Capteurs Intelligents : Nouvelles Technologies et Nouvelles Problématiques pour la Sûreté de Fonctionnement

Florent Brissaud, Dominique Charpentier, Anne Barros, Christophe Bérenguer

CAPTEURS INTELLIGENTS : NOUVELLES TECHNOLOGIES ET NOUVELLES PROBLEMATIQUES POUR LA SURETE DE FONCTIONNEMENT

INTELLIGENT SENSORS: NEW TECHNOLOGIES AND NEW DEPENDABILITY ISSUES

F. Brissaud et D. Charpentier
Institut National de l'Environnement Industriel et des Risques
INERIS – DCE
Parc Technologique ALATA BP-2
60550 Verneuil-en-Halatte

A. Barros et C. Bérenguer
Université de Technologie de Troyes
UTT – ICD/CNRS – ROSAS
12 rue Marie Curie
10010 Troyes Cedex

Résumé

Le développement de la microélectronique a permis d'intégrer de nouvelles technologies au sein des capteurs, celles de « l'intelligence embarquée ». Grâce au numérique, de nouvelles fonctionnalités sont disponibles : correction des erreurs de mesure, auto-ajustage, autodiagnostic des mesures et de l'état du capteur, reconfiguration, communication numérique. Les industriels bénéficient ainsi d'une meilleure exactitude des mesures, de réductions de coût et de facilités d'utilisation. Pour la prévention des risques industriels, de nouvelles problématiques se posent et notamment quant à l'évaluation de la sûreté de fonctionnement. Certaines fonctionnalités sont a priori bénéfiques pour la disponibilité des systèmes de contrôle (diagnostic avancé, communication numérique). Néanmoins, la présence importante d'électronique et d'unités programmables implique des causes et des modes de défaillance supplémentaires. Dans la littérature, les études sur l'évaluation de la disponibilité des capteurs intelligents sont encore relativement faibles et n'intègrent que rarement les fonctionnalités « intelligentes ». Cet article présente certaines problématiques liées à la modélisation et à l'évaluation de la sûreté de fonctionnement de ces capteurs. L'approche proposée associe une décomposition fonctionnelle et matérielle du système, incluant ainsi les fonctionnalités particulières des capteurs et une représentation des différents types d'interactions. Les défaillances constituent la troisième composante du modèle. Les premières analyses permettent d'étudier l'impact des défaillances sur les fonctions du capteur, d'en déduire les modes de défaillance associés et leur évolution au cours du temps. L'application sur un capteur de gaz par absorption infrarouge illustre cette approche. Certains outils pour l'évaluation de la disponibilité de systèmes complexes peuvent tirer profit de ces résultats, en particulier lorsque le comportement du système en cas de défaillance est difficilement appréhendable.

Summary

New technology allows intelligent sensors by integrating new functionalities: error measure correction, self-calibration, self-diagnosis of measures and sensor status, reconfiguration, digital communication. Industrialists take advantage of more accurate measurements, cost reductions and use facilities. For industrial safety, new dependability issues appear. Some functionalities as self-diagnosis and digital communication seem to be in favour of control systems availability. On the other hand, the high amount of electronics and programmable units implies new failure causes and modes. Availability assessments of intelligent sensors are quite low in literature. Moreover, "intelligent" functionalities are usually not taken into account. In this paper, a discussion about dependability issues and modelling is presented. An approach is proposed. Both functional and structural decompositions of the system are included which allow representing sensor functionalities and types of dependencies. Failures make up the third part of the model. First analyses show the consequences of these failures on sensor functions and the corresponding failure modes during time. An infrared gas sensor is used for example. Some tools for availability assessment of complex systems can take advantage of these results, especially when dysfunctional behaviour is not well known.

1. Introduction

La science de la mesure formule deux grandes composantes : les moyens techniques qui permettent l'acquisition de données à partir de grandeurs physiques ; les moyens mathématiques qui manipulent ces données pour obtenir les informations recherchées [1]. Une évolution importante de ces technologies a été motivée par les activités industrielles et militaires. Dans les années 1980, le développement des microsystèmes électromécaniques (MEMS) a amené à une nouvelle révolution au sein des capteurs, celle de l'intelligence embarquée. Les capteurs devenus « intelligents » combinent l'acquisition des données et leur traitement interne et autonome. L'utilisation du numérique a également permis d'intégrer de nouvelles fonctionnalités comme la correction des erreurs de mesure, l'auto-ajustage, l'autodiagnostic, la reconfiguration dynamique et la communication en réseaux. Les bénéfices sont potentiellement nombreux : précision des mesures, coûts, facilités d'utilisation…
De nouveaux défis se présentent alors pour la maîtrise des risques industriels. En particulier, les systèmes instrumentés de sécurité devront tirer partie de ces technologies de façon appropriée. Dans ce contexte, de nouvelles problématiques apparaissent et notamment pour la sûreté de fonctionnement. Par exemple, si les fonctions d'autodiagnostic avancé permettent une meilleure détection des défaillances et une optimisation de la maintenance, la présence importante d'électroniques et de composants programmés implique des causes et des modes de défaillance supplémentaires et souvent difficilement définissables. De plus, les nombreuses données transmises (résultats de mesures, diagnostics sur les mesures et l'état du capteur) sont, en contrepartie, autant de sources d'erreurs supplémentaires.

L'évaluation de la disponibilité d'un capteur intelligent doit donc passer par une première phase de modélisation pour permettre la prise en compte de toutes les fonctionnalités exploitées. Ce papier apporte une première contribution à l'identification des causes et des modes de défaillance envisageables d'un capteur intelligent, ainsi que leurs conséquences sur les données transmises (résultats de mesures, diagnostics). Ces premières analyses sont, en particulier, très utiles à l'évaluation de la disponibilité d'un système de contrôle qui exploite, par exemple, des réseaux de capteurs intelligents en tirant profit de plusieurs types d'informations.
La seconde section introduit les capteurs intelligents en présentant quelques définitions et une architecture matérielle. La Section 3 expose les nouvelles fonctionnalités et les bénéfices apportés par ces capteurs, ainsi que quelques unes de leurs utilisations pour la prévention des risques industriels. Les problématiques que posent ces nouvelles technologies pour la sûreté de fonctionnement sont discutées dans la Section 4. Une étude bibliographique sur l'évaluation de leur fiabilité/disponibilité y est également présentée. Pour permettre une plus grande exhaustivité des évaluations face aux particularités d'un capteur intelligent, la Section 5 s'oriente vers la modélisation de systèmes complexes. Des approches orientées fonctions ou objets y sont décrites. Une modélisation qui permet de représenter les interactions fonctionnelles et matérielles d'un système et qui intègre les défaillances, est ensuite développée. L'exemple d'un capteur de gaz à absorption infrarouge permettra d'illustrer cette approche. Quelques ouvertures vers des analyses quantitatives à partir de ce modèle sont introduites. Des résultats sont également présentés comme l'analyse de l'impact d'une défaillance sur les fonctions du système et l'évolution des modes de défaillance du capteur au cours du temps.

