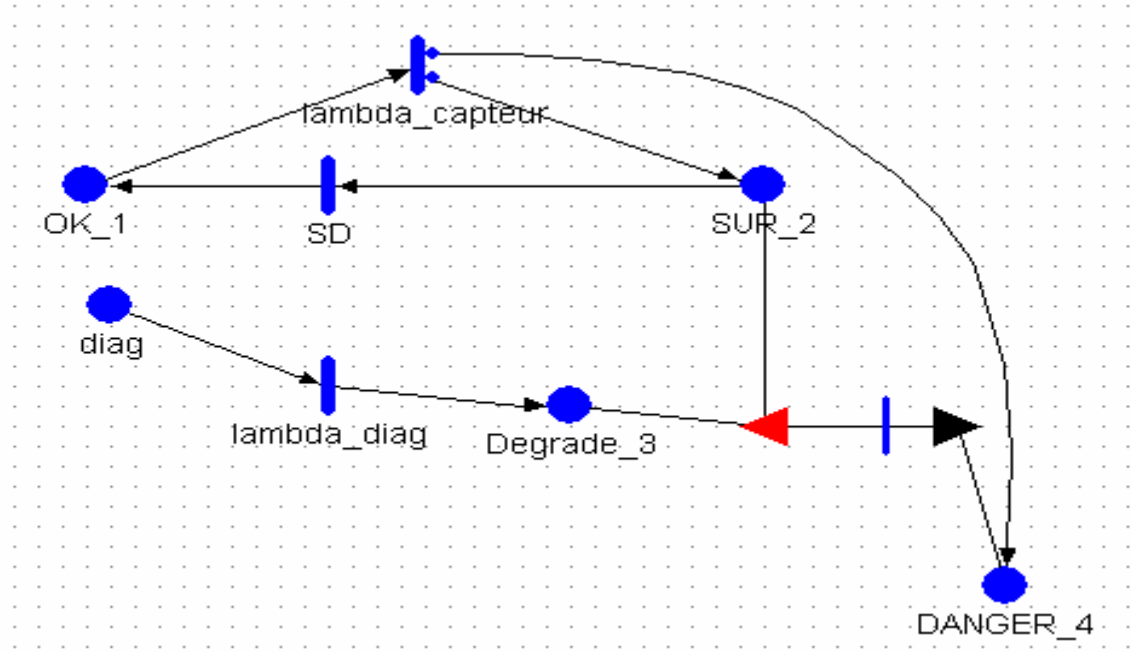


Figure 4.26 : Modèle SAN du capteur

Dans le modèle décrit par la figure 4.26, le capteur fonctionne avec succès dans les places ***OK_1*** et ***Degrade_3***. Ces places représentent les états de bon fonctionnement (1 et 3) décrits dans la figure 4.24. La défaillance du module relatif au diagnostic (tir de la transition ***lambda_diag***) entraîne l'exposition du capteur à un état de danger si celui-ci se trouvait dans un état de défaillances sûres puisque le module de diagnostic ne peut plus révéler les défaillances sûres.

La simulation de ce modèle qui tient compte des défaillances du module de diagnostic pour un temps de mission de 8760 heures nous a permis d'obtenir une probabilité de défaillances dangereuses d'une valeur de $1{,}29.10^{-2}$. Alors que la valeur de cette probabilité en ayant un module de diagnostic sans défaillances est de $1{,}25.10^{-2}$.

Cette donnée va avoir bien entendu un impact sur la PFD du système global. Il faut noter aussi que d'autres modes de défaillance sont nécessaires pour se procurer des informations sur les performances de sécurité et ceci a été mis en évidence par l'exemple d'application de ce capteur.

7. Conclusion

Dans ce chapitre, 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 performations en sécurité. Le modèle construit à base de réseaux d'activité stochastiques permet de modéliser des architectures de SIS avec des facilités offertes par un pouvoir de composition hiérarchique de l'outil de modélisation. Le choix des réseaux d'activité stochastiques qui sont une extension des réseaux de Petri stochastiques s'est avéré être adéquat pour mener à bien l'élaboration du modèle. Ce modèle a ainsi pu être simulé grâce à l'outil Möbius. 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.

Nous avons pu à travers le premier exemple montrer 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. L'exemple du réservoir dans lequel nous avons introduit des modules de validation a permis de pressentir l'action que peut avoir leur inclusion sur les défaillances sûres du système. Nous avons aussi traité le cas de la défaillance de ces modules qui a pour conséquence l'augmentation des défaillances dangereuses du système.

Nous avons pu percevoir que la notion de SIL qui revêt un grand intérêt selon la norme CEI 61508, semble insuffisante pour obtenir une bonne image de la réalité des risques encourus. L'évaluation du pourcentage de temps que passe le système dans chaque zone SIL permet d'obtenir une indication plus précise.

L'introduction des indicateurs de performances nous a permis de mieux faire la correspondance entre les niveaux d'intelligence requis dans les instruments et les performances globales en sécurité.

Conclusion générale et perspectives

Conclusion générale et perspectives

Bilan

L'objectif de nos travaux était d'évaluer la sûreté de fonctionnement des systèmes instrumentés de sécurité intégrant de l'intelligence, afin de vérifier l'impact de l'utilisation des instruments intelligents dans les applications sécuritaires conformément aux nouvelles normes relatives à la sécurité CEI 61508 et CEI 61511.

La complexité des systèmes comportant des instruments intelligents ainsi que les exigences en matière de sécurité recommandées par les normes rendent délicate la modélisation de ces systèmes et leur évaluation d'un point de vue sûreté de fonctionnement devient non triviale.

Ces systèmes sont généralement programmés et ils disposent éventuellement de multiples modes de défaillances pour un composant, les modes de défaillance ayant des effets différents sur le système, à architecture fonctionnelle variable pour une architecture matérielle donnée et ils sont souvent soumis à des tests périodiques et autotests, ce qui induit la co-existence de défaillances détectées et de défaillances non détectées, avec une très forte influence du taux de détection sur les caractéristiques de sûreté de fonctionnement du système.

Toutes ces caractéristiques font qu'ils sont particulièrement difficiles à modéliser, surtout si l'on veut utiliser des modèles classiques en sûreté de fonctionnement, tels que les arbres de défaillances. Nous avons exploré différentes voies pour modéliser et obtenir des résultats qualitatifs (coupes minimales, séquences amenant à un état indésirable) et/ou quantitatifs (indisponibilité, défiabilité) sur de tels systèmes.

L'appréhension qualitative de la logique de dysfonctionnement du système conduisant à un événement redouté prédéfini impose la méthode de l'arbre des défaillances. La représentation par graphes d'états (Markov) permet la modélisation de l'évolution prévisible du système. La méthode de l'arbre des défaillance est basée sur la logique booléenne pour représenter le système étudié et elle est adaptée à des systèmes à configuration statique, c'est-à-dire des systèmes dont les relations fonctionnelles entre leurs composants restent figées. Cette méthode est donc inappropriée dans le cas de nos travaux. La modélisation avec les graphes de Markov permet de prendre en compte les dépendances temporelles et stochastiques plus largement que les méthodes classiques. En dépit de leur simplicité conceptuelle et leur aptitude à pallier certains handicaps des méthodes classiques, les graphes de Markov souffrent de l'explosion du nombre des états, car le processus de modélisation implique l'énumération de tous les états possibles et de toutes les transitions entre ces états. Cette seconde approche

est fortement limitée par le fait que les lois régissant les transitions entre états doivent être du type exponentiel (taux de défaillance et de réparation constants). Or les durées de fonctionnement avant défaillance de nombreux composants ou systèmes ne suivent pas complètement une loi exponentielle et des lois de Dirac peuvent être mises en jeu conjointement. On peut donc en conclure que l'approche markovienne ne peut contribuer à la résolution du problème posé.

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 les SAN (*Stochastic Activity Network*). Les SAN sont un formalisme de modélisation puissant et sont une extension des réseaux de Petri stochastiques. Les SAN conservent toute la puissance de modélisation des réseaux de Petri stochastiques par l'emploi d'activités stochastiques. Un autre avantage des SAN est manifesté par le pouvoir d'accéder aux différents marquages de toutes les places à chaque instant moyennant des portes d'entrée et de sortie. Ce formalisme de modélisation est couplé à la technique de simulation (simulation de Monte Carlo) pour l'évaluation des performances. L'association des réseaux d'activités stochastiques à une méthode de simulation de Monte-Carlo constituent une approche alternative puissante pour évaluer la performance globale en sûreté de fonctionnement des systèmes présentant des aspects temporels et dynamiques.

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 Möbius. 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.

La modélisation de tous les dispositifs est conçue d'une manière hiérarchique, en partant des modèles de base du système. La composition est formée par la jonction des modèles de base qui constituent des structures génériques sous forme de bibliothèque de composants. L'évaluation des performances en sécurité est assurée par la détermination des deux métriques PFD et PFS qui se rapportent aux deux modes de défaillances cités par la norme mais aussi du niveau d'intégrité de sécurité (SIL).

A travers nos travaux, nous avons pu parvenir aux résultats suivants :

- ✓ Nous avons pu élaborer un modèle fonctionnel d'instrument intelligent intégrant un ensemble de fonctionnalités relatives au capteur intelligent et à l'actionneur intelligent pour tendre vers plus de généricité.
- ✓ A travers un premier exemple, 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.
- ✓ Nous avons pu constater par l'introduction des indicateurs de performances qu'il existe un impact direct du niveau d'intelligence sur les performances en sécurité. L'amélioration est nettement aperçue dans les valeurs des indicateurs de performances pour des applications à niveau élevé d'intelligence (exemple du réservoir).

- ✓ La notion de SIL qui revêt un grand intérêt selon la norme CEI 61508, semble insuffisante pour obtenir une bonne image de la réalité des risques encourus. L'évaluation du pourcentage de temps que passe le système dans chaque zone SIL permet d'obtenir une indication plus précise. En effet, l'exemple traité nous a permis de déterminer le niveau de SIL relatif à chaque système et de voir que l'apport de l'intelligence permet de couvrir les zones de niveaux de SIL exigés par la norme pour un SIS qui disposait d'un niveau de SIL 1 mais qui ne pouvait pas être maintenu pendant toute la durée entre deux tests d'intervalle.
- ✓ La valeur PFD qui est une exigence à satisfaire le niveau d'intégrité de sécurité de la norme CEI 61508 ne peut à elle seule décrire les performances en terme de sécurité pour les systèmes et il faut inclure la valeur PFS pour laquelle il n'existe pas actuellement de prescriptions dans le monde de la sécurité internationale, bien que les utilisateurs de système de sécurité exigent un niveau aussi bas que possible de la valeur de la PFS.
- ✓ En terme de méthodologie, nous avons pu dans nos modèles faire cohabiter l'interaction entre l'aspect fonctionnel et l'aspect dysfonctionnel pour la description du comportement du système en introduisant aussi le modèle de la demande d'activation de la fonction de sécurité. L'approche que nous proposons consiste à créer un modèle global sur lequel s'appuie l'analyse quantitative. Il est composé d'une partie fonctionnelle spécifiant le comportement du système et d'une partie dysfonctionnelle. Cette dernière consiste à formaliser l'occurrence de défaillances de composants susceptibles de tomber en panne.

