Contribution à l'évaluation de sûreté de fonctionnement des architectures de surveillance/diagnostic embarquées. Application au transport ferroviaire

Jean Gandibleux

Numéro d'ordre: 13/31

Thèse de doctorat

Pour obtenir le grade de Docteur de l'Université de

VALENCIENNES ET DU HAINAUT-CAMBRESIS

Spécialité Automatique Informatique Industrielle et Systèmes Homme Machine

Présentée et soutenue par Jean GANDIBLEUX.

Le 06/12/2013, à Valenciennes.

Ecole doctorale :
Sciences Pour l'Ingénieur (SPI)

Equipe de recherche, Laboratoire :
Laboratoire de Thermique, Ecoulement, Mécanique, Mise en Production (TEMPO)

Contribution à l'évaluation de sûreté de fonctionnement des architectures de surveillance/diagnostic embarquées. Application au transport ferroviaire.

JURY

Présidente du jury
- BAYART, Mireille. Professeur à l'Université de Lille 1, LAGIS.

Rapporteurs
-THIRIET, Jean-Marc. Professeur à l'Université Joseph Fourier de Grenoble, GIPSA Lab.

AUBRUN, Christophe. Professeur à l'Université de Lorraine, CRAN.

Examinateur
-GENON-CATALOT, Denis. Maître de conférences à l'Université Pierre Mendès France, LCIS-Grenoble INP.

Directeur de thèse
- CAUFFRIEZ, Laurent. Maître de conférences HDR à l'Université de Valenciennes et du Hainaut-Cambrésis, TEMPO/PSI.

- Co-encadrant : CLARHAUT, Joffrey. Maître de conférences à l'Université de Valenciennes et du Hainaut-Cambrésis, TEMPO/PSI.

Membre invité
- BRANGER, Guillaume. Ingénieur R&D, BOMBARDIER Transport France, Crespin.

Avant propos

Les travaux présentés dans ce mémoire de thèse ont été réalisés dans le cadre du projet FUI SURFER (SURveillance active FERroviaire), au Laboratoire TEMPO (Thermique, Ecoulement, Mécanique, Matériaux, Mise en Forme, PrOduction) et à l'entreprise BOMBARDIER Transport France. Le laboratoire TEMPO est une unité de recherche (EA 4542) membre de l'institut Carnot ARTS. Le laboratoire TEMPO se situe à l'université de Valenciennes et du Hainaut-Cambrésis (UVHC).

J'adresse tous mes remerciements à Monsieur Laurent CAUFFRIEZ, Maître de conférences Habilité à Diriger des Recherches, et Monsieur Joffrey CLARHAUT, Maître de conférences, d'avoir accepté de diriger cette thèse. Je les remercie des nombreuses critiques constructives dont ils m'ont fait part pour ce travail de thèse.

Je remercie Madame Mireille BAYART, Professeur des Universités, d'avoir présidé le jury lors de la soutenance de cette thèse.

J'exprime toute ma gratitude à Monsieur Jean-Marc THIRIET, Professeur à l'Université Joseph Fourier, et Monsieur Christophe AUBRUN, Professeur à l'Université de Lorraine, de m'avoir fait l'honneur d'être rapporteurs des travaux de ce mémoire.

Je remercie également Monsieur Denis GENON-CATALOT, Maître de conférences, de l'intérêt qu'il a porté à ce travail de recherche en acceptant de participer à ce jury en tant qu'examinateur.

Je tiens à remercier Damien TRENTESAUX, Professeur à l'Université de Valenciennes et du Hainaut-Cambrésis et Guillaume BRANGER, ingénieur R&D chez BOMBARDIER Transport France, d'avoir accepté ma candidature à ce sujet de thèse.

Je remercie les deux partenaires de cette thèse, à savoir l'entreprise BOMBARDIER Transport et l'Université de Valenciennes et du Hainaut-Cambrésis, de m'avoir accueilli et d'avoir rendu cette recherche possible. Durant cette thèse, j'ai intégré l'équipe FIELD-FRACAS-REX de BOMBARDIER Transport France et je n'oublie pas de remercier l'ensemble de ses membres (Christophe DUPAS, Quentin COUTADEUR, Aurélien DUCATILLON, Luc RAUWEL, Jo STEVENS, Guillaume BRANGER, Reynald COPIN) pour leur collaboration et pour la transmission de leur expérience et de leur savoir-faire. Je remercie également l'ensemble des personnes (ouvriers, techniciens et ingénieurs) que j'ai croisées et que je n'ai pas citées ci-dessus, pour leur collaboration.

Sommaire

Abréviations et acronymes utilisés

A(t)	Disponibilité instantannée
CTAA	(de l'anglais " Cumulative Time spent on analyzing All Alarms ") : temps cumulé passé à analyser toutes les alarmes
CTFA	(de l'anglais " Cumulative Time spent on analyzing False Alarms ") : temps cumulé passé à analyser des fausses alarmes
CTTA	(de l'anglais " Cumulative Time spent on analyzing True Alarms ") : temps cumulé passé à analyser des vraies alarmes
EDCD	(de l'anglais " Embedded Decentralized and Cooperative Diagnosis ") : diagnostic embarqué décentralisé et coopérant
FMD	Fiabilité, Maintenabilité, Disponibilité
FUI	Fonds Unique Interministériel
GAMAB	Globalement Au Moins Aussi Bon
LCC	(de l'anglais " Life Cycle Cost ") : coût global de possession
MDT	(de l'anglais " Mean Down Time ") : durée moyenne d'indisponibilité
MTTF	(de l'anglais " Mean Time To Failure ") : temps moyen avant la première défaillance
MTTR	(de l'anglais " Mean Time To Repair ") : durée moyenne de réparation
NAA	(de l'anglais " Number of All Alarms") : nombre total d'alarmes
NFA	(de l'anglais " Number of False Alarms ") : nombre de fausses alarmes
N_{RE}	(de l'anglais " Number of Residual Errors") : nombre d'erreurs résiduelles sur les réseaux de communication
NTA	(de l'anglais " Number of True Alarms ") : nombre de vraies alarmes
PTFA	Pourcentage de Temps d'analyse passé à analyser des Fausses Alarmes
RCD	(de l'anglais " Remote Centralized Diagnosis") : diagnostic distant centralisé
RdP	Réseaux de Petri
RdPC	Réseaux de Petri Colorés
SURFER	SURveillance active FERroviaire
S_D	Système de Diagnostic local "bas niveau"
S_D*	Système de Diagnostic local "haut niveau"
S_E	Système Elémentaire
S_EDN	(de l'anglais " Embedded Diagnosis Network") : Réseau de communication embarqué pour le diagnostic
S_GD	(de l'anglais " Global Diagnosis System ") : Système de diagnostic global
S_TWN	(de l'anglais " Train-to-wayside Network ") : Réseau de télécommunication train-sol

Introduction générale

Dans le transport ferroviaire, le coût global de possession du matériel roulant est une question majeure. Pour les exploitants de matériel roulant, cet élément représente un facteur de compétitivité important face aux autres modes de transport ou encore face à l'arrivée d'une nouvelle concurrence, suite à l'ouverture des marchés d'exploitation des lignes conventionnelles en 2010 (CCE,2004).

Cette mise en concurrence pousse de plus en plus les exploitants à vouloir acquérir des matériels roulants en prenant en compte le coût global de possession LCC (de l'anglais « Life Cycle Cost »), optimisant le coût de maintenance pendant la vie du matériel roulant. Le LCC est un des indicateurs de performance des marchés modernes (Schweiger,2009). En effet, il existe une demande forte en maintenance plus efficace, plus réactive (compte-tenu de la concurrence d'autres exploitants) et moins coûteuse, au lieu du modèle historique de maintenance préventive organisée sur le territoire national.