2. Des « Capteurs intelligents » ?

2.1 Définitions

Notons tout d'abord que le mot *capteur* est employé par abus de langage. Par définition, un capteur est le dispositif qui transforme une grandeur physique observée (température, pression, niveau) en une grandeur utilisable (intensité électrique, position d'un flotteur). Pour cela, il possède au moins un transducteur dont le rôle est de convertir une grandeur physique en une autre. Par extension, *capteur* est utilisé pour désigner l'ensemble constitué de capteurs, conditionneurs, transmetteurs de signaux, alimentation. Pour ne pas rompre avec la terminologie usuelle, nous conserverons, dans ce document, cette dernière appellation. Le qualificatif *intelligent* pourrait quand à lui se justifier par les facultés suivantes [2] :
- connaître (par les transducteurs)
- s'adapter aux situations (avec des organes internes de calcul)
- communiquer (par des interfaces de communication)

Deux définitions de *capteur intelligent* semblent alors répandues. La première fait référence à la présence d'un microprocesseur embarqué. Celui-ci peut avoir comme objectif de modifier le comportement interne du capteur afin d'optimiser sa capacité à collecter les données [1], ou simplement pour effectuer localement des traitements et des calculs [3]. La seconde définition se focalise sur la capacité de communication bidirectionnelle du capteur, avec des systèmes extérieurs et des opérateurs humains [4]. Le capteur reçoit et traite des commandes extérieures, et envoie des mesures et des informations de statut [4].
En anglais, une différence entre *smart sensor* (éventuellement traduit en français par *futé*) et *intelligent sensor* a parfois été proposée. L'exploitation d'un micro-processeur embarquée suffirait alors à qualifier un capteur de *smart* [5]. En revanche, c'est sa capacité à participer pleinement au système de contrôle (validation des mesures, diagnostic avancé, reconfiguration dynamique), permis par la communication bidirectionnelle, qui le rendrait, en plus, *intelligent* [6]. Cette distinction n'est cependant pas universelle [6] et il semblerait que ces deux qualificatifs soient maintenant couramment employés comme synonymes.

2.2 Architecture matérielle

Une architecture matérielle applicable à la plupart des capteurs intelligents est proposée sur la figure 1. Elle s'accorde notamment avec le modèle, plus succinct, décrit dans la norme NF EN 60770-3 [4] pour l'évaluation des performances des capteurs intelligents.
L'ensemble *transduction* est composé d'un ou de plusieurs transducteurs utilisés pour générer des signaux électriques représentatifs des grandeurs principales i.e. mesurandes que l'on cherche à observer ; un ou plusieurs transducteurs auxiliaires chargés de surveiller les grandeurs d'influence internes ou externes i.e. grandeurs qui impactent sur les résultats de mesure ou les indications du capteur (température, pression, tension d'alimentation, gaz poisons etc.) ; des conditionneurs de signaux (multiplexeurs, amplificateurs, filtres, convertisseurs analogique-numérique) ; une mémoire pour le stockage de données relatives aux transducteurs (numéro d'identification, grandeur mesurée, caractéristiques métrologiques) utilisées dans les traitements numériques ; des organes actifs comme des commutateurs pour effectuer certaines procédures d'auto-ajustage, d'autodiagnostic ou de reconfiguration (voir section 3.1).
L'ensemble *unité de traitement* contient les logiciels ; stocke en mémoire les paramètres métrologiques et fonctionnels (avec une datation permise par l'horloge interne) ; assure les traitements des données, les calculs et les fonctionnalités du capteur à l'aide de son microprocesseur. L'unité de traitement commande généralement les autres sous-ensembles.
L'ensemble *communication* intègre plusieurs sous-ensembles. La *transmission du signal de mesure* peut être analogique (avec un convertisseur numérique-analogique) ou numérique. Des informations de diagnostic, transmises par le sous-ensemble *communication système*, viennent généralement compléter les résultats. La sortie analogique en 4-20mA, proportionnelle à la grandeur mesurée, est la plus répandue dans l'industrie. Pour y inclure des diagnostics en cas d'erreurs, une plage étendue à 0-24mA est souvent utilisée (par exemple, 0mA pour un problème d'alimentation, 1mA pour des facteurs d'influence hors limites, 24mA lors un dépassement de seuil etc.). La technologie HART [7] utilise le câblage standard en 4-20mA comme support à une communication numérique. Les résultats de mesure sont transmis analogiquement et les informations de diagnostic sont superposées numériquement grâce à un codage de fréquences. Le courant porteur en ligne (CPL) peut également être utilisé pour transmettre des informations de diagnostic tout en évitant des câblages supplémentaires [8]. Les bus de terrain (Profibus, Interbus, Device Net, SafetyBus, Modbus, LonWorks, AS-i etc.) ou les réseaux sans-fil se développent également. Afin de standardiser les interfaces de communications numériques, certains référentiels ont été développés, par exemple par l'Object Management Group (OMG) [9] ou l'IEEE [10].

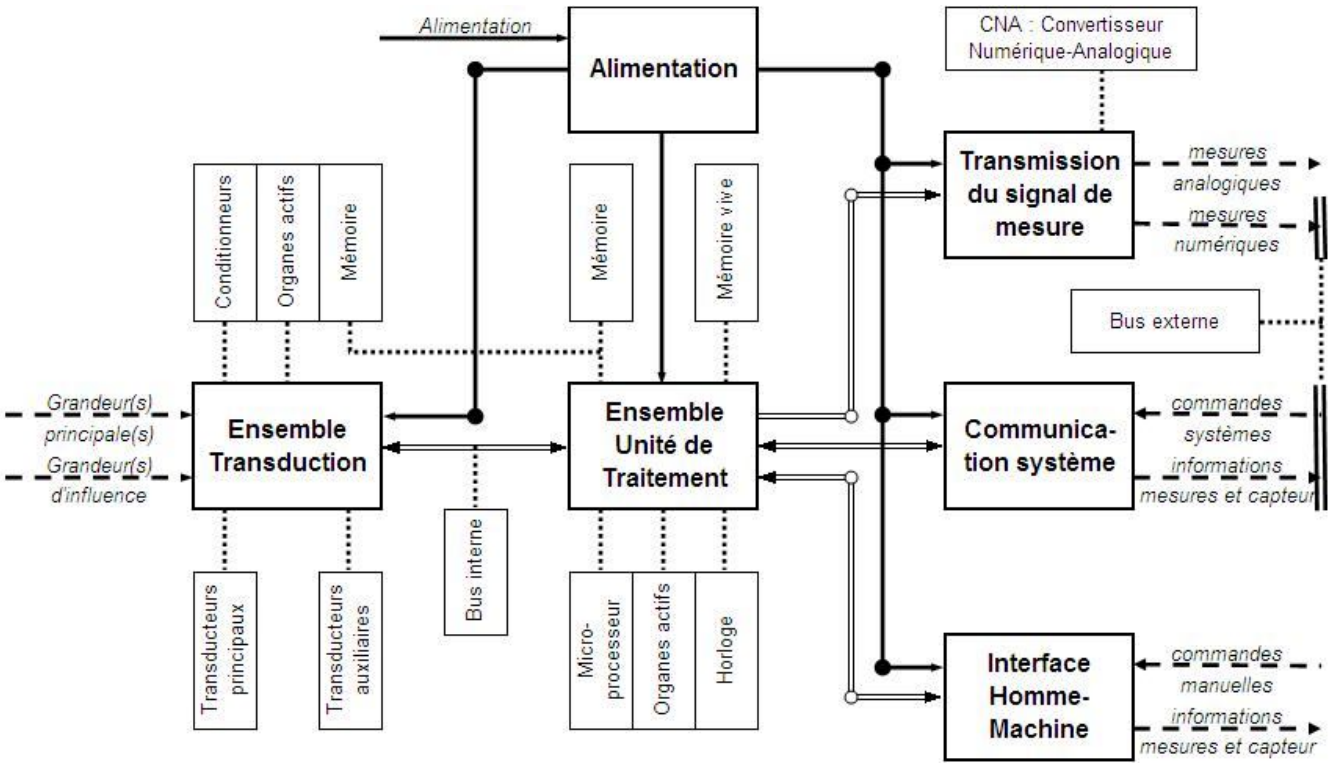

Figure 1. Architecture matérielle d'un capteur intelligent

Indépendamment des protocoles de communication (HART, bus de terrain), des logiciels comme PACTware [11] ont été développés pour la gestion des configurations et des diagnostics de systèmes intelligents. Enfin, des *interfaces homme-machine* (IHM) équipent souvent les capteurs intelligents, par exemple pour communiquer via une console portable.