Perspectives

Les résultats obtenus dans cette thèse se situent dans le cadre formulé par un ensemble d'hypothèses: composants non réparables, taux de défaillance constants, absence de causes communes de défaillances. Les perspectives de ces travaux visent à revenir sur ces hypothèses en proposant et en mettant en évidence quelques perspectives d'extension des résultats obtenus :

- ✓ Concernant les normes CEI 61508 [CEI 00] et CEI 61511 [CEI 03] :
  - o La prise en compte des paramètres qui figurent dans ces normes tels que le facteur β de défaillances de cause commune. La prise en compte de ce facteur se fait en ajoutant au modèle dysfonctionnel des instruments en redondance le modèle SAN à ces défaillances de cause commune.
  - o L'exploration du cas des systèmes disposant de taux de demandes élevé ou continu. Cela implique l'évaluation du taux de défaillances par heure (PFH) comme exigé par les normes dédiées à la sécurité CEI 61508 et CEI 61511.
  - o L'analyse de l'impact sur les défaillances sûres spécialement en relation avec la fraction des défaillances sûres.
- ✓ La généralisation du cas de l'incorporation de l'intelligence niveau 3 à une architecture répartie disposant d'une multitude d'instruments intelligents communicant entre eux et échangeant leurs informations.
- ✓ Le traitement du cas de la défaillance du réseau de communication (pertes de trames…) et voir son influence sur les paramètres en sécurité.

- ✓ L'utilisation d'un réseau de terrain dédié à la sécurité dans l'architecture globale du système de sécurité.

Annexes

Annexe 1 : La sûreté de fonctionnement

La sûreté de fonctionnement

1. Concepts de la sûreté de fonctionnement

La sûreté de fonctionnement est la science de défaillances [VIL 88]. Elle inclut ainsi leur connaissance, leur évaluation, leur prévision, leur mesure et leur maîtrise. Au sens strict, c'est la propriété qui permet à ses utilisateurs de placer une confiance justifiée dans la qualité du service délivré [LAP 88].

Les entraves de la sûreté de fonctionnement : fautes, erreurs et défaillances sont les circonstances indésirables, causes ou résultats de la non sûreté de fonctionnement.

Une ***défaillance*** du système survient lorsque le service délivré dévie de l'accomplissement de la fonction du système, c'est-à-dire de ce à quoi le système est destiné. Une ***erreur*** est la partie de l'état du système qui est susceptible d'entraîner une défaillance, c'est-à-dire qu'une défaillance se produit lorsque l'erreur atteint l'interface du service fourni, et le modifie. Une ***faute*** est la cause adjugée ou supposée d'une erreur. Il existe donc une chaîne causale entre faute, erreur et défaillance.

La sûreté de fonctionnement englobe les attributs suivants :

- ✓ La fiabilité qui est l'aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné,
- ✓ La disponibilité qui est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs est assurée,
- ✓ La maintenabilité qui est l'aptitude d'une entité à être maintenue ou rétablie, sur un intervalle de temps donné, 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,
- ✓ L'intégrité qui est la non-occurrence d'altérations inappropriées de l'information,
- ✓ La sécurité confidentialité (ou encore immunité) qui est l'absence de divulgation non autorisée d'informations,
- ✓ La sécurité innocuité, qui est la non-occurrence de conséquences catastrophiques pour l'homme, l'environnement et les biens.

L'association des qualificatifs *innocuité* et *immunité* permet de lever l'ambiguïté associée à *sécurité*. Il est à noter que cette ambiguïté n'existe pas en anglais, qui dispose de ***safety*** pour la sécurité innocuité et de ***security*** pour la sécurité-immunité, sûreté de fonctionnement étant ***dependability***.

Le développement d'un système sûr de fonctionnement passe par l'utilisation combinée d'un ensemble de méthodes, appelées moyens de la sûreté de fonctionnement, qui peuvent être classées en :

- ✓ Prévention des fautes, comment empêcher par construction, l'occurrence ou l'introduction de fautes
- ✓ Tolérance aux fautes, comment fournir par redondance, un service conforme à la spécification en dépit des fautes,
- ✓ Elimination des fautes, comment minimiser par vérification la présence de fautes,
- ✓ Prévision des fautes, comment estimer la présence, la création et les conséquences de fautes.

Le schéma complet de la taxonomie de la sûreté de fonctionnement est donné à la figure A.1 :

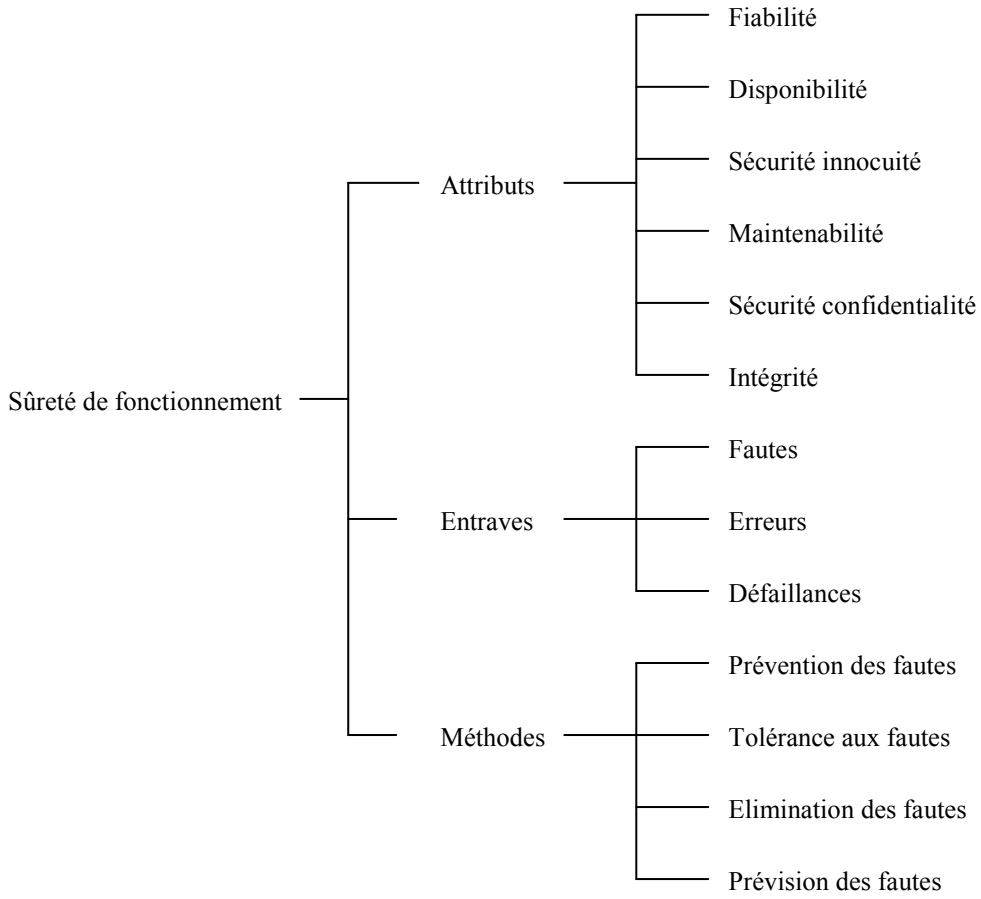


Figure A.1 : Taxonomie de la sûreté de fonctionnement [AVI 04]

2. Méthodes d'analyse de la sûreté de fonctionnement

Les méthodes d'analyse de la sûreté de fonctionnement utilisent pour la plus part une décomposition des grands systèmes en sous-systèmes ou composants individuels dont les caractéristiques sont supposées connues.

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. Les

principales méthodes utilisées lors d'une analyse de la sûreté de fonctionnement sont décrites ci-dessous.

2.1. Analyse préliminaire de risques

L'Analyse Préliminaire des Risques (APR) est une extension de l'Analyse Préliminaire des Dangers (APD) qui a été utilisée pour la première fois aux Etats-Unis, au début des années soixante [VIL 88]. Depuis, cette utilisation s'est généralisée à de nombreux domaines tels que l'aéronautique, chimique, nucléaire et automobile.

Cette méthode a pour objectifs :

1) d'identifier les dangers d'un système et de définir ses causes,

2) d'évaluer la gravité des conséquences liées aux situations dangereuses et les accidents potentiels.

L'APR permet de déduire tous les moyens, toutes les actions correctrices permettant d'éliminer ou de maîtriser les situations dangereuses et les accidents potentiels. Il est recommandé de commencer l'APR dès les premières phases de la conception. Cette analyse sera vérifiée, 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 l'étude de sûreté de fonctionnement, en particulier par la méthode des arbres de défaillances qui sera décrite par la suite.

2.2. L'analyse des modes de défaillances, de leurs effets et de leur criticité

L'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC) est une extension naturelle de l'Analyse des Modes de Défaillance et de leurs Effets (AMDE) utilisée pour la première fois à partir des années soixante pour l'analyse de la sécurité des avions [VIL 88]. L'AMDEC considère la probabilité d'occurrence de chaque mode de défaillance et la classe de gravité de ces défaillances, mais aussi les classes correspondantes de probabilités d'occurrence plus que les probabilités elles-mêmes. On peut ainsi s'assurer que les modes de défaillance ayant d'importants effets ont des probabilités d'occurrence suffisamment faibles, grâce aux méthodes de conception, aux diverses vérifications et aux procédures de test.

2.3. Arbres des causes

La méthode a pour objectifs [VIL 88] la détermination des diverses combinaisons possibles d'événements qui entraînent la réalisation d'un événement indésirable unique, la représentation graphique de ces combinaisons sous forme d'une structure arborescente.

Un arbre des causes est composé de portes et d'événements. Les événements sont combinés par les portes classiques (ET, OU) ou des portes étendues (*m* sur *n*…).

L'analyse par arbre des causes est une analyse déductive qui permet de représenter graphiquement les combinaisons d'événements qui conduisent à la réalisation de l'événement redouté.

L'analyse par arbre des causes doit rechercher, à partir d'un événement indésirable (ou redouté), les défaillances de composants dont la combinaison entraîne l'apparition de l'événement indésirable.

Deux aspects d'analyse peuvent être élaborés :

- ✓ l'aspect qualitatif en déterminant l'ensemble des coupes minimales (la coupe minimale est la combinaison d'événements de base entraînant l'événement redouté),
- ✓ l'aspect quantitatif permettant la détermination par un calcul la probabilité d'apparition de l'événement redouté ou indésirable.

L'analyse par arbre des causes est largement utilisée dans les études de sûreté de fonctionnement car elle caractérise de façon claire les liens de dépendance, du point de vue dysfonctionnement, entre les composants d'un système. Bien que cette méthode soit efficace, elle présente des limites. L'une de ces limites est que l'ordre d'occurrence des événements menant vers l'état redouté n'est pas pris en compte.

2.4. Diagrammes de fiabilité

Un diagramme de fiabilité permet le calcul de disponibilité ou la fiabilité du système modélisé, mais avec les mêmes restrictions qu'un Arbre des causes. Tous les chemins entre l'entrée et la sortie décrivent les conditions pour que la fonction soit accomplie. On suppose que les composants n'ont que deux états de fonctionnement (fonctionnement correct ou panne).

2.5. Analyse de Markov

La méthode de graphes de Markov est utilisée pour analyser et évaluer la sûreté de fonctionnement des systèmes réparables. La construction d'un graphe de Markov consiste à identifier les différents états du système (défaillants ou non défaillants) et chercher comment passer d'un état à un autre lors d'un dysfonctionnement ou d'une réparation. A chaque transition, de l'état E_i vers l'état E_j, est associé un taux de transition τ_{ij} défini de telle sorte que $\tau_{ij}.dt$ est égal à la probabilité de passer de E_i vers E_j entre deux instants très proches t et t+dt sachant que l'on est en E_i à l'instant de temps t.

Les états sont classés en deux catégories :

- ✓ Des états de fonctionnement : ce sont les états où la fonction du système est réalisée, des composants du système pouvant être en panne, l'état du bon fonctionnement est l'état où aucun composant n'est en panne,
- ✓ Des états de panne : ce sont des états où la fonction du système n'est plus réalisée, un ou plusieurs composants du système étant en panne.