Pour optimiser la maintenance, une approche consiste à améliorer le diagnostic (Marquez et al.,2008)(Utne et al.,2012). Dans ce cadre, Bombardier Transport conduit actuellement plusieurs projets de recherche (Cauffriez et al.,2013)(Bombardier,2010) (Gandibleux et al.,2011). Cette thèse est réalisée dans le cadre du projet SURFER (pour SURveillance active FERroviaire) financé par le FUI (Fonds Unique Interministériel), qui vise le développement d'une architecture de diagnostic efficace (ISO13374-1,2003). La nouvelle architecture de diagnostic repose sur l'utilisation de capteurs intelligents et de réseaux de communication. Ces technologies offrent de nouvelles possibilités mais engendrent cependant de nouvelles contraintes notamment en matière de sûreté de fonctionnement. La complexité induite par l'intégration des systèmes intelligents rend la quantification du niveau de sûreté de fonctionnement plus difficile.

De plus, le projet FUI SURFER se déroule dans le transport ferroviaire français, où la démarche de risque est préconisée (EN50126,2000). Dans ce secteur, le risque doit être abordé selon le principe GAMAB (acronyme de "Globalement Au Moins Aussi Bon"). Selon le principe GAMAB, l'architecture de diagnostic développée doit être non-intrusive, c'est-à-dire qu'elle ne doit pas interférer avec le bon fonctionnement du système élémentaire (existant). L'architecture de diagnostic ne doit donc pas diminuer la disponibilité du système élémentaire (EN50126,2000). La non-intrusivité, qui diffère de l'approche classique pour les systèmes tolérants aux fautes (voir chapitre 1), est imposée par Bombardier Transport et donc le système de diagnostic et le système élémentaire (c'est-à-dire le système soumis au diagnostic) sont indépendants. Cette exigence de non-intrusivité provient de l'indisponibilité en exploitation, suite aux défaillances de ces systèmes. Cette indisponibilité est habituellement liée à une gravité importante (EN50126,2000).

Pour ces raisons, la conception d'une nouvelle architecture de diagnostic est un défi. Ceci a conduit à cette thèse. Les travaux présentés dans ce mémoire de thèse proposent des modèles et un protocole de validation, afin d'évaluer la FMD (Fiabilité, Maintenabilité, Disponibilité) d'architectures de diagnostic. La tâche est rendue difficile, du fait de la complexité inhérente aux systèmes intelligents, du fait de l'emploi de réseaux de communication et du fait de la grande taille d'un système de transport ferroviaire. Ces observations ont orienté le choix vers les réseaux de Petri colorés.

Dans le premier chapitre, les notions de fiabilité, maintenabilité et disponibilité et les notions de base en surveillance, diagnostic et gestion de faute non-intrusive sont rappelées afin de donner un cadre théorique aux travaux réalisés. Puis, quelques travaux de la littérature, proches de la problématique d'évaluation d'architectures de diagnostics sont recensés. Les formalismes utilisés pour l'évaluation de FMD des architectures de diagnostic sont également présentés.

Nous détaillons au deuxième chapitre le contexte général et les objectifs de ces travaux de thèse, qui se déroulent dans le cadre du projet FUI SURFER. Les architectures de diagnostic du transport ferroviaire sont présentées, afin de mieux cerner les limites de la situation actuelle et la solution envisagée dans le projet FUI SURFER. Cette présentation permet de poser les objectifs de cette thèse, qui consiste à modéliser et évaluer d'un point de vue FMD des architectures de diagnostic. Enfin, les verrous scientifiques de cette thèse liés aux réseaux de communication, au diagnostic et à la sûreté de fonctionnement sont identifiés.

Le troisième chapitre justifie et présente le formalisme retenu, à savoir les Réseaux de Pétri colorés associés à la résolution par simulation de Monte Carlo. Dans un premier temps, nous proposons un modèle générique pour les réseaux de communication, qui occupent une place centrale dans les architectures de diagnostic du transport ferroviaire. Puis nous proposons des modèles en Réseaux de Pétri colorés des architectures de diagnostic. Les modèles proposés sont ensuite validés, par un protocole composé de cas pessimistes et optimistes, qui permet de valider les résultats en sortie du modèle pour les valeurs d'entrée retenues.

Le quatrième chapitre applique les modèles proposés sur un cas réel proposé par Bombardier, où les systèmes élémentaires sont des accès voyageurs. Dans un premier temps, la distribution du taux de défaillance et la distribution des temps de réparation sont estimées à partir du retour d'expérience fourni par Bombardier. Puis, les paramètres des réseaux de communication et des systèmes de diagnostic sont quantifiés. Les résultats pour l'application réelle sont obtenus et discutés. Devant le manque de données concernant le réseau de communication bord sol et le réseau de communication embarqué pour le diagnostic, nous décidons de présenter des études de sensibilité afin d'étudier l'influence de leur dysfonctionnement sur la FMD des architectures de diagnostic.

Le cinquième chapitre présente la conclusion de nos travaux de recherche et introduit les perspectives identifiées, tant sur le plan scientifique que sur le plan industriel.

Chapitre 1 : état de l'art

Chapitre 1 : état de l'art

Introduction

Ce chapitre présente les différentes notions utilisées dans cette thèse, qui a pour but d'évaluer d'un point de vue FMD (Fiabilité, Maintenabilité, Disponibilité) des architectures de diagnostic. Pour ce faire, la partie 1 présente des notions d'ordre général sur la FMD, qui fait partie de la sûreté de fonctionnement ainsi que les méthodes généralement utilisées pour réaliser une évaluation FMD. La partie 2 rappelle les notions sur le diagnostic et présente une typologie d'architectures de diagnostic. Enfin, la partie 3 présente un état de l'art sur l'évaluation FMD des architectures de diagnostic.

1. Sûreté de fonctionnement

Cette partie vise à rappeler les concepts de sûreté de fonctionnement qui sont utilisés par la suite. La première section présente les concepts fondamentaux de la sûreté de fonctionnement : les attributs, les moyens et les entraves. La seconde section présente les mathématiques de la sûreté de fonctionnement. La troisième section présente les méthodes usuelles pour quantifier les attributs de la sûreté de fonctionnement des systèmes.

1.1. Concepts fondamentaux

Les concepts fondamentaux de la sûreté de fonctionnement sont habituellement illustrés par l'arbre de la sûreté de fonctionnement. Ceux-ci comprennent les notions de fiabilité, de disponibilité, de maintenabilité et de sécurité.

1.1.1. L'arbre de la sûreté de fonctionnement

La sûreté de fonctionnement est « l'aptitude d'une entité à réaliser une ou plusieurs fonctions requises dans des conditions données ». Elle est la science des défaillances (Zwingelstein,1995) (Villemeur,1991).

La sureté de fonctionnement peut être appliquée au niveau d'un processus, d'un système, d'un composant, suivant la profondeur de l'analyse. Dans la suite de cette section sur la sûreté de fonctionnement, le terme "entité" est utilisé pour faire référence à l'élément considéré dans l'analyse (un processus, un système, un composant…).

Les concepts fondamentaux de la sûreté de fonctionnement sont classés en trois groupes dans l'arbre de la sûreté de fonctionnement (Avizienis et al.,2000)(Figure 1) : les attributs de la sûreté de fonctionnement, les entraves à la sûreté de fonctionnement, et les moyens par lesquels la sûreté de fonctionnement est atteinte.