3. Nouvelles technologies au sein des capteurs

3.1 Fonctionnalités innovantes

Les nouvelles technologies et en particulier l'utilisation du numérique ont rendu disponibles des fonctionnalités innovantes au sein des capteurs. La *correction des erreurs de mesure*, l'*auto-ajustage*, l'*autodiagnostic*, la *reconfiguration dynamique* et la *communication numérique et bidirectionnelle* sont celles présentées ici. Ces cinq capacités jouent, directement ou indirectement, un rôle dans les fonctions génériques d'un capteur intelligent, décrites par M. Robert *et al.* [12] : mesurer, configurer, valider et communiquer. Elles contribuent ainsi à l'objectif principal du capteur qui est de fournir une mesure validée [12].
Parmi les fonctionnalités les plus répandues, on trouve la *correction des erreurs de mesure*. Les transducteurs auxiliaires et les contrôles internes permettent de corriger numériquement les résultats obtenus en fonction des grandeurs d'influence. Les paramètres de correction peuvent être conservés en mémoire. Le stockage avec datation des résultats permet, par exemple, de corriger la linéarité, quelques dérives, voir de remplacer ponctuellement des mesures manquantes ou aberrantes. Des filtrages numériques sont utilisés pour atténuer les bruits. Ils peuvent, dans certains cas, remplacer des filtres analogiques, souvent considérés comme plus couteux et sources de plus grandes dérives et d'imprécisions.
L'*auto-ajustage* est le procédé par lequel un capteur ou un groupe de capteurs se met en conformité avec une fonction de transfert définie lors de l'étalonnage, afin de faire correspondre les indications transmises avec les valeurs des mesurandes [4, 5]. A.H. Taner [13] détaille quatre procédures basiques qui utilisent des commutateurs (organes actifs) pour appliquer en entrée du capteur un signal connu. Des paramètres internes sont alors ajustés pour faire correspondre les résultats de sorti avec ceux attendus. Avec un signal d'entrée nul (relié à la terre), l'ajustement du zéro est obtenu en soustrayant numériquement la valeur du biais observé. Par commutation sur un signal connu et non nul, l'ajustement du gain s'obtient avec des coefficients multiplicateurs. De même, en générant numériquement un signal d'entrée croissant ou échelonné à quelques valeurs connues, il est possible de contrôler la linéarité. Enfin, l'ajustement de la température (grandeur d'influence la plus répandue et souvent simple à mesurer) requière des transducteurs auxiliaires. À partir de quelques échantillons de résultats de mesure et de température, les paramètres de corrections adéquats sont estimés et stockés numériquement. Lorsqu'il y a redondance des capteurs, des ajustages par comparaison des résultats de mesure sont également envisageables. Dans certains cas, par exemple si des dérives importantes sont observées, un auto-ajustage peut être commandé par le capteur lui-même ou le système de contrôle, d'après les informations d'autodiagnostic.
L'*autodiagnostic* utilise généralement des procédures similaires de comparaison des données de sortie avec celles, connues, appliquées en entrée. Ce procédé peut être appliqué aux connectiques (contrôle de la force de transmission), aux éléments de calcul et de traitement des données (vérification du bon déroulement d'un algorithme [12], d'une opération arithmétique, d'un temps de réponse). Des références internes (température de l'électronique, tension d'alimentation) ou externes (facteurs d'influence) peuvent être surveillées. Certains composants ou unités disposent de leurs propres modules de détection des anomalies (condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise [14]). Toutes ces données sont ensuite utilisées dans des modélisations mathématiques, des techniques de reconnaissance des formes ou des réseaux de neurones [3, 15] pour la détection et l'isolation des anomalies (FDI, *Fault Detection and Isolation*). À l'aide de ces résultats, la validation consiste à confirmer ou non la pertinence des informations transmises par le capteur, ou au minimum d'évaluer le degré de confiance que l'on peut leurs accorder. Différents niveaux de validation existent [6, 16] : validation technologique (vérification des ressources physiques), validation fonctionnelle (vérification de la cohérence des données), et validation opérationnelle (par rapport au système de contrôle). A.W. Moran *et al.* [17] présentent trois méthodes probabilistes pour quantifier la validité d'un capteur. Un capteur intelligent est alors potentiellement capable de transmettre des informations sur ses mesures (grandeurs qualitatives ou symboliques [16], incertitude de mesure [15], indice de validité [17]), ou sur son état de fonctionnement [17].
La *reconfiguration dynamique* est une autre fonctionnalité d'un capteur intelligent et qui bénéficie des informations de diagnostic. Certaines caractéristiques du capteur peuvent être modifiées en temps réel, permettant par exemple de répondre à des exigences métrologiques (réglages) : adaptation de la plage de mesure et de la fréquence d'acquisition des données en fonction de l'évolution du phénomène observé et des facteurs d'influence. La reconfiguration peut également avoir des objectifs fonctionnels : gestion optimale des ressources, des fréquences de transmission des données. De plus, des techniques de tolérance aux anomalies peuvent être incluses. Elles consistent à maintenir les aptitudes du capteur en présence de conditions anormales (erreurs logicielles, composants défectueux). Les performances peuvent alors être dégradées mais, à l'échelle du capteur, les anomalies ne doivent pas conduire à une défaillance [18]. Si l'anomalie est faible, il est possible de la compenser numériquement grâce à des paramètres de calcul (accommodation), de la même façon que pour la correction des erreurs de mesure ; le cas échéant, une modification fonctionnelle du capteur (restructuration), par exemple en exploitant des ressources redondantes, permet de maintenir un état de fonctionnement acceptable. F. Guenab [19] intègre des critères de fiabilité pour le choix optimal des configurations.
La *communication* entre le capteur et le système de contrôle ou les interfaces homme-machine est souvent *numérique* afin de transmettre plusieurs types d'information. Elle est également *bidirectionnelle*. Le capteur envoie les résultats de mesure et des informations de diagnostic, et reçoit des commandes et paramètres de fonctionnement du système de contrôle.

3.2 Bénéfices apportés

Les principales motivations qui participent au développement des capteurs intelligents semblent être l'amélioration de la qualité des mesures et la réduction des coûts. Ainsi, l'exactitude des mesures bénéficie des fonctionnalités de correction des erreurs pour l'amélioration de la fidélité (réduction des erreurs aléatoires), et d'auto-ajustage pour l'amélioration de la justesse (réduction des erreurs systématiques). Les informations d'autodiagnostic peuvent aussi participer à ces corrections et la reconfiguration jouer un rôle dans les performances métrologiques. Il est également avancé que la numérisation de la mesure dès son origine réduit la détérioration de la qualité du signal au cours du traitement [2].
Les coûts directs d'un capteur intelligent sont probablement accentués par les éléments électroniques et les logiciels requis (pour les traitements, les calculs, la communication numérique). Néanmoins, ces coûts sont souvent considérés comme faibles par rapport au câblage, à la mis en service, aux contrôles, aux calibrages et à la maintenance des capteurs [2]. Ces aspects bénéficient quant à eux des fonctionnalités apportées par un capteur intelligent. Notons en particulier l'utilisation des bus de terrain qui permettent de réduire les coûts de câblage.
Les facilités d'utilisation que procurent les capteurs intelligents [20] sont également à mentionner, en particulier grâce à la réduction du câblage, à la centralisation des informations simplifiée par la communication numérique, à l'auto-ajustage. Les gains de temps qui en découle sont également un facteur non négligeable [20].