Le processus d'analyse comprend trois parties :

- ✓ Le recensement et le classement de tous les états du système en états de bon fonctionnement ou états de panne.
- ✓ Le recensement de toutes les transitions possibles entre ces différents états et l'identification de toutes les causes de ces transitions.
- ✓ Le calcul des probabilités de se trouver dans les différents états au cours d'une période de vie de système ou le calcul des caractéristiques de sûreté de fonctionnement.

La modélisation avec les graphes de Markov permet de prendre en compte les dépendances temporelles et stochastiques plus largement que les méthodes classiques. En dépit de leur simplicité conceptuelle et leur aptitude à pallier certains handicaps des méthodes classiques,

les graphes de Markov souffrent de l'explosion du nombre des états [MON 98], car le processus de modélisation implique l'énumération de tous les états possibles et de toutes les transitions entre ces états.

Annexe 2 : Les réseaux de Petri

Les réseaux de Petri

1. Introduction

Les réseaux de Petri constituent un outil mathématique de modélisation développé au début des années soixante par le mathématicien allemand Carl Adam Petri. Les réseaux de Petri décrivent des relations existant entre des conditions et des événements et ils modélisent le comportement de systèmes dynamiques à événements discrets [DAV 97].

Les réseaux de Petri présentent des caractéristiques intéressantes à savoir le parallélisme, la synchronisation, le partage des ressources,…

2. Notions de base

2.1. Structure d'un réseau de Petri

Un réseau de Petri comporte deux types de nœuds, les places et les transitions reliés par des arcs orientés. L'état d'un système est représenté par son marquage.

Un RdP ordinaire non marqué est un quadruplet Q = < P, T, Pré, Post > tel que :

P = { P1, P2, …, Pn } est un ensemble fini et non vide de places,

T = { T1, T2, …, Tn } est un ensemble fini et non vide de transitions,

P ∩ T = Ø, P et T sont disjoints,

Pré : P x T → { 0, 1 } est l'application d'incidence avant ;

Post : P x T → { 0, 1 } est l'application d'incidence arrière.

Un marquage initial est une distribution des marques dans l'ensemble des places P à l'instant 0.

Si on associe au couple Pi, Tj (Ti, Pj) la valeur 0, alors il n'existe pas d'arc entre Pi et Tj (Ti et Pj), sinon (à ce même couple, on associe la valeur 1) il existe un arc de poids (valuation) 1 entre ces deux arcs.

Le RdP noté Q = < P, T, Pré, Post > est dit réseau de Petri ordinaire [DAV 97].

La représentation graphique d'un réseau de Petri utilise des cercles pour représenter les places et des traits (rectangles parfois) pour représenter les transitions. Les arcs sont des flèches auxquelles on associe la valuation (si elle nulle, on ne représente pas d'arc, il n'existe pas).

Exemple de réseau de Petri

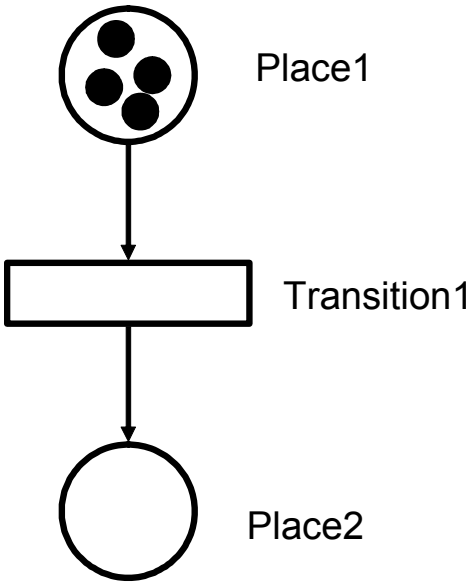


Figure A2.1 : Exemple d'un réseau de Petri

2.2. Marquage

Le marquage M d'un réseau de Petri est une application de P vers IN :

$$M : P \rightarrow IN$$

La figure A2.1 représente un réseau de Petri marqué. Les places 1 et 2 contiennent des nombres entiers (positifs ou nuls) de marques ou jetons. Le nombre de marques contenu dans la place P1 est noté M(P1) et on a M(P1) = 4. Pour le même exemple, M(P2) = 0. Le marquage M du réseau entier est défini par le vecteurs de ces marquages tel que M = (M(P1), M(P2)) = (4, 0), dans le cas de la figure précédente. L'état à un certain instant définit l'état du RdP qui reflète l'état du système modélisé par le réseau. L'évolution du marquage par franchissement des transitions dans un RdP traduit l'évolution du système modélisé dans ces différents états après l'occurrence de certains événements.

2.3. Franchissement des transitions

Une transition est franchissable si chacune des places en amont de cette transition contient au moins une marque [DAV 97]. Dans l'exemple précédent, la Transition 1 est franchissable ou validée.

Le franchissement (tir) d'une transition Tj consiste à retirer une marque dans chacune des places en amont de la transition Tj et à ajouter une marque dans la place en aval de la transition Tj.

Après franchissement, le RdP possède un nouveau marquage M'. Une suite de franchissements de transitions à partir d'un marquage donné est appelée séquence de franchissement.

2.4. Quelques propriétés des réseaux de Petri

Un RdP est utilisé pour décrire un système et l'étudier. L'évolution dynamique de ce système est décrite par l'évolution du marquage. Les notions de RdP vivant, de RdP sans blocage sont importantes ainsi que la notion de conflit.

2.4.2. Réseau borné

Une place Pi est bornée pour un marquage initial M_0 s'il existe un entier naturel k, tel que pour tout marquage accessible à partir de M_0, le nombre de marques dans Pi est inférieur ou égal à k (on dit que Pi est k-bornée).

Un RdP borné pour un marquage initial M_0 si toutes les places sont bornées pour M_0.

Un réseau est sauf pour un marquage initial M_0 si pour tout marquage accessible, chaque place contient au plus une marque. Toutes les places sont 1-bornées.

2.4.1. Vivacité

Un réseau de Petri est vivant, si et seulement si, à partir d'un marquage initial, pour toute transition t du réseau et tout marquage M accessible, il existe une séquence de franchissement qui contient t.

Toutes les transitions sont donc franchissables lors de l 'évolution du marquage du réseau et il y a toujours une possibilité de franchir n'importe quelle transition.

2.4.3. Blocage

Un blocage (ou état puits) est un marquage tel qu'aucune transition n'est validée.

Un RdP est sans blocage pour un marquage initial M_0 si aucun marquage accessible Mi à partir de M_0 n'est un blocage.

2.4.4. Conflits

Un réseau de Petri sans conflit est un réseau dans lequel toute place a au plus une transition de sortie.

Un conflit **structurel** correspond à l'existence d'une place P1 qui a au moins deus transitions de sortie T1, T2,…

Un conflit **effectif** est l'existence d'un conflit structurel K et d'un marquage M tel que le nombre de marques dans Pi est inférieur au nombre de transitions de sortie Pi qui sont validées par M.

Un RdP est sans conflit effectif pour un marquage initial M0, si pour tout marquage accessible M, il n'y a pas de conflit effectif.

2.5. Graphe de marquage d'un réseau de Petri

Le graphe des marquages accessibles (ou graphe d'accessibilité) est défini comme le graphe dont les nœuds sont les marquages accessibles à partir d'un marquage initial et dont les arcs

étiquetés par les noms des transitions sont définis par la relation de franchissement entre les marquages [DIA 01].

La recherche du graphe des marquages sous-jacent à un réseau de Petri marqué, donne une représentation de l'ensemble des états accessibles. Des propriétés qualitatives et quantitatives peuvent être ensuite extraites de cette nouvelle représentation.

L'analyse par un graphe de marquage nécessite la connaissance au préalable d'un marquage initial, ce qui n'est pas toujours le cas.

3. Extension des réseaux de Petri

Le pouvoir d'expression et de modélisation des RdP est amélioré par de nombreuses extensions qui ont été développées. Ils introduisent entre autres l'aspect temporel et permettent d'enrichir les structures des réseaux.

3.1. Réseaux de Petri généralisés

Les RdP généralisés attribuent des poids (nombres entiers strictement positifs) aux arcs. Une transition est franchissable dans un réseau de Petri généralisé, si toutes les places Pi en amont des transitions Tj contiennent au moins le nombre de jetons associés aux arcs. Tous les arcs dont le poids n'est pas explicitement spécifié ont un poids égal à 1. Lors du franchissement de la transition Tj, les nombres de jetons dans les places en aval de cette transition sont augmentés par le poids p.

Cette extension des RdP permet la réduction de la taille du RdP ordinaire. Toutefois, la transformation est possible du RdP généralisé vers le RdP ordinaire.

3.2. Réseaux de Petri synchronisés

A chaque transition, correspond un événement (une garde), et le franchissement de cette transition s'effectue si :

- ✓ la transition est validée,
- ✓ quand l'événement se produira.

Ces réseaux de Petri permettent de faire communiquer et interagir le système avec l'environnement ou un système extérieur. Ils permettent donc de modéliser des systèmes soumis à des contraintes externes.

3.3. Réseaux de Petri temporisés

Cette extension est caractérisée par l'ajout de temporisations, et donc une introduction de la variable temps. Il existe des RdP T-temporisés et des RdP P-temporisés. Dans le premier cas une durée est ajoutée aux transitions. La transition est donc validée après écoulement de la durée qui est allouée. Dans le second cas, la temporisation est ajoutée aux places.

Ces temporisations peuvent traduire les durées de déroulement des actions ou d'opérations associées aux transitions ou aux places.

Il existe une équivalence entre les réseaux T-temporisés et les réseaux P-temporisés, et un passage d'un formalisme à l'autre est possible par transformation.

3.4. Réseaux de Petri colorés

Les réseaux de Petri colorés facilitent la modélisation de systèmes de grande taille. Ils présentent un grand intérêt pour modéliser certains systèmes complexes.

Le principe consiste à représenter l'information par les ensembles place/marque. Aux marques de chaque place sont associées une couleur (ou identificateur). Le franchissement de ces marques peut être effectué de plusieurs manières en fonction des couleurs associées aux transitions. La relation entre les couleurs de franchissement et le marquage coloré est définie par des fonctions associées aux arcs.

Il existe plusieurs types de RdP qui peuvent être dis colorés, avec des variantes dans leur définition comme par exemple les réseaux de Petri à prédicats.

Les réseaux de Petri à prédicats comportent des marques auxquelles on attribue des paramètres. Les arcs portent des étiquettes et les prédicats sont associés aux transitions. Le prédicat peut pendant le tir de la transition modifier la valeur des marques utilisées pour le franchissement.

3.5. Réseaux de Petri stochastiques

Les réseaux de Petri stochastiques ont été introduits par Natkin [NAT 80] et Molloy [MOL 81] afin de répondre à certains problèmes d'évaluation quantitative des systèmes informatiques industriels.

Dans les réseaux de Petri stochastiques, les délais associés aux transitions sont aléatoires contrairement aux durées déterministes et constantes associées aux RdP temporisés. Ces temps sont modélisés par des variables aléatoires dont la loi la plus courante est la loi exponentielle qui permet d'approcher le graphe des marquages à un processus markovien homogène.

Les réseaux de Petri stochastiques sont très utilisés en sûreté de fonctionnement. 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 à un état de panne.