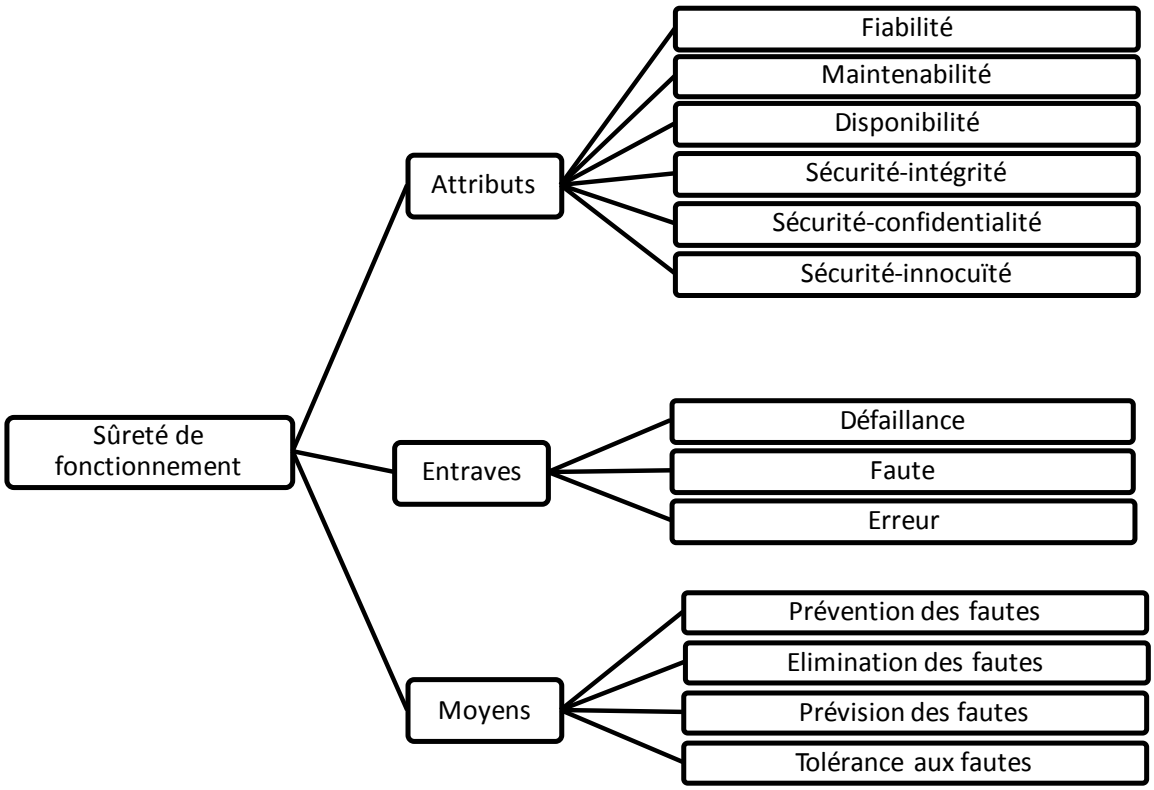


Figure 1 : Arbre de la sûreté de fonctionnement, adapté de (Avizienis et al.,2000).

Les attributs de la sûreté de fonctionnement expriment les objectifs attendus pour l'entité en termes de fiabilité, disponibilité, maintenabilité et sécurité pour l'entité.

1.1.2. La fiabilité

La fiabilité est l'aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné. Il est généralement admis que l'entité est en état d'accomplir la fonction requise au début de l'intervalle de temps donné (Villemeur,1991).

Selon les circonstances, la fiabilité peut être évaluée à l'aide d'un ensemble de critères :

- la probabilité, notée *R(t)*, que l'entité soit non-défaillante sur l'intervalle de temps [0,t[, sachant qu'elle n'était pas
- défaillante à t=0
- la probabilité, notée $F(t)$, pour que l'entité fasse l'objet d'une défaillance sur un intervalle de temps donné. Pour une entité à 2 états :

$$F(t) = 1 - R(t) \quad (1)$$

- le temps moyen avant la première défaillance, noté MTTF (« Mean Time To Failure » en anglais),

$$\mathrm{MTTF} = \int_0^{\infty} \mathrm{R(t)dt} \quad (2)$$

- le taux de défaillance instantané, noté λ(t), qui se définit par (Villemeur,1991) :

$$\lambda(t) = \frac{-\frac{dR(t)}{dt}}{R(t)} \quad (3)$$

Dans la pratique, λ(t) est calculé par (Villemeur,1991):

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{1}{\Delta t} \frac{P\left(\begin{matrix}entité\ soit\ défaillante\ entre\ t\ et\ t+\Delta t \\ et\ non\ défaillante\ sur\ [0;t]\end{matrix}\right)}{P(\ entité\ soit\ non\ défaillante\ sur\ [0;t]\ )} \quad (4)$$

La courbe représentant le taux de défaillance λ(t) a l'allure d'une « baignoire » (Figure 2). Celle-ci permet d'illustrer les 3 périodes de la vie d'un système (Kumamoto & Henley,1996) : la période de déverminage, la période de vie utile et la période de vieillissement.

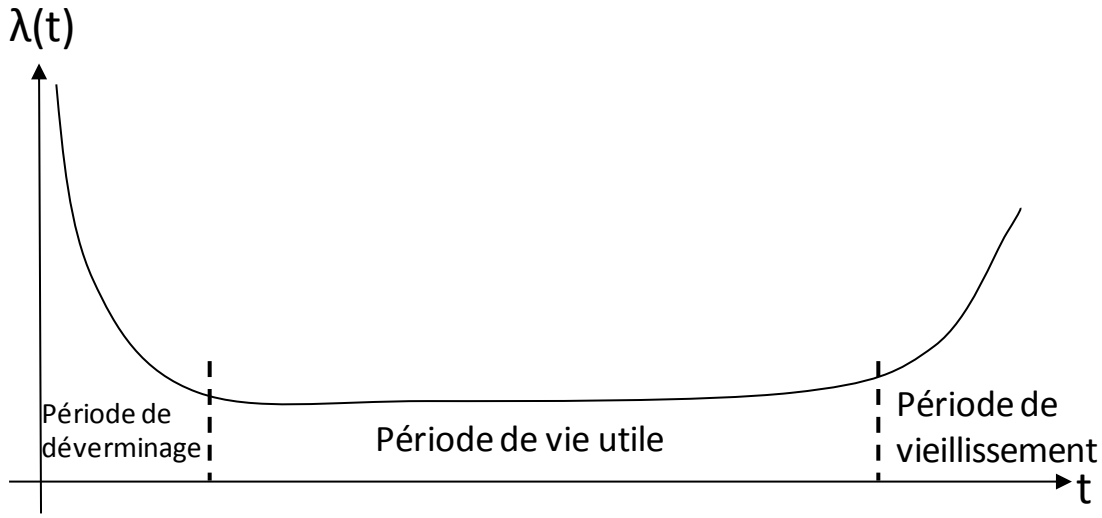


Figure 2 : Evolution du taux de défaillance d'un système.

1.1.3. La maintenabilité

Lorsque l'entité est réparable, elle est caractérisée par sa maintenabilité. La maintenabilité, notée M(t), est l'aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données, avec des procédures et des moyens prescrits. L'entité est en panne au début de l'intervalle (Villemeur,1991).

La maintenabilité est donc liée à la maintenance, qui est "l'ensemble de toutes les actions techniques, administratives et de management durant le cycle de vie d'un bien, destinées à le maintenir ou à le rétablir dans un état dans lequel il peut accomplir la fonction requise" (DIN EN13306,2010).

Il existe plusieurs types de maintenance, qui peuvent être classés en 2 groupes (Zwingelstein,1996) (Procaccia et al.,2011) : avant l'occurrence d'une défaillance (maintenance préventive) ou après l'occurrence d'une défaillance (maintenance corrective) (Figure 3).

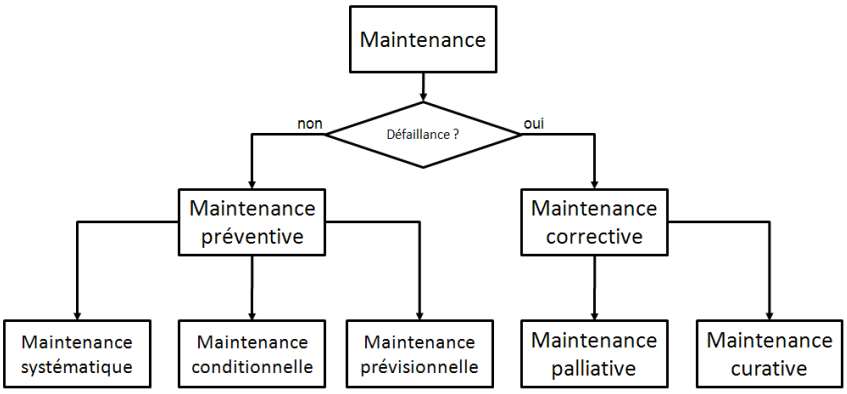


Figure 3 : Classification des types de maintenance (Zwingelstein,1995).