3.3 Utilisations pour la prévention des risques industriels

Les principaux fabricants de détecteurs/capteurs-transmetteurs pour la prévention des risques industrielles commercialisent des systèmes que l'on peut qualifier d'intelligents. Les premiers de ce type arrivés en France ont été des capteurs de pression différentielle, commercialisés par Honeywell dans les années 1980 [2]. Aujourd'hui, des capteurs multivariable (MVD) de chez Micro Motion ou Honeywell combinent des mesures de pression

statique, pression différentielle, flux volumétrique, et compensent en température interne et externe. Des autodiagnostics avancés, auto-validations des résultats de mesures et certaines reconfigurations sont également disponibles. Des capteurs de température de chez Rosemount, installés en redondance, sont coordonnés afin d'améliorer les autodiagnostics et de pouvoir se reconfigurer en cas de défaillance d'un des capteurs. Les détecteurs ou capteurs de gaz, notamment ceux par absorption infrarouge (Industrial Scientific Oldham, Honeywell, Simtronic, Draeger Safety), permettent souvent d'effectuer de nombreuses corrections des erreurs de mesure : encrassement des optiques, température (facteur d'influence important dans la mesure de concentration de gaz), conditions climatiques, vieillissement… De plus, ils disposent de certaines capacités d'auto-ajustage et de nombreuses valeurs d'autodiagnostic sont autocontrôlées. Un exemple de ce type de capteur est présenté dans la section 5.2. Des détecteurs de flamme à rayons infrarouges et ultraviolets de chez Industrial Scientific Oldham possèdent des caractéristiques similaires. Ce dernier fabricant propose également des systèmes de test et d'ajustage automatique à distance, via réseaux. La communication analogique en 4-20mA, ou étendu à 0-24mA est encore la plus répandue. Néanmoins la plupart des fabricants intègre maintenant la technologie HART et certains réseaux de terrain s'installent progressivement.

4. Nouvelles problématiques pour la sûreté de fonctionnement

4.1 Des bénéfices pour la sûreté de fonctionnement ?

Bien que les fonctionnalités offertes par un capteur intelligent apportent certains bénéfices pratiques (voir section 3.2), il convient également d'étudier l'impact de ces particularités sur la sûreté de fonctionnement, en particulier pour la maîtrise des risques. Dans cette section, nous proposons quelques discussions sur les aspects a priori favorables ou défavorables à la sûreté de fonctionnement d'un capteur intelligent, selon trois critères : fiabilité, maintenabilité et sécurité. L'étude de la disponibilité peut se faire par l'intermédiaire de la fiabilité et de la maintenabilité qui sont des attributs de celle-ci.

La *fiabilité* est l'aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps données [21]. Par rapport à un capteur classique, un capteur intelligent intègre de nombreux éléments électroniques additionnels, ainsi que des unités programmables et des aspects logiciels nécessaires au traitement des données, aux calculs, à la communication numérique. Tout ceci représente des causes de défaillances, des sources d'erreurs (pour les résultats de mesure, les informations de diagnostics) et des modes de défaillance supplémentaires. Dans une certaine mesure, ces inconvénients peuvent être, au moins en partie, compensés par des techniques de tolérance aux anomalies. Ainsi, si une anomalie est identifiée par autodiagnostic, elle peut par exemple être compensée numériquement par un changement de paramètres internes ou contournée par l'exploitation de ressources non défectueuses (reconfigurations) [16]. De plus, certaines défaillances qui apparaissent dans la durée, comme les dérives, peuvent être évitées par des corrections d'erreurs ou des auto-ajustages. D'un autre coté, une mauvaise exécution de ces fonctionnalités à cause, par exemple, d'une anomalie logicielle ou matérielle, peut provoquer des défaillances qui ne se seraient pas produites le cas échéant. La communication numérique pose des problématiques similaires. Bien qu'il soit avancé que la réduction du câblage électrique améliore localement la fiabilité [5], les bus de terrain transportent à eux seuls une grande quantité d'informations ce qui leur confère un rôle critique face aux causes communes de défaillance.

La *maintenabilité* tire avantages de l'autodiagnostic. Elle est définie comme (…) l'aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise (…) [21]. Des informations, par exemple sur les dérives, les grandeurs d'influence, les dépassements de seuils, l'alimentation, peuvent être suivis au cours du temps. De plus, un historique des anomalies et des défaillances, avec les circonstances correspondantes, peut être tenu à jour. Toutes ces informations sont ensuite utiles pour optimiser la maintenance préventive par la prévision d'occurrence de certaines défaillances. La centralisation des données, par exemple sur un poste de commande général, est simplifiée grâce à la communication numérique. Chaque capteur peut stocker ses informations personnelles (numéro de série, date de défaillance, du dernier ajustage, de maintenance) qui sont ensuite lisibles par une interface homme-machine. Les actions de maintenance sont ainsi facilitées. Enfin, l'utilisation des bus de terrain rendent la localisation des défaillances et les actions de maintenance corrective plus simples que lors d'un câblage dense.

La *sécurité* est l'aptitude à éviter les dommages inacceptables pour une application donnée. Ici, ce sont encore les capacités d'autodiagnostic qui permettent d'améliorer cet aspect grâce à une meilleure couverture des défaillances détectées. Les conditions de mise en position de replie du capteur, c'est-à-dire conduisant à un état sûre, peuvent être définies avec plus de détails. De plus, la transmission de ces informations à un poste de contrôle permet d'effectuer rapidement les actions correctives adéquates avant l'apparition d'un dommage redouté.

Dans les sections suivantes, après une brève présentation des études disponibles dans la littérature sur l'évaluation de la sûreté de fonctionnement d'un capteur intelligent, quelques problématiques à ces évaluations seront discutées. Une fois ce contexte identifié, une contribution de ce papier sera développée dans la Section 5.

4.2 Évaluation de la sûreté de fonctionnement

L'autodiagnostic se trouve parmi les fonctionnalités les plus déterminantes dans l'évaluation de la sûreté de fonctionnement d'un capteur intelligent. Il s'agit d'une fonction élémentaire pour effectuer ensuite des corrections numériques (correction des erreurs de mesure, auto-ajustage, accommodation) ou physiques (restructuration). Que ce soit pour l'auto-validation ou la tolérance aux anomalies, la fiabilité est utilisée comme critère de décision mais n'est pas le sujet de l'évaluation. Les données de fiabilité sont des attributs d'entrée, pour une configuration matérielle définie et une fonction donnée (généralement la fonction *transmettre une mesure validée* ou *transmettre une mesure qui répond aux critères de précision*).

M. van der Meulen [22] s'est intéressé aux causes communes de défaillances d'un capteur intelligent. Des analyses des modes de défaillance et de leurs effets (AMDE) sont proposées. Il est parfois avancé que la disponibilité d'un capteur intelligent serait comparable à celle d'un capteur classique. Cependant, une problématique des évaluations réside dans l'existence de nouveaux modes de défaillance [22]. Ces derniers pourraient en particulier mener à des causes communes de défaillance supplémentaires.

Un autre aspect important dans l'évaluation de la sûreté de fonctionnement est la communication numérique, par exemple en utilisant des réseaux de terrain. Plusieurs équipements peuvent communiquer sur le même réseau, ce qui lui confère une place centrale dans la disponibilité de tout le système. L. Cauffriez *et al.* [23] présentent un ensemble de contraintes liées aux bus de terrain ainsi que des AMDE. R. Ghostine *et al.* [24] proposent une évaluation quantitative de la disponibilité d'un bus de communication soumis à des erreurs de transmissions. Pour cette analyse, une extension des réseaux de Petri, nommée *Stochastic Activity Networks* (SANs), est choisie. Les réseaux de Petri colorés sont quant à eux utilisés par P. Barger *et al.* [25] pour l'évaluation d'une boucle de sécurité constituée de capteurs, d'actionneurs et d'une unité de contrôle. Les résultats sont obtenus par simulation de Monte Carlo. Face au manque d'informations généralement disponibles sur les données de fiabilité, C. Simon *et al.* [26] intègrent à ces évaluations la théorie des possibilités. Une approche plus formelle, développée par Y.S. Dai *et al.* [27], étudie la fiabilité d'un réseau en fonction de sa topologie. Enfin, d'autres travaux cherchent à optimiser la répartition des capteurs au sein d'un réseau de surveillance de processus industriels. Des critères de mesure, de fiabilité et de coût sont généralement considérés [28], ainsi que ceux de détection et d'isolation des défaillances [29].