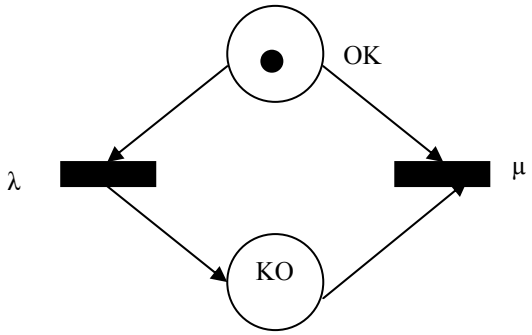


Figure A2.2 Modélisation des états normal et de panne d'un composant

Dans la figure A2.2, la variable λ représente le taux de défaillance du composant et la variable μ représente le taux de réparation de ce même composant.

Dans un réseau de Petri stochastique, chaque transition Ti est lui est associée une durée de franchissement aléatoire di. Cette durée correspond au temps qui s'écoule entre la sensibilisation et le tir effectif de la transition. On peut associer une fonction de répartition à la variable aléatoire (durée de franchissement) :

$$F_i(t) = 1 - e^{-\lambda_i(M)t}$$

où le paramètre λi(M) dépend du marquage M courant. Ce paramètre est appelé taux de transition relativement au marquage M.

3.5.1. Types de réseau de Petri stochastiques

Il existe deux types de réseaux de Petri stochastiques :

- ✓ Les réseaux de Petri stochastiques qui sont déduits des RdP autonomes (RdP décrivant le fonctionnement d'un système évoluant de façon autonome et où les instants de franchissement ne sont pas connus ou indiqués) : c'est le modèle initialement défini. Les marques sensibilisant les transitions ne sont pas réservées,
- ✓ Les réseaux de Petri à temporisation stochastique : ils sont issus des réseaux de Petri temporisés; lorsqu'une transition est sensibilisée, celle-ci réserve le ou les jetons.

Ces deux types de réseaux de Petri ont le même comportement s'il n'y a pas de conflit effectif.

Le marquage d'un RdP stochastique (et non pas d'un RdP à temporisation stochastique) est un processus markovien homogène, et donc à tous RdP, on peut associer une chaîne de Markov homogène.

3.5.2. Analyse d'un réseau de Petri stochastique

L'analyse d'un RdP stochastique consiste en deux approches :

- ✓ l'approche qui concerne les propriétés de conservation dans un RdP. Celles-ci sont déduites du calcul des invariants de marquages de places et franchissements de transitions. On obtient alors des relations de conservation du marquage et du taux de franchissement,
- ✓ l'approche qui consiste à construire le graphe des marquages accessibles du RdP autonome sous-jacent et à étiqueter chaque arc par un taux de franchissement qui dépend du taux associé à la transition et du marquage des places en amont de cette transition.

L'analyse du RdP stochastique se ramène à celle d'un processus de Markov homogène à espace d'états discrets à tems continu. Cette analyse est faite uniquement dans le cas où le RdP sous-jacent est borné.

3.6. Réseaux de Petri stochastiques généralisés

Les transitions dans les réseaux de Petri stochastiques sont associées toutes à une temporisation selon une distribution de loi exponentielle par exemple. [AJM 95] a introduit les réseaux de Petri stochastiques généralisés afin de s'affranchir de certaines restrictions.

Dans les RdPSG (réseaux de Petri stochastiques généralisés), les transitions autorisées sont de deux types et elles peuvent soient :

- ✓ Des transitions temporisées basées sur des distributions exponentielles,
- ✓ Des transitions déterministes à temporisation nulle (transition immédiate) basée sur une distribution de Dirac. Ces transitions sont franchies immédiatement dès qu'elles sont sensibilisées.

Les transitions immédiates expriment des synchronisations ou encore elles approximent des durées très faibles par rapport aux durées des transitions stochastiques.

Annexe 3 : L'outil de modélisation Möbius

L'outil de modélisation Möbius

1. Introduction

Möbius est un outil de modélisation supportant les SAN (*Stochastic Activity Network*). Il permet la combinaison de modèles simples jusqu'aux modèles composés. Les modèles se composent de la description de la structure du réseau et des variables de performances désirées et des méthodes utilisées pour l'évaluation de ces performances.

2. SAN

Les SAN sont une généralisation des réseaux de Petri stochastiques [MOV 84]. Les modèles offrent la possibilité de la concurrence, tolérance aux fautes et la représentation d'états dégradés dans un simple modèle. Les SAN sont plus flexibles que beaucoup d'autres extensions de RdP telles que les SPN et les GSPN (respectivement, les réseaux de Petri stochastiques et les réseaux de Petri stochastiques généralisés) [AZG 05]. Les SAN offrent aussi des propriétés concernant les RdP colorés par l'existence de places spécifiques appelées "*extended places*".

La structure des SAN est composée de places, de portes d'entrée (***Input Gates***), de portes de sorties (***Output Gates***) et d'activités. Les activités sont similaires aux transitions pour les RdP. Elles sont de deux types : temporisés ou instantanées. Les activités temporelles "*timed*" représentent les actions du système modélisé dont la durée a un impact sur la performance du système. Les activités instantanées "*Instantaneous Activity*" représentent les activités du système dont l'occurrence est immédiate. Les portes d'entrée et de sortie contrôlent la validation des activités et assurent des comparaisons ou tests (portes d'entrée) et des affectations (portes de sorties). Ces portent définissent aussi le marquage lorsque l'activité est achevée.

Une porte d'entrée dispose d'une sortie unique et de plusieurs entrées en quantité limitée. Elle représente un lien entre ces places et l'activité unique liée à la sortie de la porte.

Une porte de sortie dispose d'une entrée unique et de plusieurs sorties en quantité limitée. Elle caractérise le lien entre une activité unique en amont et les places en aval de la porte.

La figure A3.1 montre la représentation graphique des portes d'entrée et de sortie :

Figure A3.1 représentation graphique des portes d'entrée et de sorties

Graphiquement, dans l'outil Möbius présenté dans la section suivante, les portes d'entrées sont représentées par un triangle à lignes rouges horizontales tandis que les portes de sortie sont représentées par un triangle à lignes noires verticales.

Les modèles SAN sont utilisés pour l'évaluation de systèmes appartenant à un large domaine et ils sont supportés par des outils de modélisation tels que UltraSAN [SAN 95] et Möbius [DEA 02].

Un des objectifs des SAN concerne l'évaluation des performances et de la sûreté de fonctionnement. L'évaluation de ces performances de la sûreté de fonctionnement est effectuée par la définition d'un ensemble de mesures dans le modèle.

Le développement de nos modèles est réalisé par l'outil Möbius qui est un support pour l'utilisation des SAN.

3. La modélisation par l'outil Möbius

Möbius est un outil qui permet de modéliser le comportement des systèmes complexes. La première version est apparue en 2001 comme successeur de l'outil populaire et réussi d'UltraSAN. Bien que Möbius ait été à l'origine développé pour étudier la fiabilité, la disponibilité, et la performance des systèmes informatiques et systèmes liés par un réseau, son utilisation a augmenté rapidement. Il est maintenant employé pour une large gamme des systèmes à événement discret [Möbius]. Le but de cette partie est de présenter le logiciel *Möbius tool* et les mécanismes de bases qui par la suite permettent de développer des modèles plus complexes et accéder à leur étude.

La large gamme de l'utilisation est rendue possible en raison de la flexibilité et de la puissance de l'outil Möbius.

L'outil de Möbius est un environnement pour soutenir des formalismes multiples de modélisation. Pour qu'un formalisme soit compatible avec Möbius, le concepteur doit pouvoir traduire un modèle établi dans son formalisme dans un modèle équivalent qui emploie des composants de Möbius. Puisque des modèles sont construits dans des formalismes spécifiques, les avantages expressifs des formalismes particuliers sont préservés. Puisque tous les modèles sont transformés en composants de Möbius, tous les modèles et techniques de solution dans Möbius avec les propriétés compatibles peuvent agir l'un sur l'autre les uns avec les autres [Möbius].

3.1. Modèle atomique

La première étape dans la construction du modèle est de produire un modèle en utilisant un certain formalisme. Le modèle le plus fondamental s'appelle un modèle atomique (***atomic model***), il se compose des variables d'état et actions. Les variables d'état (les places) tiennent des informations d'état sur un modèle, alors que des actions (transitions) sont le mécanisme qui permet le changement d'état du modèle.

Chaque modèle atomique dans *Möbius* est formé de places simples, de places étendues (l'équivalent des places colorées), d'activités instantanées, d'activités temporelles, de portes d'entrée et de portes de sorties (*input gate* et *output gate*). Tous ces composants créent la partie statique d'un réseau SAN, les jetons formant la partie dynamique. Chaque composant possède différents attributs.

Le modèle atomique est constitué de places, d'activités temporelles et instantanées et de portes d'entrée et de sortie.

Places : les places sont de deux types : simples et étendues. Dans *Möbius,* la notion de place étendue est utilisée pour représenter les places colorées. Chaque place simple possède un nom et un marquage initial, elle est graphiquement représentée comme un cercle bleu. Une place étendue (***extended place***) possède un nom et une structure : la structure sera l'équivalent de la couleur.

Activités : une activité peut être de deux types, instantanée et temporelle. Une activité instantanée possède un nom et un nombre de cas. Si le nombre de cas est plus grand que un, une probabilité est associée à chaque cas. La somme des probabilités de tous les cas doit être égale à un. Une activité temporelle possède tous les attributs d'une activité instantanée plus un champ dédié au temps d'activation de l'activité. Le temps est stochastique et peut être défini suivant plusieurs lois de probabilité (exponentielle, normale, binomiale…).

Portes d'entrée : les portes d'entrée sont représentées graphiquement par un triangle rouge dont le sommet est du côté des places d'entrée et la base est du côté de l'activité. Une porte d'entrée relie une ou plusieurs places à une seule activité. Une porte d'entrée possède un nom et deux fonctions : la fonction de validation qui définit les conditions d'activation d'une activité et une fonction de porte qui permet de modifier le marquage des places en entrée une fois l'activité franchie.

Portes de sortie : les portes de sortie sont représentées par un triangle noir dont la base est du côté de l'activité et le sommet est du côté des places en sortie. Une porte de sortie possède un nom et une fonction de porte qui permet de modifier le marquage des places après le franchissement de l'activité.

Les arcs : les arcs relient les places au portes d'entrée, les portes d'entrée aux activités, les activités aux portes de sorties et les portes de sorties aux places de sortie.

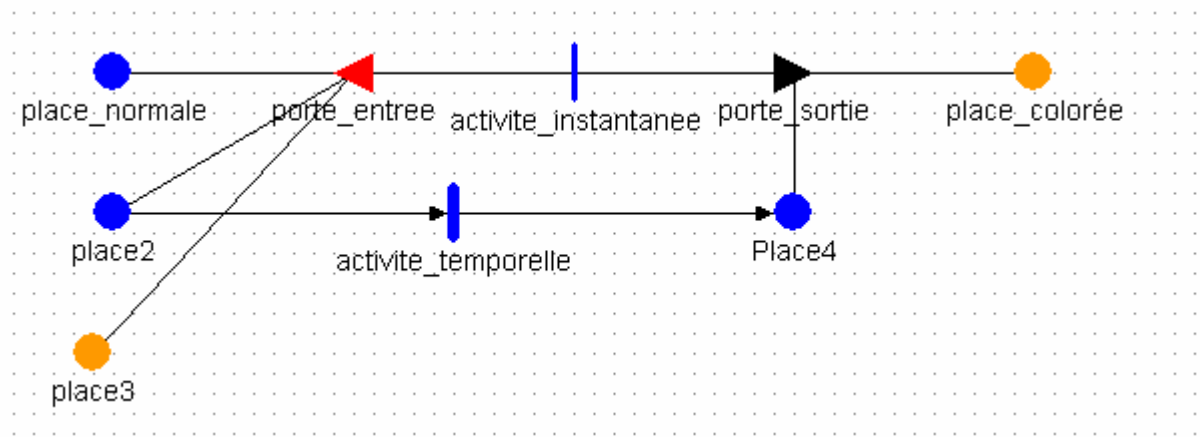


Figure A3.2 : Exemple d'un modèle atomique sous Möbius

3.2. Modèle composé

Si le modèle construit est prévu pour faire partie d'un plus grand modèle, l'étape suivante est de construire une composition (***composed model***) avec d'autres modèles (c'est-à-dire, modèles atomiques ou composés) pour former un plus grand modèle. Ceci est parfois employé comme technique commode pour rendre le modèle modulaire et plus facile à construire. Le modèle composé est hiérarchiquement construit à partir des sous-modèles, qui préservent en grande partie leurs caractéristiques spécifiques de sorte que le modèle composé ne détruise pas les propriétés structurelles des sous-modèles.