Plusieurs types de maintenance préventive existent ; elles s'appliquent avant l'occurrence d'une défaillance :

- la maintenance systématique, où les actions peuvent être déclenchées en accord avec un calendrier statique préétabli ou en accord avec une durée de fonctionnement (Zwingelstein,1996). Lorsqu'il est possible de déterminer l'état de santé des matériels, deux cas peuvent être distingués:
- la maintenance conditionnelle, qui "comprend une combinaison de surveillance en fonctionnement et/ou d'essai, d'analyse et les actions de maintenance qui en découlent" (DIN EN13306,2010). Cette maintenance est déclenchée lors du franchissement d'un seuil, qui peut être qualifié par une information issue d'une mesure sur le bien (Lavina & Perruche,1998)
- la maintenance prévisionnelle (aussi appelée maintenance prédictive (Lavina & Perruche,1998)), est "exécutée suite à une prévision obtenue grâce à une analyse répétée ou à des caractéristiques connues et à une évaluation des paramètres significatifs de la dégradation du bien" (DIN EN13306,2010).

Après l'occurrence de la défaillance, le matériel défaillant est remplacé (cas d'une entité élémentaire) ou réparé (cas d'un système complexe réparable) (Procaccia et al.,2011). Dans ce cadre :

- la maintenance corrective vise à “remettre un bien dans un état dans lequel il peut accomplir une fonction requise” (DIN EN13306,2010). Il est possible de distinguer parmi les opérations de maintenance corrective :
    - la maintenance palliative (ou maintenance corrective d'urgence) destinée à permettre à un matériel non critique d'accomplir provisoirement tout ou partie d'une fonction requise (Procaccia et al.,2011). Elle correspond aux dépannages provisoires.
    - la maintenance curative (ou maintenance corrective différée), qui vise à "rétablir un bien dans un état spécifié ou à lui permettre d'accomplir une fonction requise" (Zwingelstein,1995). Le résultat des activités doit présenter un caractère permanent et a pour objet de supprimer la (les) défaillance(s).

Chaque type de maintenance correspond à un optimum en vue d'atteindre un niveau de fiabilité et de sûreté tout en minimisant les coûts de maintenance (Zwingelstein,1996).

La maintenabilité peut être directement évaluée par :

- la probabilité, notée M(t), qu'une opération donnée de maintenance puisse être effectuée pendant un intervalle de temps donné, lorsque la maintenance est assurée dans des conditions données et avec l'utilisation des procédures et de moyens prescrits.
- la durée moyenne de réparation, notée MTTR (« Mean Time To Repair » en anglais),
- le taux de réparation instantané, noté μ(t), dont la définition est donnée par (Villemeur,1991):

$$\mu(t) = \frac{\frac{dM(t)}{dt}}{1-M(t)} \quad (5)$$

Dans la pratique, μ(t) est calculé par (Villemeur,1991):

$$\mu(t) = \lim_{\Delta t \to 0} \frac{1}{\Delta t} P\left(\begin{matrix} entité\ soit\ réparée\ entre\ t\ et\ t+\Delta t \\ sachant\ qu'elle\ était\ en\ panne\ sur\ [0;t] \end{matrix}\right) \quad (6)$$

Attribut	Probabilité	Taux instantané	Indicateurs temporels
Fiabilité	$R(t) = e^{-\int_0^t \lambda(x)dx}$	$\lambda(t) = \frac{-\frac{dR(t)}{dt}}{R(t)}$	$MTTF = \int_0^\infty R(t)dt$
Maintenabilité	$M(t) = 1 - e^{-\int_0^t \mu(x)dx}$	$\mu(t) = \frac{\frac{dM(t)}{dt}}{1-M(t)}$	$MTTR = \int_0^\infty [1-M(t)]dt$

Tableau 1 : Attributs de la sûreté de fonctionnement et mesures associées

1.1.4. La disponibilité

L'attribut combinant la fiabilité et la maintenabilité est la disponibilité. La disponibilité, est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné, en supposant que la fourniture des moyens nécessaires est assurée (Villemeur,1991).

Elle peut être mesurée par :

- la probabilité, notée A(t), qu'une entité soit disponible à l'instant t.
- la durée moyenne d'indisponibilité, notée MDT (« Mean Down Time » en anglais).

Pendant la durée moyenne d'indisponibilité (MDT), il est possible de distinguer deux grandes activités : le diagnostic et la réparation (Figure 4). Lorsqu'une défaillance se produit (t_0), un certain temps est nécessaire pour la détecter (de t_0 à t_1). Il s'écoule ensuite des délais techniques et administratifs (de t_1 à t_2 : recherche des pièces détachées, consignation des matériels…) avant de débuter la réparation. A partir du temps t_2, les opérations de maintenance sont réalisées. L'entité est finalement remise en service (de t_3 à t_4). La MDT peut être approximée par :

$$MDT = délai\ de\ découverte + délais\ techniques + MTTR \quad (7)$$

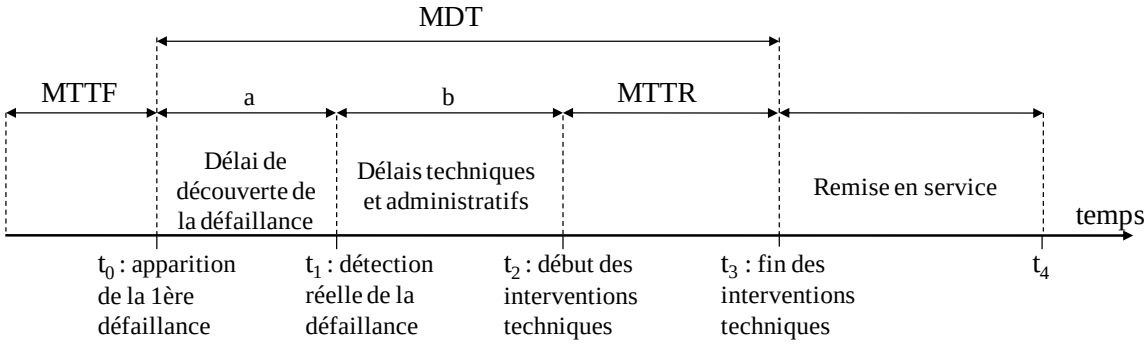


Figure 4 : Chaînage temporel des activités de détection et de remise en service, adapté de (Zwingelstein,1996).

La représentation du MTTR présenté Figure 4 est spécifique à (Zwingelstein,1996). Dans d'autres approches (Kumamoto,2007), la notion de MTTR comprend : 1) le temps pour détecter la défaillance, 2) les délais techniques et administratifs, 3) le temps pour réparer l'entité, 4) le temps de remise en service.

1.1.5. La sécurité

La sécurité est l'aptitude d'une entité à éviter de faire apparaître dans des conditions données, des événements critiques ou catastrophiques (Villemeur,1991). Dans le domaine des systèmes informatiques, la sécurité a trois aspects (Laprie,1995):

- la sécurité-innocuité (en anglais « safety-innocuity »), qui est liée à la non-occurrence de conséquences catastrophiques pour l'environnement,
- la sécurité-confidentialité (en anglais « safety-confidentiality »), qui est liée à la non-occurrence de divulgations non-autorisées de l'information,
- la sécurité-intégrité (en anglais « safety-integrity »), qui est liée à la non-occurrence d'altérations inappropriées de l'information.

1.1.6. Liens entre attributs

Les attributs présentés ci-dessus sont dépendants et leurs effets sur la sûreté de fonctionnement peuvent être synthétisés par la Figure 5. Pour une entité (Ciame,2009) :

- une mauvaise fiabilité peut conduire à une mauvaise disponibilité ou une mauvaise sécurité (lors de nombreuses défaillances),
- une maintenabilité insuffisante (cas des systèmes réparables) peut réduire la disponibilité et la sécurité,
- les contraintes de sécurité peuvent influer négativement sur la disponibilité et inversement.
- un système peut être fiable et maintenable sans être sécuritaire.