Hormis la communication via des réseaux de terrain, les autres fonctionnalités d'un capteur intelligent ne sont pas prises en compte dans ces études. En particulier, les multiples informations transmises (mesures, diagnostics) et les différents modes de défaillances correspondants ne sont pas inclus. Les capteurs ne sont alors pas étudiés en tant que *capteurs intelligents* mais comme des « boites noires » qui transmettent ou non une mesure, supposée correcte.

4.3 Problématiques pour la sûreté de fonctionnement

Comme présenté dans la section 4.1, les fonctionnalités d'un capteur intelligent posent certaines interrogations quant à leurs impacts, bénéfiques ou non, sur la sûreté de fonctionnement. Pourtant, les études qui portent sur l'évaluation de la disponibilité d'un capteur intelligent sont relativement rares dans la littérature. De plus, les particularités de ces capteurs : correction des erreurs de mesure, auto-ajustage, autodiagnostic, reconfiguration, communication des mesures et des informations de diagnostic, ne sont généralement pas inclues dans les analyses. Les modes de défaillance correspondants ne sont donc pas considérés, bien que leurs effets supposés sur la disponibilité d'un système, et notamment face aux causes communes de défaillance, semblent déterminants. De nombreux travaux requièrent pourtant des données de fiabilité, par exemple pour optimiser les stratégies de validation des informations, de reconfiguration, de communication en réseau, de répartition des capteurs. Il serait donc intéressant de développer des études qui concernent plus spécifiquement la sûreté de fonctionnement d'un capteur intelligent. L'objectif est de pouvoir définir son comportement en cas de défaillance ainsi que sa fiabilité (modes de défaillance et quantification) pour permettre l'intégration des particularités « intelligentes » dans des études plus globales, comme par exemple sur les réseaux de capteurs. Les problématiques suivantes se posent alors :

- comme il s'agit de technologies relativement récentes, peu de retour d'expérience qualitatif (modes de défaillance observés) et quantitatif (données de fiabilité) sont disponibles
- les capteurs intelligents sont des systèmes complexes, i.e. de nombreuses interactions peuvent exister entre les composants, mais également entre les fonctions assurées (les paramètres d'autodiagnostic obtenus sont utilisés pour l'auto-ajustage et la correction des erreurs de mesure ; pour maintenir les aptitudes du capteur, une reconfiguration peut donner lieu à une réduction des performances des autres fonctions etc.)
- ces capteurs intègrent des unités programmées et de nombreux aspects logiciels dont les comportements en cas de défaillance ou d'anomalies sont difficilement définissables. De plus, leurs effets peuvent être nuancés parmi plusieurs composants ou fonctions et les différentes informations transmises
- les informations transmises par un capteur intelligent sont multiples et parfois de nature continue (résultats de mesure, incertitudes, indices de validité). Les règles de décision d'un système de contrôle combinent généralement les résultats de mesures et les informations de diagnostic. Ces deux types d'information doivent donc être inclus dans l'analyse des effets des défaillances, ainsi que les combinaisons possibles (bonne mesure mais mauvais diagnostic et vice-versa, etc.)

D'après la norme IEC 61508 [14], un capteur intelligent est donc un système dit de « type B » (modes de défaillance et comportements mal connus, peu de retour d'expérience). Les deux niveaux de complexité d'un capteur intelligent (nombreuses interactions matérielles et fonctionnelles à l'échelle du système, comportements dysfonctionnel sont mal connus à l'échelle des composants) ne permettent pas à une AMDE d'être suffisamment exhaustive et limitent l'utilisation des arbres de défaillance. Pour permettre une évaluation de la sûreté de fonctionnement d'un capteur intelligent nous proposons donc, dans la section suivante, de s'intéresser aux méthodes de modélisations préconisées pour les systèmes complexes.

5. Modélisation de la sûreté de fonctionnement d'un capteur intelligent

5.1 Modélisations orientées *fonctions* ou *objets*

Une distinction sera faite entre les approches orientées *fonctions* qui permettent une décomposition hiérarchique des fonctionnalités d'un système et une représentation de leurs interactions (architectures fonctionnelles) ; et celles orientées *objets* qui centre l'étude sur les éléments matériels (architectures structurelles). Les modèles comportementaux (ou opérationnels) font le lien entre ces deux architectures.

Les analyses fonctionnelles permettent deux aspects : définir, lors de la conception, les fonctions qu'un système doit assurer ; comprendre le fonctionnement effectif d'un système par ses fonctions et ses caractéristiques [30]. C'est ce second point qui nous intéresse ici. La méthode la plus répandue est probablement la méthode SADT (*Structured Analysis and Design Technique*). Des actigrammes représentent les activités d'un système sous forme de boite, et des flèches les contraintes : données d'entrée, de sortie, de contrôle, et les moyens mis en œuvre. Une décomposition hiérarchique par analyse descendante illustre différents niveaux de détails. Cette représentation est proposée par M. Robert *et al.* [12] pour les capteurs intelligents. À l'origine purement descriptive, une extension pour la quantification de la disponibilité nommée Safe-SADT a été développé par V. Benard *et al.* [31]. Les résultats sont obtenus par simulation de Monte Carlo. Elle nécessite néanmoins une très bonne connaissance du système quant aux relations composants-fonctions, aux modes de défaillance et à leurs conséquences sur le système. Moins répandue, les SADT par datagrammes construisent des boites de données reliées entre elles par des flux d'activités. Parmi les principaux inconvénients des SADT on note l'absence d'opérateur logique (porte « ET », « OU ») et de séquences de fonctions. La méthode FAST (*Functional Analysis System Technique*) pallie à cela par une décomposition fonctionnelle suivant trois axes : « Comment ? », « Pourquoi ? », « Quand ? ». Une troisième approche, nommée MFM (*Multilevel Flow Modelling*), analyse les systèmes techniques en deux axes : « moyens – objectifs » et « parties du système – système tout entier ». L'étude se focalise principalement sur les flux (matière, énergie, activité, informations) et est donc particulièrement adaptée aux industries de procédés. Toutes ces méthodes sont semi-formelles [30] et leur objectif premier est descriptif, ce qui posent quelques difficultés pour leur utilisation dans des approches quantitatives.

Plus formalisé, le langage UML (*Unified Modeling Language*) a été développé pour le génie logiciel et permet des modélisations par objets selon 13 types de diagrammes. Pour l'analyse de la qualité de service (performance, temps de réponse) et plus spécifiquement de la disponibilité, les plus utilisés sont :

- les diagrammes de cas d'utilisation (diagrammes de type comportemental) qui expriment les besoins des utilisateurs face au système et recensent les principales fonctionnalités
- les diagrammes de classes (diagrammes de type structurel) qui donnent une représentation abstraite des objets du système et de leurs relations
- les diagrammes d'états-transitions (diagrammes de type comportemental) qui décrivent le comportement du système et de ses composants à l'aide d'automates à états finis

L'approche générale consiste dans un premier temps à utiliser ces diagrammes pour décrire formellement la structure et le comportement du système. Des paramètres dysfonctionnels sont intégrés : états défaillants, modes et taux de défaillance, délais de réparation… Des procédures automatisées transforment ensuite les modèles UML en outils classiques pour la sûreté de fonctionnement, le plus souvent par des réseaux de Petri stochastiques [32]. Les résultats de fiabilité, disponibilité, temps de réponse etc. sont obtenus par simulation. M. Monnin [33] utilise par exemple des diagrammes de classes pour représenter les interactions matérielles et fonctionnelles d'un système soumis à des agressions extérieures. Ensuite, la disponibilité est calculée par simulation à l'aide des *Stochastic Activity Networks* (SANs). Des modèles orientés objets, pour capteurs intelligents, semblables à l'UML, ont été proposés par D. Luttenbacher [34]. AltaRica [35] est un langage formel pour la représentation d'automates de modes (diagrammes d'états-transition), adaptés à la sûreté de fonctionnement. Des logiciels utilisant ce langage ont été développés pour en déduire des arbres de défaillance, des graphes de Markov ou des réseaux de Petri [36]. C. Kheren [37] a par exemple utilisé cette modélisation pour évaluer la sûreté de fonctionnement de systèmes embarqués complexes pour l'aéronautique. Par nature, les modèles orientés *objets* permettent plus aisément la représentation des interactions matérielles que fonctionnelles. En particulier pour la quantification de la disponibilité, ils demandent une description par états du système.