La jonction des modèles atomiques est assurée par les fonctions ***join*** et ***replicate*** qui réalisent respectivement la jonction de plusieurs modèles avec une édition d'un ensemble de places partagées de même type et la représentation de copies de modèles de composants.

Join : la fonction *join* permet la jonction de plusieurs modèles. La seule condition pour joindre deux ou plusieurs modèles est que ces modèles partagent une ou plusieurs places appelées places communes ou places partagées. Les places communes doivent être de même nature i.e contenant la même structure et le même marquage initial. C'est à l'intérieur de la fonction *join* qu'on définit les places partagées.

Replicate : prenons l'exemple d'un système qui contient *n* composants identiques, la prise en compte de ces *n* composants dans la modélisation peut se faire en faisant un modèle représentant le composant et *n*-1 copies du même composant. Cela est possible en utilisant la fonction *replicate*. La fonction *replicate* possède un seul attribut qui définit le nombre de copies.

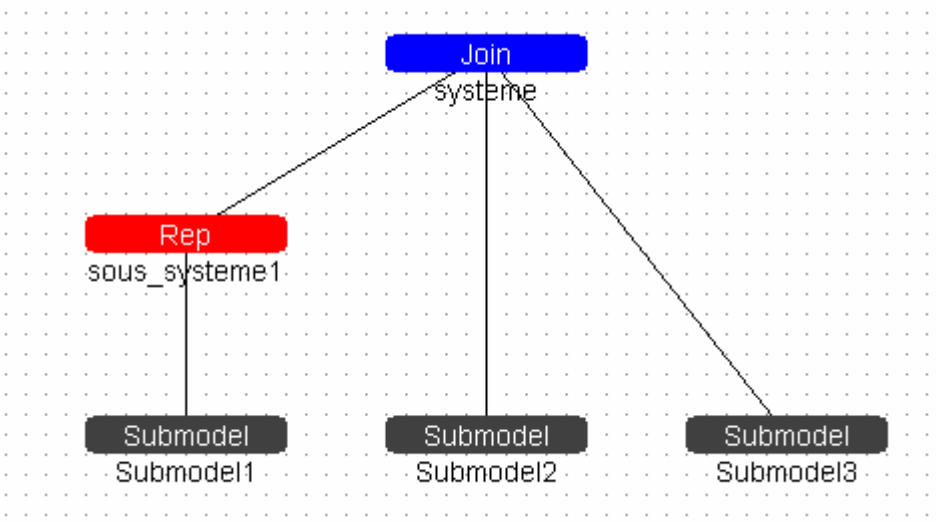


Figure A3.3 : Exemple d'un modèle composé dans Möbius

3.3. Fonction de récompense

Après qu'un modèle composé soit créé, l'étape suivante consiste à indiquer quelques mesures d'intérêt sur le modèle en utilisant un formalisme de spécifications de récompense (***reward model***).

Dans cette étape l'évaluation de paramètres peut être décrite par la détermination de durée de séjour dans une place ou le nombre de franchissements d'une transition.

Deux fonctions sont définies dans *reward*:

Rate reward : cette fonction est utilisée pour évaluer les paramètres dépendant du temps, comme par exemple la durée où une condition a été valide. Les conditions peuvent être des conditions sur les marquages des places. Par exemple si la présence d'un jeton dans une place P1 représente l'indisponibilité d'un composant, alors l'indisponibilité du composant peut être calculée à partir de la fonction *rate reward* suivante :

If (P1->Mark ()= =1)

return 1;

Ce code retourne la durée pendant laquelle la condition P1->Mark()= =1 était valide.

Impulse reward : cette fonction permet d'évaluer les paramètres dépendant des franchissements des activités, comme le nombre de franchissement ou la probabilité de franchissement des activités.

/*defaillance*/

return 1;

Si on considère que l'activité *defaillance* représente une défaillance dans le système, ce code nous permet de calculer le nombre de fois où cette transition sera franchie durant une durée déterminée.

3.4. Study

L'attribution des valeurs propres aux variables est réalisée par l'étape qui concerne une étude particulière (***study***). Dans cette étape, la possibilité de modification des valeurs des variables est toujours possible sans retourner aux modèles atomiques.

3.5. Solutions

L'étape suivante consiste typiquement à appliquer un certain solutionneur (***solver***) pour calculer une solution au modèle de récompense. Un solutionneur peut opérer indépendamment du formalisme dans lequel le modèle a été construit, à condition que le modèle ait les propriétés nécessaires pour le solutionneur.

La solution calculée à une variable de récompense s'appelle un résultat. Puisque la variable de récompense est une variable aléatoire, le résultat est exprimé comme la caractéristique d'une variable aléatoire. Ceci peut être, par exemple, la moyenne, la variance, ou la distribution de la variable de récompense. Le résultat peut également être l'intervalle de confiance.

Les résultats estimant les variables recherchées peuvent être donnés par un calcul numérique exact ou bien par simulation. Cette dernière est utilisée pour tous les modèles conçus dans Möbius.

En général la solution par simulation peut être utilisée pour tous les modèles conçus dans *Möbius,* tandis que la solution numérique ne peut être utilisée que pour des modèles respectant les conditions suivantes :

- ✓ toutes les activités ont une distribution exponentielle sur la durée d'activation,
- ✓ toutes les activités ont ou bien une distribution exponentielle, ou bien une distribution déterministe sur la durée d'activation. En plus une seule action déterministe peut être activée au même instant.

Dans les deux solutions un nombre de traces peuvent être sauvegardées pour mieux comprendre le comportement du modèle, comme l'instant des franchissements des activités ou le marquage des places avant et après le franchissement.

Il est important de signaler que les solutions par simulation donnent des valeurs approximées et non pas les valeurs exactes des variables recherchées

Références bibliographiques

Références bibliographiques

[AJM 95] M. Ajmone Marsan, G. Balbo, G. Conte, S. Donatelli et G. Franceschini, Modelling with generalized stochastic Petri nets. Wiley series in parallel computing. 1995.

[ALB 91] J. S. Albus. Outline for a theory of intelligence. IEEE Transactions on Systems, Man, and Cybernetics, Vol. 21, N°. 3, 1991.

[ANT 03] L. Antoni, Injection de fautes par reconfiguration dynamique de réseaux programmables. Thèse de doctorat de l'Institut National Polytechnique de Grenoble (INPG). 2003.

[ARC 05] ARC Advisory Group, Siemens Process Safety Systems Deliver Modern Features on a Proven Platform, October 2005. http://www.automation.siemens.com/cd/safety/ftp/arc_white_paper_process_safety.pdf

[AUB 04] O. Aubry. Sécurité des procédés industriels. Forum ELEC/MESUCORA. ELEC 2004. Endress + Hausser. Décembre 2004.

[AVI 04] A. Aviziennis, J. C. Laprie, B. Randell, Dependability an its threats : a taxonomy, in Proceeding of the building the information society: Proc. IFIP 18th World Computer Congress, Toulouse, France, august, 2004.

[AZG 05] A. Azgomi, A. Movaghar, Hierarchical Stochastic Activity Networks: Formal definitions and behaviour, International Journal of Simulation, Systems, Science and Technology, Vol. 6, No 1-2, pp. 56-66. 2005.

[BAE 01] K. H. BAE, H. C. KIM, M. H. Chang, S. K. Sim. Safety evaluation of the inherent and passive safety features of the smart design. Annals of Nuclear Energy 28. pp 333-349. 2001.

[BAI 07] H. Baikeche, Diagnostic des systèmes linéaires en boucle fermée. Thèse de doctorat de l'Institut National Ploytechnique de Lorraine. 2007.

[BAR 03] P. Barger, 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, 2003.

[BAR 02] P. Barger, J. M. Thiriet, M. Robert, Performance and dependability evaluation of distributed dynamical systems, European Conference on System Dependability and Safety (ESRA 2002/lambda-Mu13), Lyon (France), 19-21st March 2002, pp. 16-22.

[BAY 05] M. Bayart - B. Conrard - A. Chovin - M. Robert, capteurs et actionneurs intelligents, Techniques de l'ingénieur, S7520, Informatique Industrielle, Mars 2005, Vol S2.

[BAY 94] M. Bayart, "Instrumentation intelligente - Systèmes automatisés de production à intelligence distribuée", Habilitation à Diriger des Recherches, Université de Sciences et Technologies de Lille, 21 décembre 1994.

[BAY 93] M. Bayart, M. Staroswiecki, "A Generic Functional Model of Smart Instrument for Distributed Architectures", Intelligent Instrumentation for remote and on site measurement, Bruxelles, Belgique, 12-13 mai 1993.

[BEA 93] F. Beaudoin, J.M. Favennec "Les capteurs intelligents : le concept et les enjeux", Revue Générale de l'Électricité, Mars 1993, No 3, pp. 1-8.

[BEN 04] V. Benard, Evaluation de la sûreté de fonctionnement des systèmes complexes, basée sur un modèle fonctionnel dynamique : la méthode SAFE-SADT, Thèse de doctorat de l'Université de Valenciennes et du Hainut Cambresis, décembre 2004.

[BEN 01] Benoit E., Foulloy L., Tailland J., *"InOMs model: a Service Based Approach to Intelligent Instruments Design"*, 5th World Conf. on Systemics, Cybernetics and Informatics (SCI 2001), Vol. XVI, Orlando, USA, July 2001, pp. 160-164.

[BER 96] N. Bergé. Modélisation au moyen de réseaux de Petri temporisés stochastiques d'une application de contrôle/commande de poste de transformation d'énergie électrique répartie sur le réseau de terrain FIP. Thèse de doctorat. Université Paul Sabatier de Toulouse. 1996.

[BEU 06] J. Beugin, Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé. Thèse de doctorat de l'Université de Valenciennes et du Hainaut-Cambrésis, décembre 2006.

[BIS 05] P. Bishop, R. Bloomfield, S. Guerra, K. Tourlas. Justification of smart sensors for nuclear applications. SAFECOMP 2005, LNCS 3688, pp, 194-207, 2005.

[BOU 97] A. Bouras, "Contribution à la conception d'architectures réparties : modèles génériques et interopérabilité d'instruments intelligents", Thèse de Doctorat, Université des Sciences et Technologies de Lille, Juillet 1997.

[BOW 94] M.E.C. Bowen, G.B. Smith, Design of flexible ASIC's including embedded processors for smart sensor applications, Application Specific Integrated Circuits for Measurement Systems, IEE Colloquium, Feb 1994.

[BRO 05] S. R. Brown, M. Menezes. Measurement best practices for safety instrumented systems. ISA EXPO 2005, Chicago, Illinois, 25-27 Octobre 2005.

[CAR 93] Carroll, J.B., 1993. Human cognitive abilities. Cambridge University Press, Cambridge.