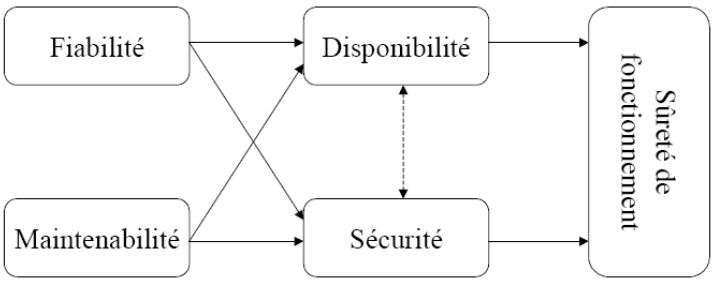


Figure 5 : Relations entre les attributs de la sûreté de fonctionnement (Ciame,2009).

1.1.7. Les moyens

Les objectifs de sûreté de fonctionnement sont atteints par trois moyens (Laprie,1995) :

- L'évitement des fautes, qui passe par la prévention des fautes puis l'élimination des fautes.
- La tolérance aux fautes, qui permet de fournir un service à même de remplir les fonctions du système en dépit des fautes.
- La prévision des fautes, regroupe l'ensemble des méthodes et techniques destinées à estimer la présence, la création et les conséquences des fautes.

1.1.8. Les entraves

Les entraves à la sûreté de fonctionnement sont définies comme les circonstances indésirables, mais non attendues, causes ou résultats de la non-sûreté de fonctionnement (Ciame, 2009). Il est généralement distingué :

- la défaillance, qui est un évènement défini comme la « cessation de l'aptitude d'une entité à accomplir une fonction requise » (DIN EN13306, 2010),
- la faute, qui est la cause supposée d'une erreur (Villemeur, 1991),
- l'erreur, qui est la partie de l'état d'un système qui est susceptible d'entraîner une défaillance (Laprie, 1995). Lorsque l'erreur devient active, une défaillance se produit.

1.2.Mathématiques de la sûreté de fonctionnement

Les statistiques sont utilisées en sûreté de fonctionnement. Des variables aléatoires modélisent les défaillances et réparations des entités. Ces variables aléatoires suivent des lois de probabilité.

1.2.1. Processus de défaillance et processus de réparation

Les défaillances et réparations d'une entité sont caractérisées par des variables aléatoires (Kumamoto & Henley,1996) :

- la défaillance d'une entité est caractérisée par une variable aléatoire, qui représente la durée de fonctionnement de cette entité.
- la réparation d'une entité est caractérisée par une variable aléatoire, qui représente le temps nécessaire pour réparer l'entité.

Les variables aléatoires des durées de fonctionnement et de réparation suivent des lois de probabilité. Les principales lois de probabilité utilisées en sûreté de fonctionnement sont présentées ci-dessous.

1.2.2. Principales lois de probabilité

Parmi les lois de probabilité utilisées en sûreté de fonctionnement, les lois de probabilité discrète ou continue sont distinguées (Tableau 2) :

- les lois de probabilité discrètes sont utilisées, par exemple, lorsqu'il s'agit de quantifier la défaillance à la sollicitation (Lyonnet,2006), qui se produit lorsqu'une entité refuse de changer d'état lorsque cela lui est demandé (Villemeur,1991).
- les lois de probabilité continues sont associées aux variables aléatoires continues, par exemple, lorsqu'il s'agit de quantifier la durée de bon fonctionnement d'une entité (Villemeur,1991).

Type de variable aléatoire	Nom de loi	Application
Discrète	loi binomiale	défaillance à la sollicitation
	loi de Poisson	défaillance à la sollicitation, lorsque le nombre d'expériences est élevé et quand l'espérance mathématique de la variable aléatoire est constante
Continue	loi de Weibull	taux de défaillance décroissant, croissant ou constant
	loi exponentielle	taux de défaillance constant
	loi normale	incertitude liée à des mesures, fabrication
	loi Log-Normale	données de maintenabilité et défaillances dues à la fatigue
	loi gamma	très générale

Tableau 2 : Principales lois de probabilité utilisées en sûreté de fonctionnement

Les caractéristiques détaillées, les tracés des ces lois de probabilité et des méthodes pour estimer les paramètres de ces lois sont présentés en Annexe 1.

1.3.Méthodes usuelles en sûreté de fonctionnement

La littérature (IEC60300-3-1,2003)(Hoyland & Rausand,2004)(Kumamoto,2007)(Ciame,2009) (Cauffriez et al.,2012) distingue un certain nombre de méthodes pour réaliser une étude FMD. Une méthode particulière peut être choisie en fonction des buts de l'étude ou en fonction du type de résultats, qui peut être quantitatif, qualitatif ou combiner les deux aspects (Tableau 3).

Méthode	Quantitative /qualitative	Statique/ dynamique	Objectifs
Analyse Préliminaire des Dangers	Qualitative	Statique	Identification a priori du risque
Analyse des Modes de Défaillance, de leurs effets et de leur Criticité (AMDEC)	Qualitative	Statique	Evaluation des possibles conséquences des défaillances
Arbre de Défaillance	Qualitative/ quantitative	Statique	Evaluation des scénarios d'évènements
Bloc diagramme de Fiabilité (BDF)	Qualitative/ quantitative	Statique	Construction d'un modèle du système basé sur la fiabilité des composants
Arbre d'Evènements	Qualitative/ quantitative	Statique	Evaluation des possibles conséquences d'un évènement
Méthode du Diagramme Cause Conséquence	Qualitative/ quantitative	Statique	Analyse d'un évènement initiateur
Table de vérité	Qualitative	Statique	Analyse de toutes les combinaisons d'état
Graphes de Markov	Qualitative/ quantitative	Dynamique	Identification de l'évolution du système dans les états bon fonctionnement, dégradé, panne
Réseaux de Petri	Qualitative/ quantitative	Dynamique	Identification de l'évolution du système dans les états bon fonctionnement, dégradé, panne
Fiabilité dynamique	Quantitative	Dynamique	Identification de l'évolution du système dans les états bon fonctionnement, dégradé, panne pour les systèmes hybrides
Réseaux Bayésiens dynamiques	Qualitative/ quantitative	Dynamique	Identification de l'évolution du système dans les états bon fonctionnement, dégradé, panne

Tableau 3 : Classification des principales méthodes dans le domaine de la sûreté de fonctionnement (Cauffriez et al.,2012).

Les méthodes statiques se distinguent des méthodes dynamiques. Les méthodes statiques ne prennent pas en compte l'évolution du système dans le temps (Cauffriez et al.,2012). Sept méthodes statiques sont utilisées (Tableau 3):

- L'Analyse préliminaire des dangers permet d'identifier et évaluer les dangers inhérents à un système. Elle peut être considérée comme une étape préliminaire à toute analyse de sûreté de fonctionnement supplémentaire (Villemeur,1991).
- L'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC) vise à identifier les modes de défaillance, les causes et les effets des défaillances des composants du système (Villemeur,1991).
- L'Arbre de Défaillance (Lyonnet,2006) permet de représenter graphiquement les causes d'un événement indésirable (c'est-à-dire une défaillance redoutée). Le processus déductif est poursuivi jusqu'à déterminer les évènements de base, auxquels il est possible d'associer une probabilité (Pagès & Gondran,1980).

- La Méthode du Bloc Diagramme de Fiabilité conduit à un diagramme logique représentant le fonctionnement du système, où chaque entité est modélisée par un bloc. Le diagramme obtenu permet de calculer la fiabilité d'un système non réparable (Villemeur,1991).
- L'Arbre d'Evénements est une méthode graphique inductive qui vise à identifier et évaluer les conséquences d'un événement initiateur (i.e. une défaillance) (Villemeur,1991).
- La Méthode de la Table de Vérité consiste à analyser systématiquement les combinaisons d'états (bon fonctionnement ou panne) de chaque composant et des effets qui s'ensuivent. Le résultat est présenté sous forme de tableau, permettant d'exprimer l'état du système en fonction de l'état de ses composants, pour chaque combinaison d'état des composants.