Dans la section suivante, nous proposons une modélisation à la fois orientée *fonctions* et *objets*. Elle est destinée à identifier les effets des défaillances sur les fonctions d'un système qui présente de nombreuses interactions fonctionnelles et matérielles, et ainsi d'en déduire les modes de défaillance correspondant. Les résultats obtenus peuvent en particulier être utilisés pour la définition des états d'un système au comportement dysfonctionnel mal connu.

5.2 Modèle *3-steps* : fonctions, matériels, défaillances

Un capteur qui mesure une concentration de gaz par absorption infrarouge servira d'exemple à la modélisation. Celui-ci se compose de deux unités de mesure infrarouge (IR). La première est celle de travail dont la longueur d'onde du rayon émis est proportionnelle à la concentration du gaz à mesurer. La seconde est l'unité de référence qui émet un rayon insensible au gaz. Par un rapport des longueurs d'onde réceptionnées, une correction de l'encrassement des optiques (vitre et miroir réfléchissant) et des variations des puissances d'émissions est effectuée. Lorsqu'un seuil d'encrassement est atteint, les corrections adéquates ne sont plus possibles et une information de diagnostic le signale. Des organes de chauffe sont intégrés aux éléments optiques afin d'éviter la formation de bué. Le sous-ensemble de mesure optique, constitué des deux unités de mesure IR et des optiques, est commandé par la carte numérique. La concentration de gaz mesurée est fonction de la température. Des corrections numériques sont donc effectuées par l'unité de traitement à partir des mesures faites par les capteurs de température. Lorsque la température est hors du domaine d'acceptabilité, les corrections numériques ne sont plus adaptées et une information de diagnostic le signale. Une alimentation générale est commune au système, et un convertisseur 12V est utilisée par les unités de mesure IR. Ici, nous nous intéresserons uniquement à la partie « capteur » du système, c'est-à-dire aux fonctions suivantes :

- *mesurer* i.e. calculer la concentration de gaz corrigée des grandeurs d'influence (encrassement des optiques, puissance des émissions de rayon IR, température)
- *diagnostiquer* i.e. vérifier que les grandeurs d'influence sont dans les domaines d'acceptabilité
- *ajuster les paramètres* (le zéro et la sensibilité) i.e. définir régulièrement les paramètres numériques utilisés pour les fonctions *mesurer* et *diagnostiquer*

La fonction *communication des informations* n'est pas incluse dans cette étude. *Mesurer* (respectivement *diagnostiquer*), consiste à *acquérir les mesures* issues des unités IR de travail et de référence, ainsi que des capteurs de température. Le *traitement des résultats* (calcule de la concentration de gaz pour la mesure, vérification des seuils d'acceptabilité pour le diagnostic) est ensuite assuré par l'unité de traitement.

Le modèle développé est constitué des *Goal Tree – Success Trees* (*GTST*) pour l'aspect fonctionnel et matériel, combiné aux *Master Logic Diagrams* (*MLD*) pour l'aspect comportemental, initialement proposés par M. Modarres *et al.* [38]. Une telle approche s'adapte particulièrement aux analyses en sûreté de fonctionnement. Elle a notamment été utilisée par A. Jalashgar [39] pour identifier certaines défaillances d'un système complexe. Dans le modèle présenté ici, une adaptation proposée consiste à inclure une représentation des défaillances en tant que composante à part entière. La démarche va ainsi permettre d'évaluer l'impact de chaque défaillance sur les composants puis sur les fonctions du système, et d'identifier les modes de défaillance associés. L'exemple du capteur de gaz par absorption IR est donné sur la Figure 2. La modélisation comprend trois aspects disposés en escalier (*3-steps model*). Le premier est l'arbre des objectifs. L'objectif global du système (*transmettre une mesure et un diagnostic*) est décomposé en fonctions générales (abstraites) puis en fonctions de base (physiques). Une distinction est faite entre les fonctions principales (en traits continus) et les fonctions supports (en traits discontinus). Ces dernières sont présupposées avoir une influence sur le déroulement des premières. Sur le même principe, une décomposition du système (capteur IR) en ses éléments matériels est menée, des sous-systèmes aux unités de base, pour les éléments principaux et support. Le troisième aspect représente un inventaire des défaillances ou anomalies envisageables. Pour cet exemple, nous avons précisé les expressions des fonctions de défiabilité correspondante. Différents niveaux de détail dans la décomposition fonctionnelle, matérielle et pour les défaillances sont bien sûr possibles.

Les relations entre fonctions de base, fonctions support, éléments de base, éléments support, et défaillances, sont symbolisées par des cercles dont la couleur dépend du degré de dépendance. Par exemple, l'impacte de l'unité de mesure IR de référence sur l'ajustage est faible, et elle est moyenne sur les fonctions d'acquisition des mesures principales et auxiliaires.

5.3 Premières analyses

Pour effectuer différents types analyses, nous proposons de traduire les relations de dépendance en probabilités. Les valeurs 0.00, 0.33, 0.67 et 1.00 sont ainsi respectivement attribuées aux relations nulle, faible, moyenne et totale (voir tableau 1, « probabilité par défaut »). Par exemple, l'impact d'une défaillance des capteurs de température peut se lire ainsi : « sachant que l'élément de base "capteurs de températures" est défaillant, la probabilité pour que la fonction *ajuster* soit défaillante est de 1.00 (relation totale), indépendamment des autres éléments matériels ». Cette probabilité est 0.67 pour les fonctions *acquérir les mesures principales* et *acquérir les mesures de diagnostic* (relations moyennes).

Chaque colonne représente des dépendances de type « ET ». Cela signifie par exemple que la défaillance de la fonction *traiter mesures principales* se produit avec une probabilité de 0.67 si la fonction *ajuster* est défaillante « OU » avec une probabilité de 1.00 si l'élément *unité de traitement* est défaillant. Des calculs classiques de fiabilité permettent ainsi de déduire les relations équivalentes entre les défaillances et les fonctions principales de base. Les résultats obtenus sont ensuite traduis graphiquement grâce au tableau 1 (« traduction des résultats ») et sont donnés en tant que « résultats d'analyse » sur la Figure 2. Il est ensuite possible, selon le même principe, de déduire l'impact de chacune des défaillances sur les fonctions principales générales (*mesurer* et *diagnostiquer*). Ici nous définirons les modes de défaillance comme les combinaisons possibles de ces deux fonctions générales : défaillance sans effet, perte du diagnostic seul, perte de la mesure seule, perte commune du diagnostic et de la mesure

En modélisant l'occurrence de chaque défaillance par la fonction de défiabilité adéquate (fonctions *F(t)* sur la Figure 2), il est possible de décomposer chacune des probabilités de défaillance à la demande selon le mode de défaillance causé au système. Dans notre exemple, le capteur IR utilise en redondance deux capteurs de température. La probabilité de défaillance à la demande des capteurs de température, en fonction du temps (*PFD(temps)*), est représentée sur la Figure 3. D'après ce résultat, la défaillance des deux capteurs de température entraine avec une plus forte probabilité la perte de la mesure seule plutôt que du diagnostic seul, mais dans la majorité des cas, ces deux fonctions ne sont plus assurées. En combinant l'occurrence de toutes les défaillances listées à la Figure 2, la répartition dans le temps des modes de défaillance du capteur IR est représentée sur la Figure 4. Toutes défaillances confondues, on constate alors que, dans un premier temps, il y a une probabilité relativement importante qu'une défaillance n'implique la perte que d'une seule fonction (*mesurer* ou *diagnostiquer*), ou soit sans effet. En revanche, après un certain temps d'exploitation du capteur IR, la probabilité pour que toutes les fonctions soient perdues (*mesurer* et *diagnostiquer*), à cause d'une ou de plusieurs défaillances, est dominante.