[CAU 04] L. Cauffriez, J. Ciccotelli, B. Conrard, M. Bayart, the members of the working-group CIAME. Design of intelligent distributed control systems: a dependability point of view. Reliability Engineering and System Safety. Vol 84. pp, 19-32. 2004.

[CAU 03] L. Cauffriez, B. Conrard, J. M. Thiriet, M. Bayart. Fieldbuses and their influence on dependability. IMTC 2003 IEEE. Instrumentation and Measurement Technology Conference. Vail, CO, USA. pp, 83-88. May 2003.

[CAL 90] J. P. Calvez, "Spécification et conception des systèmes - une méthodologie", Édition Masson, Paris, 1990.

[CAM 01] J. C. Campelo, P. Yuste, P.J. GIL, J.J. Serrano, DICOS: a real-time distributed industrial control system for embedded applications, Control Engineering Practice 9 (2001), pp. 439-447.

[CAM 99] J. C. Campelo, F. Rodriguez, A. Rubio, R. Ors, P.J. Gil, L. Lemus, J.V. Busquets, J. Albaladejo, .J. Serrano, Distributed industrial control systems: a fault-tolerant architecture, Microprocessors and Microsystems 23 (1999), pp.103–112.

[CAM 97] J. C. Campelo, F. Rodriguez, P. J. Gil, J.J. Serrano : Dependability evaluation of fault tolerant architectures in distributed industrial control system. WFCS'97, 2nd IEEE International Workshop on Factory Communication Systems, Barcelona, Spain (1997).

[CEI 05] CEI 62061. Sécurité des machines, sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité. Commission Electrotechnique Internationale, Genève, Suisse, 2005.

[CEI 03] CEI 61511, Sécurité fonctionnelle des systèmes instrumentés pour les industries de Process. Commission Electrotechnique Internationale, Genève, Suisse 2003.

[CEI 00] CEI 61508. Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité. Commission Electrotechnique Internationale, Genève, Suisse, 2000.

[CEI 91] CEI 61069 Norme internationale- Mesure et commande dans les processus industriel- Appréciation des propriétés d'un systèmes en vue de son évaluation –Partie 5 Evaluation de la sûreté de fonctionnement d'un système. Commission Electrotechnique Internationale, Genève, Suisse, 1991.

[CEN 00] CENELEC, NF EN 50126, Applications ferroviaires : spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS). CENELEC, Comité Européen de Normalisation Electrotechnique. Fontenay-aux-Roses, France UTE, Union Technique de l'Electricité et de la communication, 2000.

[CHE 02] J. Chen, J. Howell. Towards distributed diagnosis of the Tennessee Eastman process benchmark. Control Engineering Practice 10. pp, 971-987. 2002.

[CHO 96] A. Chovin, Capteurs et actionneurs intelligents – du concept aux applications, Edition Terrain, juin 1996.

[CHU 03] Y. J. Chung, S. H. Kim, H. C. Kim. Thermal hydraulic analysis of SMART for heat removal transients by a secondary system. Nuclear Engineering and Design 225. pp, 257-270. 2003.

[CIA 99] CIAME. Réseaux de terrain: description et critères de choix. Editions Hermès. 1999.

[CLA 00] D. W. Clarke, Intelligent Instrumentation, Transactions of the Institute of Measurement and Control 22,1 pp. 3-27, 2000.

[CLA 95] D. W. Clarke. Sensor, actuator and loop validation. IEEE Control Systems Magazine. Vol 15, issue 4. pp 39-45. august 1995.

[CON 99] B. Conrard : Contribution à l'évaluation quantitative de la sûreté de fonctionnement des systèmes d'automatisation en phase de conception . Thèse de doctorat. Université Henri Poincaré, Nancy 1, 1999.

[DAI 03] Y.S. Dai, M. Xie, K.L. Poh, G.Q. Liu, A study of service reliability for distributed systems, Reliability Engineering and System Safety 79, 2003, pp. 103-112.

[DAV 97] R. David, H. Alla, du grafcet aux réseaux de Petri, 2éme édition, Hermès, 1997.

[DEA 02] D. D. Deavours, G. Clark, T. Courtney, D. Dalys, S. Derisavi, J. M. Doyle, W.H. Sanders, P. G. Webster. The Mobuis framework and its implementation. IEEE Trans. On Soft. Engineering, Vol. 28, N°10, pp 956-969, 2002.

[DES 06] X. Desforges, B. Archimède. Multi-agent framework based on smart sensors/actuators for machine tools control and monitoring. Engineering Application of Artificial Intelligence 19. pp, 641-655. 2006.

[DIA 01] M. Diaz, Les réseaux de Petri, Modèles fondamentaux, Hermès, Paris, 2001.

[DOB 98] A. Dobbing, D. Godfrey, M. J. Stevens and B. A. Wichmann. Reliability of Smart Instrumentation. NPL, National Physical Laboratory. Middx, UK. August, 1998.

[DOR 93] R. C. Dorf. The Electrical Engineering HandBook. IEEE Press, 1993.

[EN 96] EN 954-1, Sécurité des machines. Partie des systèmes de commandes relatives à la sécurité. Partie 1 : Principes généraux, décembre 1996.

[FAE 00] E. Fae, J. L. Durka, Conception et évaluation de la sécurité fonctionnelle des systèmes instrumentés de sécurité. Rapport Final, Institut National de l 'Environnement Industriel et des Risques, INERIS, 2000, www.ineris.fr

[FAL 04] R. Faller. Project experience with IEC 61508 and its consequences. Safety Science, vol 42. pp, 405-422. 2004.

[FAR 04] S. M. Farritor, S. Goddard. Intelligent highway safety markers. IEEE Intelligent Systems. Vol 19, n° 6 . pp, 8-11. Nov/Dec 2004.

[FAR 67] F. R. Farmer, Siting criteria - a new approach, in 'Symposium Containment and Siting of Nuclear Power Plants, International Atomic Energy Agency, Wieden'. 1967.

[FAU 02] S. Faucou. Description d'architectures opérationnelles valides temporellement. Thèse de doctorat de l'Institut de Recherche en Communications et en Cybernétique de Nantes (IRCCyN), Décembre 2002.

[FRA 00] R. Frank. Understanding Smart Sensors. Second Edition. Artech House, 2000.

[GAR 02] C.J. Garett, G.E. Apostolakis, Automated hazard analysis of digital control systems, Reliability Engineering and System Safety 77, 2002, pp. 1-17.

[GAR 98] R. Garnier. Une méthode efficace d'accélération de la simulation des réseaux de Petri stochastiques. Thèse de l'université de Bordeaux, 1998.

[GEH 94] A.L. Géhin, "Analyse fonctionnelle et modèle générique des capteurs intelligents - Application à la surveillance de l'anesthésie", Thèse de Doctorat, Université des Sciences et Technologies de Lille, 26 janvier 1994.

[GEO 05] B. Georgiev, Field Control Systems. 6th international PhD Workshop on Systems and Control, Izola, Slovenia, Octobre 2005.

[GEY 05] J. Gey, D. Courdeau, Pratiquer le management de la santé et de la sécurité au travail : Maîtriser et mettre en oeuvre l'OHSAS 18001, ISBN 2124750836, AFNOR Editions. 2005.

[GHO 08] R. Ghostine. Influence des fautes transitoires sur la fiabilité d'un système commandé en réseau.. Thèse de doctorat de l'INPL (Institut National Polytechnique de Lorraine), 2008.

[GOB 05] W. M. Goble, H. Cheddie. Safety Instrumented Systems Verification, Practical Probabilistic Calculations. ISA (The instrumentation, Systems, and Automation Society). 2005.

[GOB 01] W. M. Goble, J. V. Bukowski, Extending IEC61508 Reliability Evaluation Techniques to Include Common Circuit Designs Used in Industrial Safety Systems, Proceedings Annual Reliability and Maintenability *Symposium,* Philadelphia, PA, USA, pp 339-343, 2001.

[GOB 98] W. M. Goble, Control systems safety evaluation and reliability (2nd edition), Research triangle park (NC), ISA (The instrumentation, Systems, and Automation Society), 1998.

[GOU 03] R. Gouriveau, Analyse des risques. Formalisation des connaissances et structuration des données pour l'intégration des outils d'étude et de décision, Thèse de Doctorat de l'INPT (Institut National Polytechnique de Toulouse) 2003.

[GRE 91] GREPA : Le GRAFCET – de nouveaux concepts, Cépaduès-éditions, 1991.

[GRI 98] A. Griffault, S. Lajeunesse, G. Point, A. Rauzy,J.-P. Signoret, P. Thomas. *The Altarica language.* International Conference on Safety and Reliability. ESREL'98, p000-999. Rotterdam, Juin 1998.

[GRI 03] M. Gribaudo, A. Horvath, A. Bobbio, E. Tronci, E. Ciancamerla, M. minichino. Fuild Petri nets and hybrid model-checking : a comparative case study. Reliability Engineering Systems Safety (RESS), vol 81, pp 239-257, 2003.

[GRU 98] P. Gruhn, J. Pittmann, S. Wiley, T. Leblanc. Quantifying the impact of partial stroke valve testing of safety instrumented systems. ISA Transactions 37. pp, 87-94. 1998.

[GUO 07] H. Guo, X. Yang. A simple reliability block diagram method for safety integrity verification. Reliability Engineering Systems Safety (RESS), vol 92, pp 1267-1273, 2007.

[HER 97] F. Hermann, Contribution à la répartition des traitements et des données sur une architecture distribuée équipée d'un réseau de terrain FIP : Application à un processus thermique pilote, Thèse de l'Université Henri Poincaré, Nancy I, novembre 1997.

[HOK 04] P. Hokstad, K. Corneliussen. Loss of safety assessment and the IEC 61508 standard. Reliability Engineering Systems Safety (RESS), vol 83, pp 111-120, 2004.

[HSE 95] Health and Safety Executive – Out of control HSE books, United Kingdom 1995.

[IEE 04] IEEE Std 1451.4, IEEE Standard for A Smart Transducer Interface for Sensors and Actuators: Mixed-Mode Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats, IEEE Std 1451.4- 2004.

[IEE 98] IEEE Std 802.3, Edition: Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 3: Carrier senses multiple access with

collision detection (CSMA/CD) access method and physical layer specifications,1998.

[INN 06] F. Innal, Y. Dutuit, A. Rauzy, J. P. Signoret. Quelques interrogations et commentaires relatifs à la norme CEI 61508. Congrès λμ 15. Lille, France. Octobre 2006.

[INN 05] F. Innal, Y. Dutuit, M. Djebabra. Analyse critique des formules de base de données dans la norme internationale CEI 61508-6. 6ème congrès international pluridisciplinaire, Qualité et sûreté de fonctionnement. Bordeaux, France. Mars, 2005.

[ISA 04] ISA 84.00.01–2004, Functional Safety Instrumented Systems for the Process Industries, Parts 1–3, 2004.

[ISA 96] ISA, Application of Safety Instrumented Systems for the process Industries, ANSI / ISA-S84.01,1996.

[ISE 92] R. Isermann,. Estimation of physical parameters for dynamic processes with application to an industrial robot. International Journal of Control 55 (6), pp. 1287 1298. (1992).

[ISO 99] ISO/CEI Guide 51. Aspects liés à la sécurité. Principes directeurs pour les inclure dans les normes. International Organisation for Standardization. 1999.

[JIA 03] Q. Jiang, C. H. Chen. A numerical algorithm of fuzzy reliability. Reliability Engineering and System Safety. Vol 80. pp, 299-307. 2003.