Les méthodes dynamiques intègrent l'évolution dynamique du système mais sont souvent limitées par le nombre d'états (Cauffriez et al.,2012). Sont habituellement distinguées (Tableau 3):

- Les graphes de Markov, qui s'appliquent aussi aux systèmes (réparables ou non réparables) qui suivent un processus markovien homogène (Lyonnet,2006). Cette méthode permet d'identifier les états (bon fonctionnement ou panne) et les transitions entre les états recensés, puis les probabilités que le système soit dans les différents états.
- La fiabilité dynamique, qui offre un cadre pour l'évaluation des systèmes hybrides, c'est-à-dire les systèmes dont la sureté de fonctionnement peut dépendre d'évènements aléatoires mais aussi de variables physiques (par exemple le niveau d'eau d'un réservoir) (Cabarbaye & Laulheret,2005) (Broy et al.,2011). Les problèmes de fiabilité dynamique nécessitent d'être résolus par des techniques numériques. Cependant, des difficultés peuvent être rencontrées, car le nombre d'états (et potentiellement le nombre de transitions) est important (Barger,2003).
- Les Réseaux Bayesiens dynamiques, qui permettent de calculer la fiabilité et la disponibilité d'un système après avoir établi les liens de cause à effet entre les évènements du système (Weber et.,2012). Deux approches existent : l'approche "time-sliced" et l'approche "event based". L'approche "time-sliced" est très générale. Elle est pilotée par une analyse dynamique et rend le Réseau Bayésien plus complexe, car les nœuds sont répétés pour chaque intervalle de temps. L'approche "event based" ne traite que les systèmes non réparables, car cette approche admet que chaque évènement n'a lieu qu'une fois (Boudali & Dugan,2005).

Dans la partie suivante sont rappelées les notions de base sur le diagnostic et les architectures du diagnostic.

2. Diagnostic

La première section rappelle des notions d'ordre général sur la surveillance et le diagnostic. La deuxième section présente les méthodes utilisées pour le diagnostic. La troisième section présente les architectures de diagnostic habituelles, qui constituent le point de départ de nos travaux de recherche.

2.1.Surveillance, diagnostic et gestion de fautes

Les performances des systèmes peuvent être altérées par l'occurrence de défaillances soudaines ou progressives, qui peuvent causer des dégâts sérieux au système. Pour prévenir la détérioration de ces

systèmes, une solution consiste à ajouter des systèmes de diagnostic (Aubrun et al.,2008). Le diagnostic est en fait composé de deux tâches essentielles : la surveillance et le diagnostic (Ribot,2009). Une fois que le diagnostic est établi, la réaction appropriée est mise en œuvre, ce qui correspond à la gestion de la faute (Figure 6).

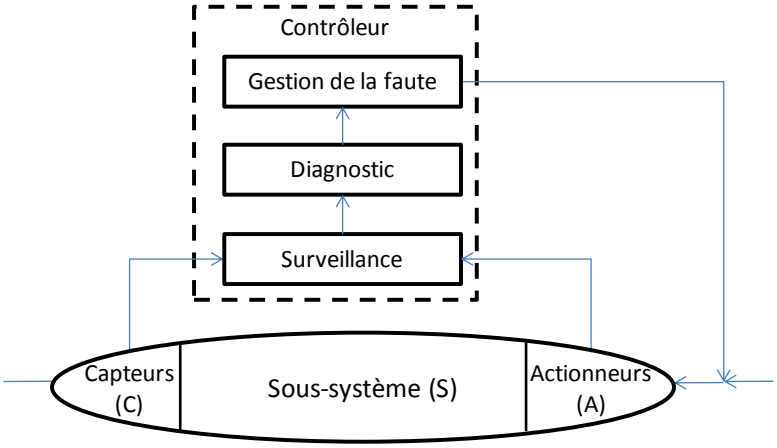


Figure 6 : La détection, le diagnostic et la gestion de fautes (adapté de Isermann,2006)

- La surveillance

Afin de déterminer si un sous-système remplit correctement ses objectifs, celui-ci est surveillé de manière précise à l'aide de capteurs positionnés stratégiquement (Figure 6). La fonction de surveillance consiste alors à détecter le passage du sous-système en fonctionnement anormal (Agudelo et al.,2013). Elle récupère les informations issues des capteurs et les transforme en indicateurs de défaillance illustrant le fonctionnement normal ou anormal du sous-système. Lorsqu'un indicateur franchit un seuil prédéterminé, une alarme est déclenchée (Ribot,2009).

- Le diagnostic

L'objectif du diagnostic est d'identifier la cause probable de la (ou des) défaillance(s) (NF ISO13372,2005) (Feldman,2010), à l'aide d'un raisonnement logique fondé sur un ensemble d'informations provenant d'une inspection, d'un contrôle ou d'un test (Zwingelstein,1995). Un des objectifs du diagnostic est qu'il soit minimal (Aubrun et al.,2010), c'est-à-dire un diagnostic qui ne contient pas d'autres diagnostics et qui est le plus petit possible en taille (Metodi et al.,2012). Plusieurs méthodes pour diagnostiquer les fautes sont présentées à la section suivante (Zwingelstein,1995) (Dubuisson,2001).

- La gestion de fautes

En fonction du niveau de danger de la faute diagnostiquée sur le sous-système, plusieurs types de réactions peuvent être mis en œuvre (Isermann,2006):

1. L'exploitation sûre ; ce qui signifie l'arrêt en cas de danger imminent pour le processus ou l'environnement.
2. L'exploitation fiable ; par exemple en "masquant" l'extension de la faute. Pour ce faire, l'exploitation peut continuer, mais en baissant la charge ou la vitesse.

3. La reconfiguration ; en utilisant par exemple des composants redondants (capteurs, actionneurs…) pour garder le processus sous contrôle.
4. L'inspection ; qui consiste à réaliser un diagnostic détaillé par des mesures additionnelles (sur le processus)
5. La réparation ; (instantanément ou dès que possible) afin d'éliminer la faute.

Par la suite, nous qualifions de "non-intrusive" une réaction (à la suite d'une faute) dont la mise en œuvre n'implique aucune action sur le processus. La réaction (à la suite d'une faute) est non-intrusive dans le sens où le processus n'est pas arrêté ou désactivé. L'inspection, telle qu'elle est définie ci-dessus, entre dans ce cadre. Ce type de réaction diffère d'autres types de réactions, où la partie défaillante peut être arrêtée ou désactivée, lors de l'occurrence d'une faute (Amari et al.,2008).

2.2.Méthodes de diagnostic

Le choix d'une méthode de diagnostic dépend surtout de la connaissance disponible sur le système. Les méthodes de diagnostic peuvent être classées en trois catégories (Ribot,2009) : les méthodes basées sur la connaissance, les méthodes basées sur le traitement de données et les méthodes à base de modèle.

- **Les méthodes basées sur la connaissance** reposent sur une connaissance explicite des relations causales entre les symptômes, les défaillances et les fautes. Cette connaissance est acquise pendant la phase de conception du système et peut provenir d'une analyse fonctionnelle (Ribot,2009). Parmi ces méthodes, il est possible de distinguer les systèmes experts, l'analyse des modes de défaillance et de leurs effets ou l'arbre de défaillances (Venkatasubramanian et al.,2003). A noter que ces deux dernières méthodes sont empruntées au domaine de la sûreté de fonctionnement.
- **Les méthodes basées sur le traitement de données** reposent uniquement sur les informations issues des capteurs du système. Ces méthodes font appel à la reconnaissance de formes, dont l'objectif est d'associer toute nouvelle donnée à une classe déterminée par la méthode d'apprentissage (Dubuisson,2001).
- **Les méthodes à base de modèle** reposent sur une connaissance physique profonde du système à diagnostiquer. Le système est représenté sous forme de modèles, représentant sa structure et son comportement nominal. La méthode consiste ensuite à comparer le comportement réel (observé sur le système physique) avec le comportement prédit (à l'aide de modèles) (Isermann,2006). Les deux principales approches sont :
    - **l'approche FDI** (de l'anglais "Fault Detection and Isolation", issue de la communauté automatique), qui utilise des modèles quantitatifs (équations différentielles) pour décrire le système (Aubrun et al.,2010).
    - **l'approche DX** (issue de la communauté de l'intelligence artificielle (Cordier et al.,2004)), qui est fondée sur une théorie logique du diagnostic. Cette approche utilise des modèles qualitatifs pour représenter les interactions entre composants du système (Calderon Espinoza,2003).