Type de relation	Probabilité par défaut (donnée d'entrée)	Traduction des résultats	
		min	max
totale / forte	1.00	0.83	1.00
moyenne	0.67	0.50	0.83
faible	0.33	0.17	0.50
nulle / très faible	0.00	0.00	0.17

Tableau 1. Codage des relations de dépendance

D'autres analyses plus détaillées pourront par exemple inclure plusieurs types de dépendance sous la forme de différentes portes logiques (« OU », « ET », « MooN »). Des séquences d'évènements pourront également être étudiées (par exemple, l'ajustage est effectuée périodiquement ou sous conditions d'autres évènements). L'évaluation des probabilités correspondantes aux différentes relations (voir tableau 1) est à approfondir. Les incertitudes sur ces données peuvent cependant être prises en compte, par exemple à l'aide de densités de probabilité ou de logique floue. Notons qu'il est aussi envisageable de définir des relations dynamiques, fonctions du temps ou d'évènements. Y. Hu *et al.* [40] proposent quelques pistes permettant de répondre à certaines de ces problématiques.

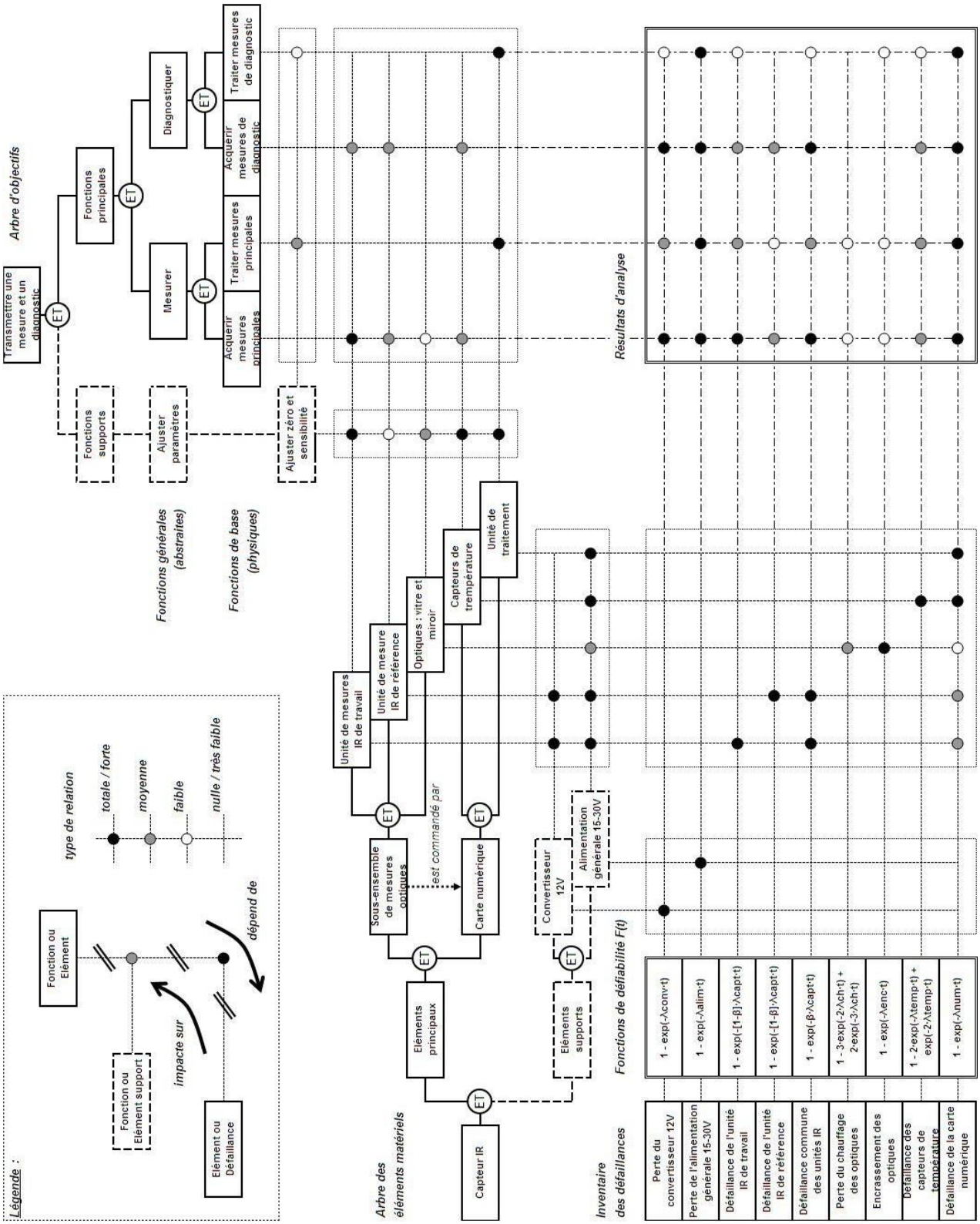

Figure 2. Modélisation « *3-steps* » d'un capteur de gaz par absorption infrarouge

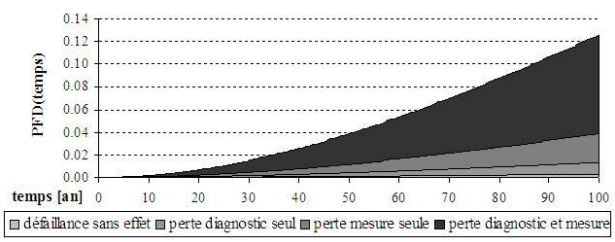

Figure 3. Probabilité de défaillance à la demande des capteurs de température avec modes de défaillance causés au capteur IR

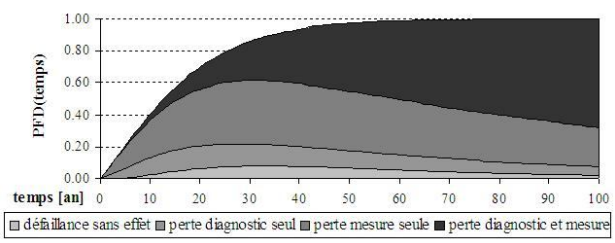

Figure 4. Probabilité de défaillance à la demande du capteur IR avec répartition des modes de défaillance

6. Conclusion

Les capteurs intelligents tirent profit des nouvelles technologies pour intégrer des fonctionnalités innovantes : correction des erreurs de mesure, autodiagnostic, reconfiguration etc. dont les bénéfices sont potentiellement nombreux. L'utilisation de tels systèmes pour la prévention des risques industriels posent cependant quelques problématiques, notamment quant à l'évaluation de la sûreté de fonctionnement. Les études sur la fiabilité et la disponibilité des capteurs intelligents sont encore relativement peu répandues dans la littérature. De plus, elles n'incluent que rarement les fonctionnalités « intelligentes » de ces systèmes. De part les nombreuses interactions matérielles et fonctionnelles, un tel capteur représente un système complexe. Différentes approches sont alors envisageables pour une modélisation adaptés à la sûreté de fonctionnement. L'utilisation de ces outils pour une évaluation quantitative rencontre cependant quelques difficultés dont celle de définir et de quantifier les modes de défaillance d'un capteur intelligent, sachant que les effets de nombreuses anomalies ou défaillances sont mal connus. Nous proposons alors une modélisation qui intègre des décompositions arborescentes des fonctions et éléments matériels, et des défaillances, avec une représentation des différentes relations associées. Les premières analyses permettent d'en déduire l'impact de chaque défaillance sur les fonctions du système, puis d'en conclure sur les modes de défaillance que cela implique. Certains résultats quantitatifs peuvent être directement obtenus comme la répartition des modes de défaillance d'un système au cours du temps. Cette approche peut également servir d'étape préliminaire à l'utilisation d'autres méthodes d'évaluation lorsque le comportement dysfonctionnel du système est difficile à appréhender.