[JON 01] C.C.M. Jones, R.E. Bloomfield, P.K.D. Froome and P.G. Bishop, "Methods for assessing the safety integrity of safety-related software of uncertain pedigree (SOUP)", Report No: CRR337 HSE Books 2001 http://www.hse.gov.uk/research/crr_pdf/2001/crr01337.pdf

[JOS96] J. F. Josserand, Cellule floue: contribution à la commande floue distribuée, thèse de doctorat, Université de Savoie, 1996.

[JUA 02] G. Juanole. Quality of service of communication networkes and distributed automation, models and performances. Invited paper, 15th TriennialWorld Congress of the IFAC, Barcelona, Spain. Juillet 2002.

[JUA 95] G. Juanole. Réseaux de Petri et communications. Rapport LAAS N°95296, Réseaux de communications et Conception de protocoles, Coordonnateurs : G. Juanole, A. Serhrouchni, D. Seret. Hermès, pp, 265-287. 1995.

[JUM 03] F. Jumel, J.M. Thiriet, J.F; Aubry, O. Malasse, Towards an information-based approch for the dependability evaluation of distributed control systems, IMTC 2003 – Instrumentation and Measurement Technologie Conference, Vail, CO, USA, 20-22 May 2003.

[KER 02] C. Kermisch et P.E. Labeau, Approche dynamique de la fiabilité des systèmes, Rapport MNFD 2002-10, Service de Métrologie Nucléaire, Université Libre de Bruxelles (Belgique), novembre 2002.

[KNE 02] B. Knegtering, Safety lifecycle management in the process industries: the development of a qualitative safety-related information analysis technique. Phd thesis, Technische Universiteit Eindhoven, 2002.

[KOS 06] K. T. Kosmowski, Functional safety concept for hazardous systems and new challenges. Journal of Loss Prevention in the Process Industries 19, pp. 298-305, 2006.

[KOS 05] Kosmowski, K.T. & Sliwinski, M. (2005). Methodology for functional safety assessment. *European conference on safety and reliability-ESREL'05 Gdynia-Sopot-Gdansk, Poland, K. Kolowrocki , vol.2*, pp 1173-1180.

[KUM 96] H. Kumamoto, E. J. Henley. Probilistic risk assessment and management for enginners and scientisits, 2th edition, IEEE Press, 1996.

[LAB 02] P. E. Labeau, C.Kermisch. Approche dynamique de la fiabilité des systèmes. Rapport MNFD 2002-07, Service de Métrologie Nucléaire,Université Libre de Bruxelles, juillet 2002

[LAF 97] Joseph La fauci, PLC or DCS : selection and trends, ISA Transactions, vol 36 n°1 pp 21 – 28, 1997.

[LAM 02] P. Lamy, Probabilité de défaillance dangereuse d'un système. Explications et exemple de calcul. INRS (Institut National de Recherche et de Sécurité), Note scientifique n° 225, 2002.

[LAN 08] Y. Langeron, A. Barros, A. Grall et C. Bérenguer, Combination of safety integrity levels (SILs):A study of IEC61508 merging rules, *Journal of Loss Prevention in the Process Industries* (2008),

[LAP 88] J. C. Laprie, Sûreté de fonctionnement et tolérance aux fautes : concepts de base, rapport LAAS n°88.287, paru dans les techniques de l'ingénieur, 1988.

[LAU 04] J. Lautrey. Hauts potentiels et talents : la position actuelle du problème. Psychologie française, vol : 49. pp, 219-232. 2004.

[LEE 01] D. Lee, J. Allan, H.A. Thompson, S. Bennett, PID control for a distributed system with a smart actuator, Control Engineering Practice 9, (2001), pp. 1235–1244.

[LEE 00] K. Lee, IEEE 1451: A standard in support of smart transducer networking, IEEE Instrumentation and Measurement Technology Conference, Baltimore, USA, 2000.

[LEW 04] Franck L. Lewis. Wireless Sensor Networks. In Smart Environments : Technology, Protocols and Applications, ed. Diane Cook and Sajal Das, John Willey, New York, 2004.

[LUN 07] M. A. Lundteigen, M. Rausand. Common cause failures in safety instrumented systems on oil and gas installations : Implementing defense measures through function testing. Journal of Loss Prevention in the Process Industries, vol 20, pp. 218-229, 2007.

[LUN 06] M. A. Lundteigen. Assessment of hardware safety integrity requirements. Proceedings of the 30th EDReDA Seminar, Trondheim, Norway. June 2006.

[MAC 04] D. Macdonald. Safety in field instruments and devices. Practical Industrial Safety. Risk Assessment and Shutdown Systems. 2004. pp, 200-229.

[MAL 94] M. Malhotra, K. S. Trivedi. Power-hierarchy of dependability-model types. IEEE Transactions on Reliability, vol 43. pp, 493-502. 1994.

[MAR 01] E. Marszal & W. Goble. High reliability computing for control and safety. Proceedings of the 2001 Particle Accelerator Conference, Chicago. IEEE. pp, 279-282. 2001.

[MAS 98] M. K. Masten. The intelligence in intelligent control. Annual Reviews in Control. Vol 22. pp, 1-11. 1998.

[MAZ 07] M. H. Mazouni, , D. Bied Charreton, J. F. Aubry. Proposal of a generic methodology to harmonize Preliminary Hazard Analyses for guided transport. IEEE(SMC), San Antonio–TX, Avril 2007.

[MED 06] M. Medjouji, Contribution à l'analyse des systèmes pilotés par calculateurs : Extraction de scénarios redoutés et vérification de contraintes temporelles. Thèse de l'Université Paul Sabatier de Toulouse. Mars 2006.

[MEI 94] G. C. M. Meijer, Concepts and focus point for intelligent sensor systems, Sensors and Actuators A, 1994, vol. 41-42, pp. 183-191.

[MEK 06] S. Mekid, Further structural intelligence for sensors cluster technology in manufacturing, Sensors, 2006, vol 6, pp. 557-577.

[MES 05] L'IEC 61508 s'impose, sa famille aussi, MESURES, Novembre 2005, www.mesures.com.

[MEU 04] M.J.P. van der Meulen. On the use of smart sensors, common cause failure and the need for diversity. 6th Int. Symp. Programmable Electronic Systems in Safety Related Applications, Cologne, Germany, TUV, 2004

[MEY 06] R. Meyers, C. Haussemand. Comment évaluer les compétences clés dans le domaine professionnel ? Revue Européenne de psychologie appliquée, Vol 56. pp, 123-138. 2006.

[MKH 08a] A. Mkhida, J. M. Thiriet, J. F. Aubry - Toward an Intelligent Distributed Safety Instrumented Systems: Dependability Evaluation, World IFAC, Séoul, Juillet 2008.

[MKH 08b] A. Mkhida, J.M. Thiriet, J.F. Aubry - Impact de l'utilisation d'un réseau de communication sur les performances en sécurité d'un système instrumenté de sécurité - 7ème Conférence Francophone de Modélisation et Simulation - Modélisation, Optimisation et Simulation des Systèmes : Communication, Coopération et Coordination, MOSIM'2008, Paris (France), 31 mars-2 avril 2008, pp.203-210.

[MKH 07] A. Mkhida, J. M. Thiriet, J. F. Aubry. Modélisation formelle d'un instrument

intelligent dans le cadre d'analyse de sûreté de fonctionnement. 7ème Congrès International Pluridisciplinaire Qualité et Sûreté de Fonctionnement, Qualita 2007.

[MKH 06a] A. Mkhida, J.M. Thiriet, J.F. Aubry - Evaluation de la fiabilité d'une vanne intelligente par une approche probabiliste - 15ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Lambda-Mu'2006, Lille (France), 9-13 octobre 2006.

[MKH 06b] A. Mkhida, J.M. Thiriet, J.F. Aubry - Effet de la variation des données de fiabilité sur le niveau de sécurité des systèmes d'automatisation distribués - 6ème Conférence Francophone de Modélisation et Simulation - Modélisation,

Optimisation et Simulation des Systèmes , MOSIM'2006, Rabat (Maroc), 3-6 avril 2006, pages: 1120-1126, ISBN: 2-7430-0892-X.

[MKH 05] A. Mkhida, P. Barger, J. M. Thiriet, J. F. Aubry – Influence of the control strategy choice on the safety level of a distributed automation system – Conference ESREL'2005 (European safety and reliability conference, Gdansk-Gdynia (Pologne), 27-30 June 2005.

[Möbius] Möbius, User Manuel. http://www.mobius.uiuc.edu/papers.html

[MON 98] G. Moncelet, «Application des réseaux de Petri à l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile», Thèse de Doctorat, N°3076, Université Paul Sabatier, Toulouse, 9 octobre 1998.

[MOL 81] M. K. Molloy,. On the integration of delay and throughput measures in distributed processing models. Th. 1981. Université de Californie, Los Angeles, EU.

[MOV 84] A. Movaghar, J.F. Meyer. Performability modelling with stochastic activity networks. Proceddings of the 1984 Real Time Systems, Symposium, Austin, TX. Pp 215-224, 2004.

[NAT 80] S. Natkin, Les réseaux de Petri stochastiques et leur application à l'évaluation des systèmes informatiques. Th. Informatique. 1980. Conservatoire National des Arts et Métiers. Paris.

[NF 04] NF EN ISO 12100 Parties 1 et 2 : Sécurité des machines - Notions fondamentales, principes généraux de conception, janvier 2004.

[KUM 96] H. Kumamoto, E. J. Henley, Probabilistic risk assessment and management for enginners and scientists, 2nd edition, IEEE Press, 1996.

[NIC 90] J. L. Nicolet, A. Carnino, J. C. Warner, Catastrophes? Non merci! La preventions des risques technologiques et humains, Edition Masson, Collection Le nouvel Ordre Economique, 1990.

[NOB 04] T. Nobes, Smart instruments in protective measures, Is your product safe? – IEE Seminar, 2004.

[NOI 95] J. L. Noizette, A. Khoury, J. M. Thiriet, M. Robert, un transmetteur intelligent de température au service de l'environnement.

[NYB 97] M. Nyberg, et L. Nielsen. Parity functions as universal residual generators and tool for fault detectability analysis. In Proceedings of the 36th IEEE Conference on Decision and Control, San Diego, USA, pp. 4483 – 4489. (1997).

[PAG 80] A. Pagès, M. Magnien. Fiabilité des systèmes. Editions Eyrolles.

[PAR 01] V. Pareto. On the distribution of wealth and income, in roots of the Italian School of Economics and Finance: from Ferrara (1857) to Einaudi (1944), M. Baldassarri and P. Ciocca, (EDS.), vol. 2, Houndmills, Palgrav. 2001.

[PAR 99] D. Paret, Le bus CAN: Applications. CAL, CANopen, DeviceNet, OSEK, SDS…, Dunod, Paris, 1999.

[PER 04] D. Perry. Selecting sensors for safety instrumented systems per IEC 61511. Emerson Process Management. Rosemount Division. Chanhassen, USA. 2004.

[PRO 02] Profibus: Théorie et pratique de la technologie. www.profibus.com. 2002.

[RAJ 05] C. R. Raju. Strengthening the weak link : the shutdown valve. Sicon / 05. Sensors for Industry Conference. Houston, Texas, USA. February 2005.

[REV 05] J. Revillard, *"*Approche centrée architecture pour la conception logicielle des instruments intelligents*"*, thèse de doctorat, Université de Savoie, Décembre 2005.

[RIC 05] B. Rique, Guide d'interprétation et d'application de la norme CEI 61508 et de ses normes dérivées IEC 61511 (ISA-84.01) et IEC 62061. ISA (The instrumentation, Systems, and Automation Society), Section France, 2005.

[RIE 02] P. Riedinger, C. Iung, J. Daafouz, Commande optimale des systèmes dynamiques hybrides, Théorie et pratique. Conférence internationale francophone d'automatique, CIFA 2002, Nantes, 2002.