Dans la pratique, les fonctions de détection, de diagnostic et de gestion de la faute peuvent être réalisées automatiquement par un contrôleur (Figure 6). De même, un système de diagnostic peut être implémenté en plusieurs types d'architectures, qu'il convient de présenter.

2.3.Architectures de diagnostic

Par la suite, nous utiliserons le terme "architecture" pour faire référence à un ensemble fini de systèmes en interaction. De même, le terme "architecture de diagnostic" fait référence à un processus en interaction avec des systèmes de diagnostic. La littérature distingue différents types d'architectures de diagnostic (Hallgren & Skog,2005) (Dievart,2010) (Koutsoukos et al.,2010). Dans ces types d'architecture, les notions de "diagnostic local" et de "diagnostic global" sont utilisées.

2.3.1. Diagnostic local et diagnostic global

Deux notions doivent être définies avant de présenter les différents types d'architecture :

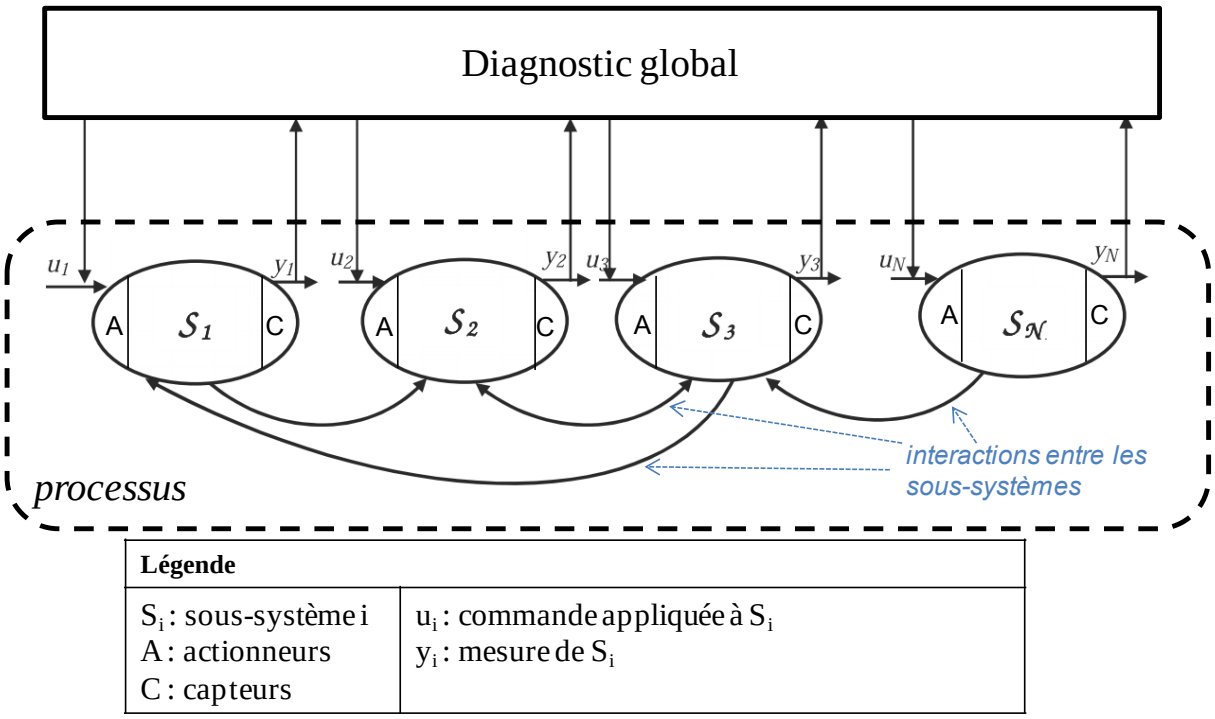
- Le diagnostic local, qui est associé à un sous-système. Le diagnostic local est principalement basé sur des observations (par exemple, les informations des capteurs) du sous-système (Su et al.,2002) et éventuellement un modèle, lorsqu'une méthode à base de modèles est utilisée.
- Le diagnostic global, qui est un diagnostic pour le processus complet (c'est-à-dire le processus soumis au diagnostic). Le diagnostic global est établi à partir des diagnostics locaux (Biteus et al.,2011).

Ces notions de diagnostic local et de diagnostic global permettent d'expliquer le fonctionnement des architectures de diagnostic.

2.3.2. Architecture centralisée

Dans le cas d'une architecture centralisée (Figure 7), un seul diagnostic global dispose d'une vue globale sur le processus (Dievart,2010), partitionné en sous-systèmes, notés S_i. Il réalise un diagnostic global à partir des données de tous les capteurs (et éventuellement des actionneurs). Cette architecture a plusieurs défauts (Dievart,2010):

- la vitesse de réponse, qui diminue lorsque la taille du système augmente,
- le système est peu robuste, car il est sensible aux fautes du diagnostic global.

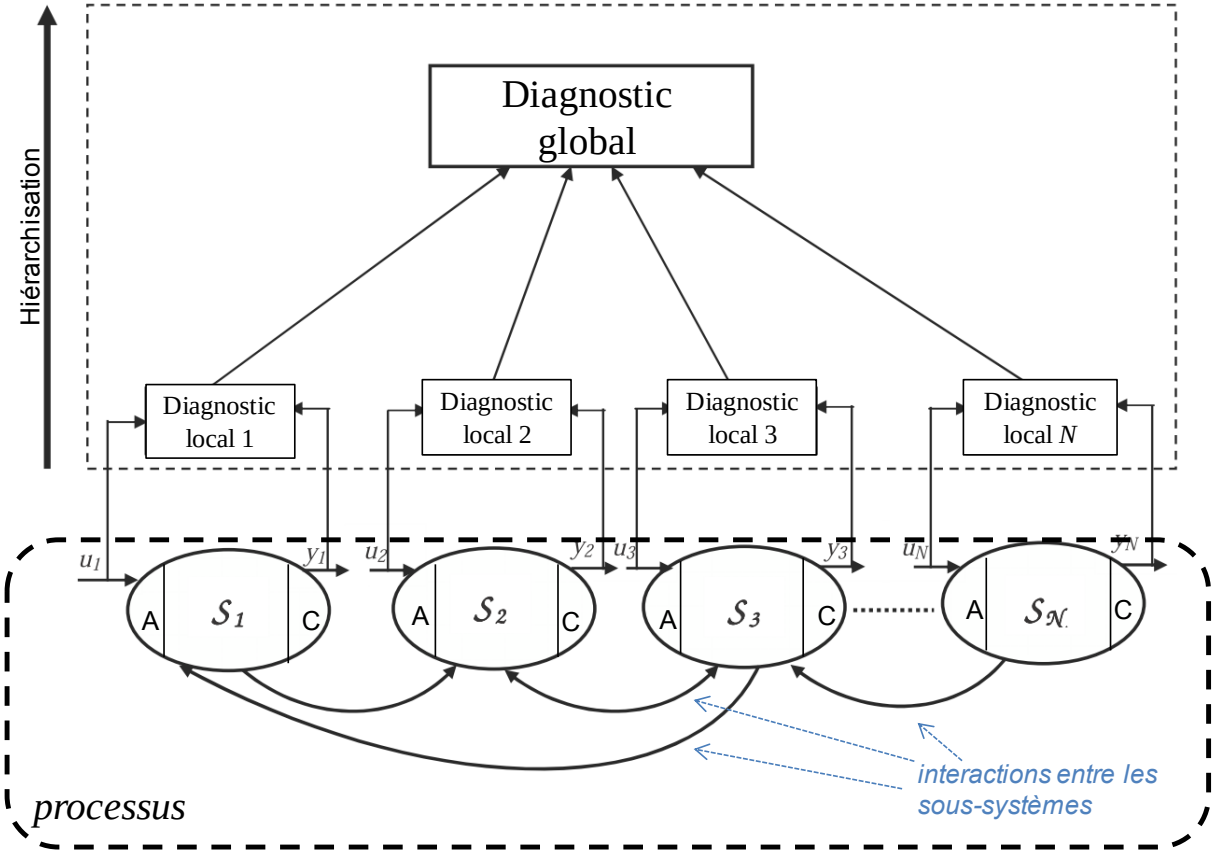


Légende	
S_i : sous-système i A : actionneurs C : capteurs	u_i : commande appliquée à S_i y_i : mesure de S_i

Figure 7 : Architecture de diagnostic centralisée, adapté de (Menighed,2010)

Dans la pratique, l'architecture centralisée peut être implémentée sous forme hiérarchique. Il s'agit alors d'une architecture centralisée hierarchisée.