Références

[1] J. E. Brignell, "The future of intelligent sensors: A problem of technology or ethics?," *Sensors And Actuators A-Physical*, vol. 56, pp. 11-15, 1996.

[2] CIAME, *Livre Blanc, Les capteurs intelligents : Réflexion des utilisateurs*. Paris : AFCET, ISBN : 1002061, 1987.

[3] H. Schodel, "Utilization Of Fuzzy Techniques In Intelligent Sensors," *Fuzzy Sets And Systems*, vol. 63, pp. 271-292, 1994.

[4] AFNOR, *NF EN 60770-3 Transmetteurs utilisés dans les systèmes de conduite des processus industriels - Partie 3 : Méthodes pour l'évaluation des performances des transmetteurs intelligents*. Norme AFNOR, 2006.

[5] G. Smith and M. Bowen, "Considerations for the utilization of smart sensors," *Sensors And Actuators A-Physical*, vol. 47, pp. 521-524, 1995.

[6] CIAME : M. Bayart, B. Conrard, A. Chovin et M. Robert, "Capteurs et actionneurs intelligents," *Techniques de l'ingénieur*, S 7 520, 2005.

[7] HART Communication Foundation, *HART Field communication protocol - Application guide HCF LIT 34*, 1999.

[8] Siemens AG, *iq-sense Communication involves intelligence, Sensors and control become one system*, 2004.

[9] Object Management Group, *Smart Transducers Interface Specification*, 2003.

[10] IEEE, *1451 Smart Transducer Interface for Sensors and Actuators*, IEEE Standard, 2007.

[11] PACTware Consortium e.V., *PACTware Efficient configuration*, 2005.

[12] M. Robert, M. Marchandiaux et M. Porte, *Capteurs intelligents et méthodologie d'évaluation*. Paris : Hermes, ISBN : 2-86601-382-4,1993.

[13] A. H. Taner and J. E. Brignell, "Aspects of intelligent sensor reconfiguration", *Sensors And Actuators A-Physical*, vol. 47, pp. 525-529, 1995.

[14] International Electrotechnical Commission, *IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems*, IEC Standard, 2002.

[15] G.Y. Tian, Z.X. Zhao and R.W. Baines, "A Fieldbus-based intelligent sensor," *Mechatronics*, vol. 10, pp. 835-849, 2000.

[16] M. Staroswiecki, "Intelligent sensors: A functional view", *Ieee Transactions On Industrial Informatics*, vol. 1, pp. 238-249, 2005.

[17] A.W. Moran, P.G. O'Reilly and G.W. Irwin, "Probability estimation algorithms for self-validating sensors," *Control Engineering Practice*, vol. 9, pp. 425-438, 2001.

[18] M. Blanke, R. Izadi-Zamanabadi, S.A. Bogh and C.P. Lunau, "Fault-tolerant control systems - A holistic view," *Control Engineering Practice*, vol. 5, pp. 693-702, 1997.

[19] F. Guenab, *Contribution aux systèmes tolérants aux défauts : Synthèse d'une méthode de reconfiguration et/ou de restructuration intégrant la fiabilité des composants*, Université Henri Poincaré, Nancy 1, 2007.

[20] Y. Belgnaoui, "Les capteurs parlent, les utilisateurs en profitent," *Industrie et Technologie*, Le dossier du mois, vol. 0873, 2005.

[21] International Electrotechnical Commission, *IEC 60050(191) International Electrotechnical Vocabulary, Chapter 191: Dependability and quality of service*, IEC Standard, 1990.

[22] M.J.P. van der Meulen, "On the use of smart sensors, common cause failure and the need for diversity," *6th International Symposium Programmable Electronic Systems in Safety Related Applications*, TUV, 2004.

[23] L. Cauffriez, J. Ciccotelli, B. Conrard and M. Bayart, "Design of intelligent distributed control systems: a dependability point of view," *Reliability Engineering & System Safety*, vol. 84, pp. 19-32, 2004.

[24] R. Ghostine, J.M. Thiriet and J.F. Aubry, "Dependability evaluation of networked control systems under transmission faults," *6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Safeprocess 2006*, Beijing, P.R. China, 2006.

[25] P. Barger, J.M. Thiriet, M. Robert and J.F. Aubry, "Dependability study in distributed control systems integrating smart devices," *Cost Oriented Automation 2004*, 7-9 June, Ottawa, Canada, 2004.

[26] C. Simon, J.M. Thiriet and P. Barger, "Reliability and credibility evaluation of networked control systems," *ESREL 2005 Advances in safety and reliability*, July, Poland, 2005.

[27] Y.S. Dai, M. Xie, K.L. Poh and G.Q. Liu, "A study of service reliability and availability for distributed systems," *Reliability Engineering & System Safety*, vol. 79, pp. 103-112, 2003.

[28] C. Benqlilou, M. Graells, E. Musulin and L. Puigjaner, "Design and retrofit of reliable sensor networks," *Industrial & Engineering Chemistry Research*, vol. 43, pp. 8026-8036, 2004.

[29] M. Bhushan, S. Narasimhan and R. Rengaswamy, "Robust sensor network design for fault diagnosis," *Computers & Chemical Engineering*, vol. 32, pp. 1067-1084, 2008.

[30] M. Lambert, B. Riera and G. Martel, "Application of functional analysis techniques to supervisory systems," *Reliability Engineering & System Safety*, vol. 64, pp. 209-224, 1999.

[31] V. Benard, L. Cauffriez and D. Renaux, "The Safe-SADT method for aiding designers to choose and improve dependable architectures for complex automated systems," *Reliability Engineering & System Safety*, vol. 93, pp. 179-196, 2008.

[32] A. Bondavalli, M. Dal Cin, D. Latella, I. Majzik, A. Pataricza and G. Savoia, "Dependability analysis in the early phases of UML-based system design," *Computer Systems Science And Engineering*, vol. 16, pp. 265-275, 2001.

[33] M. Monnin, *Approche unifiée défaillance/dommage dans la sûreté de fonctionnement pour la régénération des matériels au combat, Application aux systèmes d'armes terrestres*, Université de Valenciennes, 2007.

[34] D. Luttenbacher, *Modélisation du concept capteur intelligent par une approche orientée objet : application à un capteur intelligent de température*, Université Henri Poincaré, Nancy I, 1997.

[35] LaBRI, *Altarica Project*, http://altrica.labri.fr/wiki

[36] ARBoostTechnologies, *Altarica Data-Flow Toolbox*, http://www.arboost.com

[37] C. Kehren, *Motifs formels d'architectures de systèmes pour la sûreté de fonctionnement*, École Nationale Supérieure de l'Aéronautique et de l'Espace, Toulouse, 2005.

[38] M. Modarres and S.W. Cheon, "Function-centered modeling of engineering systems using the goal tree-success tree technique and functional primitives," *Reliability Engineering & System Safety*, vol. 64, pp. 181-200, 1999.

[39] A. Jalashgar, "Identification of hidden failures in process control systems based on the HMG method," *International Journal of Intelligent Systems*, vol. 12, pp. 159-179, 1998.

[40] Y. Hu and M. Modarres, "Evaluating system behavior through Dynamic Master Logic Diagram (DMLD) modeling," *Reliability Engineering & System Safety*, vol. 64, pp. 241-269, 1999.