[ROB 93] M. Robert, J. M. Riviere, J. L. Noizette, et F. Hermann, Smart sensors in flexible manufacturing systems, Sensors and Actuators A, vol. 37-38, pp. 239-246,1993.

[RUM 91] J. Rumbaugh, M. Blaha, W. Premerlani, F. Eddy, "Object Oriented Modeling and Design", Prentice Hall International, 1991.

[SAF 05] SafetyBus p online. Disponible à : http://www.pilz.com/english/ products/safety/bus/concept.htmi. 2005.

[SAN 95] W. H. Sanders, W. D. Obal, M. A. Qureshi, F. K. Widjanarko. The UltraSAN modelling environment. Performance Evaluation, vol 24, No. 1-2, pp. 89-115. 1995.

[SCH 04] R. Schoenig, Définition d'une méthodologie de conception des systèmes mécatroniques sûrs de fonctionnement, Thèse de L'Institut National Polytechnique de Lorraine. Octobre 2004.

[SCH 99] P. Schnoebelen, Vérification de Logiciels: Techniques et outils du model checking, ouvrage collectif, coordination P. Schnoebelen, Vuibert, ISBN 2-7117-8646-3, , Paris, 1999.

[SHE 94] A. W. Sheer. CIM Computer Integrated Manufacturing. Springer Verlag 1994.

[SHN 00] R. D. Shneeman, K. B. Lee, *"Distributed Measurement and Control Based on the IEEE1451 Smart Transducer Interface Standards"*. IEEE Transactions on Instrumentation and Measurement, 49(3), 2000.

[SHE 98] Shell Global Solutions, Instrument Protective Function Classification, Brochure The Hague Netherlands, 1998.

[SIG 07] J. P. Signoret, Y. Dutuit, A. Rauzy. High Integrity Protection Systems (HIPS): Methods and tools for efficient Safety Integrity Levels (SIL) analysis and calculations. Risk, Reliability and Societal Safety – Aven & Vinnem (eds). Taylor & Francis Group, London. pp, 663-669, 2007.

[SIG 05] J. P. Signoret. Methodology SIL evaluations related to HIPS. Total Draft Memo, April 27-2005.

[SKL 06] S. Sklet. Safety barriers: Definitions, classification and performance. Journal of Loss Prevention in the process industries, vol 19, pp 494-506, 2005.

[SMI 04] D. J. Smith, K. G. L. Simpson, Functional Safety, a Straightforward guide to applying IEC 61508 and Related Standards. Second edition. Elsevier Butterworth Heinemann, 2004.

[STA 05] M. Staroswiecki, Intelligent Sensors: A functional view. IEEE Transactions on Industrial Informatics, Vol 1 N°4. Novembre 2005.

[STA 94] M. Staroswiecki, M. Bayart, Actionneurs intelligents, Hermès, Paris, 1994.

[STE 03] Sternberg, R.J., 2003. A broad view of intelligence — The theory of successful intelligence. Consulting Psychology Journal: Practice and Research 55, 139–154.

[SUM 00a] A. E. Summers, Setting a new standard of the safety instrumented systems, Chemical Engineering, 2000.

[SUM 00b] A. Summers, B. Zachary. Partial-stroke testing of block valves. Control Engineering, 47(12). pp, 87-89. 2000.

[TAI 04] A. T. Tai, W. H. Sanders, L. Alkalai, S. N. Chau, K. S. Tso. Performability analysis of guarded-operation duration: a translation approach for reward model solutions. Performance Evaluation Journal, Vol, 56. Pp, 249–276. 2004.

[TAI 00] J. Tailland, "Instruments intelligents : modèles et outils de conception", Thèse de Doctorat, Université de Savoie, juillet 2000.

[TAN 96] A. H. Taner, N. M. White. Virtual instrumentation: a solution to the problem of design complexity in intelligent instruments. Measurement and Control. Vol 29. pp, 165-171. 1996.

[TAO 05] B. Tao, H. Ding, Y.L. Xiong, Design and implementation of an embedded IP sensor for distributed networking sensing, Sensors and Actuators A 119, (2005), pp. 567-575.

[THI 04] J. M. Thiriet, Sûreté de fonctionnement de systèmes d'automatisation à intelligence distribuée, Habilitation à diriger les recherches. Université Henri Poincaré, Nancy 1, décembre 2004.

[TIA 00] G. Y. Tian, , Z. X. Zhao, et R. W. Baines, A fieldbus-based intelligent sensor, Mechatronics, 2000, vol. 10, pp. 835-849.

[TIX 02] J. Tixier, G. Dusserre, O. Salvi, D. Gaston, 'Review of 62 risk analysis methodologies of industrial plants', Journal of Loss Prevention in the process industries 15, pp. 291–303. 2002.

[TOM 01] M.S. Tombs, Self validating actuators. The Institution of Electrical Engineers. 2001.

[VIL 06] E. Villani, P. I. Kaneshiro, P. E. Miyagi. Hybrid stochastic approach for the modelling and analysis of fire safety systems. Nonlinear Analysis, 2006, vol. 65, pp. 1123-1149.

[VIL 88] A. Villemeur, Sûreté de fonctionnement des systèmes industriels, Edition Eyrolles, Paris, 1988.

[VIN 04] A. Vincent, A. Griffault, G. Point. *Vérification formelle pour Altarica.* Maitrise des risques et sûreté de fonctionnemnt, Lambda-mu 14. Bourges, Septembre 2004.

[VYA 03] V. Vyatkin, H. M. Hanisch. Verification of distributed control systems in intelligent manufacturing. Journal of Intelligent Manufacturing. pp, 123-136, 2003.

[WAL 99] Gregory C. Walsh, Hong Ye and Linda G. Bushnell, Stability Analysis of Networked Control Systems, Proceedings of American Control Conference, June 1999.

[WAN 04] Y. Wang, Development of a computer-aided fault tree synthesis methodology for quantitative risk analysis in the chemical process industry. PhD thesis, Texas A & M University, 2004.

[WAN 01] S. J. Wang. Distributed Diagnosis in Multistage Interconnection Networks. Journal of Parallel and Distributed Computing 61. pp, 254-264. 2001.

[WEI 02] Jan A.M. Weiegerinck, Introduction to the risk based design of safety instrumented systems for the process industry, Seventh International Conference on Control, Automation, Robotics And Vision (ICARV'02), Dec 2002, Singapore.

[WOL 05] V.P. Wolfgang & M.J.M. Houtermans. The effect of the diagnostic and periodic testing on the reliability of safety systems. TUV Industrie Service GmbH, Automation, Software, Information Teschnology (ASI). 2005.

[YAN 05] S. H. Yang, Y. J. Chung, H. C. Kim. Assessment of the MDNBR enhancement methodologies for the SMART control rods banks withdrawal event. Annals of Nuclear Energy 32. pp. 1567-1583, 2005.

[YUR 06] S. Y. Yurish. Digital sensors design based on universal frequency sensors interfacing IC. Sensors and actuators A 132. pp. 265-270, 2006.

[ZHA 04] Y. Zhang, Y. Gu, V. Vlatkovic, X. Wang, Progress of smart sensor and smart sensor networks, Procedings of the 5th World Congress on intelligent Control and Automation, Juin 2004, Hangzhou, Chine.

[ZHA 03] T. Zhang, W. Long, Y. Sato. Availability of systems with self-diagnostic components-applying Markov model to IEC 61508-6. Reliability Engineering Systems Safety (RESS).

[ZHA 01] W. Zhang, M. S. Branicky, S. M. Phillips, Stability of networked control systems, IEEE Control Systems Magazine, pp. 84-99, 2001.

[ZIM 80] H. Zimmerman. OSI reference model. The ISO model of architecture for Opens Systems Interconnexion. IEEE Transaction on Communication 28(4). pp. 425-432, 1980.

INSTITUT NATIONAL
POLYTECHNIQUE
DE LORRAINE

AUTORISATION DE SOUTENANCE DE THESE
DU DOCTORAT DE L'INSTITUT NATIONAL
POLYTECHNIQUE DE LORRAINE

o0o

VU LES RAPPORTS ETABLIS PAR :
Monsieur Yvon VOISIN, Professeur, Université de Bourgogne, Auxerre

Madame Mireille BAYART, Professeur, Université de Lille 1, LAGIS, Villeneuve d'Ascq

Le Président de l'Institut National Polytechnique de Lorraine, autorise :

Monsieur MKHIDA Abdelhak

NANCY BRABOIS
2, AVENUE DE LA
FORET-DE-HAYE
BOITE POSTALE 3
F - 54501
VANDŒUVRE CEDEX

à soutenir devant un jury de l'INSTITUT NATIONAL POLYTECHNIQUE DE LORRAINE, une thèse intitulée :

"Contribution à l'évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité à Intelligence Distribuée"

en vue de l'obtention du titre de :

DOCTEUR DE L'INSTITUT NATIONAL POLYTECHNIQUE DE LORRAINE

Spécialité : « **Automatique et Traitement du Signal** »

Fait à Vandoeuvre, le 03 novembre 2008
Le Président de l'I.N.P.L.,
F. LAURENT

TEL. 33/03.83.59.59.59
FAX. 33/03.83.59.59.55

Résumé

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. L'évaluation de la sûreté de fonctionnement de ce type de systèmes n'est pas triviale. Dans ce travail, la modélisation et l'évaluation des performances relatives à la sûreté de fonctionnement des systèmes instrumentés de sécurité (SIS) sont traitées pour des structures intégrant de l'intelligence dans les instruments de terrain. La méthodologie que nous utilisons 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. La modélisation est traitée sous la forme d'une approche stochastique utilisant les réseaux d'activité stochastiques SAN (*Stochastic Activity Network*). L'introduction d'indicateurs de performances permet de mettre en évidence l'effet de l'intégration des niveaux d'intelligence dans les applications de sécurité. La méthode de Monte Carlo est utilisée pour évaluer les paramètres de sûreté de fonctionnement des SIS en conformité avec les normes de sécurité relatives aux systèmes instrumentés de sécurité (CEI 61508 et CEI 61511). Nous avons proposé une méthode et les outils associés pour approcher cette évaluation par simulation et ainsi apporter une aide à la conception des systèmes instrumentés de sécurité (SIS) intégrant quelques fonctionnalités des instruments intelligents.

Mots-clés *:* Instruments Intelligents, Systèmes d'Automatisation à Intelligence Distribuée, Système Instrumenté de Sécurité, Probabilité de défaillances, Réseaux à activité stochastique, Simulation de Monte-Carlo.

Abstract

The incorporation of intelligent instruments in safety loops leads towards the concept of intelligent safety and the systems become "Intelligent Distributed Safety Instrumented Systems (IDSIS)". The justification for using these instruments in safety applications is not fully proven and the dependability evaluation of such systems is a difficult task. Achieved work in this thesis deals with modelling and thus the performance evaluation relating to the dependability for structures which have intelligence in the instruments constituting the Safety Instrumented Systems (SIS). In the modelling of the system, the functional and dysfunctional aspects coexist and the dynamic approach using the Stochastic Activity Network (SAN) is proposed to overcome the difficulties mentioned above. The introduction of performance indicators highlight the effect of the integration of intelligence levels in safety applications. Monte-Carlo method is used to assess the dependability parameters in compliance with safety standards related to SIS (IEC 61508 & IEC 61511). We have proposed a method and associated tools to approach this evaluation by simulation and thus provide assistance in designing Safety Instrumented Systems (SIS) integrating some features of intelligent tools.

Keywords: Intelligent Instruments, Intelligent Distributed Control Systems, Safety Instrumented Systems, Probability of Failure , Stochastic Activity Network, Monte-Carlo simulation.