L'approche centralisée hiérarchisée (Figure 8) est composée de plusieurs niveaux (Koutsoukos et al.,2010). Les diagnostics locaux lisent les données des capteurs (et éventuellement des actionneurs) provenant des sous-systèmes S_i, réalisent un diagnostic et calculent des indicateurs. Le partitionnement des diagnostics peut être réalisé suivant une décomposition spatiale ou suivant une décomposition sémantique (Roos et al.,2003). Une tâche principale consiste ensuite à réaliser un diagnostic global à partir des diagnostics locaux et de résoudre les ambiguïtés.



Légende	
S_i : sous-système i A : actionneurs C : capteurs	u_i : commande appliquée à S_i y_i : mesure de S_i

Figure 8 : Architecture de diagnostic centralisée hiérarchisée, adapté de (Menighed,2010)

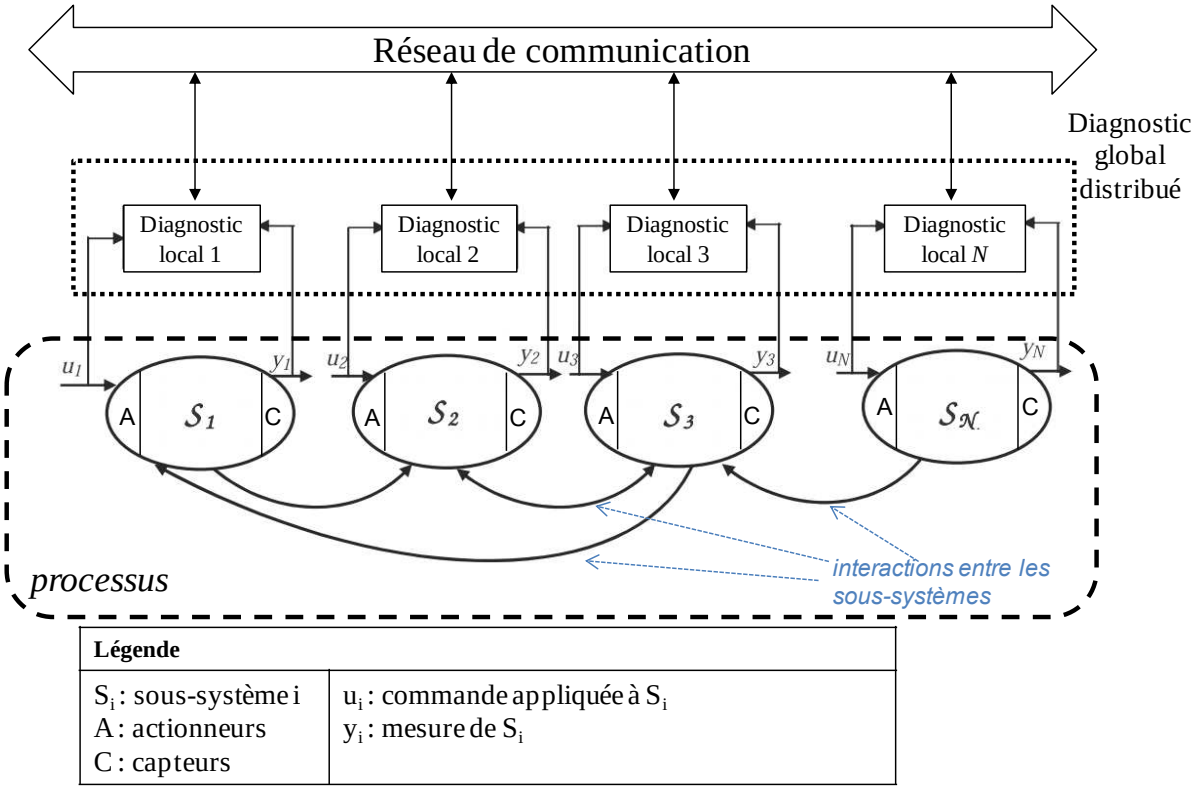
Cette approche a plusieurs inconvénients (Dievart,2010):

- Le partage des informations entre diagnostic de même niveau crée des problèmes.
- Le problème d'évolutivité : pour effectuer des modifications de structure, il faut " *refondre tout le système et mettre à jour les structures de plus haut niveau dans l'architecture* " (Dievart,2010).

L'architecture distribuée a été proposée pour contourner les inconvénients des approches centralisées.

2.3.3. Architecture distribuée

L'architecture distribuée (Figure 9) se base sur un ensemble de diagnostic locaux (Su et al.,2002). Chaque sous-système S_i a son diagnostic local, qui lui est dédié. Chaque diagnostic local est connecté aux autres diagnostics locaux par un réseau de communication. Le diagnostic local est principalement basé sur ses observations locales et la communication n'est utilisée que pour affiner le diagnostic. Le diagnostic global est distribué et est établi à partir des diagnostics locaux (Biteus et al.,2011).



Légende	
S_i : sous-système i A : actionneurs C : capteurs	u_i : commande appliquée à S_i y_i : mesure de S_i

Figure 9 : Architecture de diagnostic distribuée, adapté de (Menighed,2010)

Cette architecture a été imaginée pour contourner les difficultés liées à l'architecture hiérarchisée mais pose une nouvelle problématique, liée à la présence d'un réseau de communication.

2.3.4. Problématique de conception d'architectures de diagnostic distribué

La problématique de conception d'architectures de diagnostic distribué est similaire à celle trouvée dans d'autres domaines comme les systèmes d'automatisation à intelligence distribuée (Barger,2003). Les systèmes d'automatisation à intelligence distribuée mettent en œuvre des capteurs dits "intelligents"; la notion d'intelligence faisant référence à une architecture matérielle, qui repose sur (Ciame,2009) :

- des moyens de traitement permettant la réalisation des fonctions attendues,
- des moyens de mémorisation pour les informations de conduite, de maintenance, de gestion technique,
- des moyens de communication avec l'ensemble du système d'automatisation, pour assurer la diffusion des informations élaborées localement et recevoir les données utiles à ses actions (provenant d'un opérateur ou d'autres composants par exemple).

Les bénéfices attendus des capteurs intelligents par rapport aux systèmes traditionnels avec une connexion câblée point à point sont : la réduction du câblage (Claesson,2002), la correction d'erreur de mesure (Smith & Bowen,1995), l'autodiagnostic et validation de la mesure (Staroswiecki,2005), la reconfiguration en ligne... La connexion à un réseau de communication permet également plus de flexibilité pour la maintenance (Aubrun et al.,2008). Un technicien se connectant au réseau peut rapidement observer l'état de l'ensemble des capteurs/actionneurs connectés.

Cependant, l'aspect innovant de la conception, l'utilisation des nouvelles technologies (capteurs intelligents) et l'utilisation d'un système de communication rendent l'architecture plus complexe (Ciame,2009)(Brissaud et al.,2010). Or, la complexité est synonyme de faiblesse (Nicolet et al.,1990). (Laprie,1995) précise qu'il existe une corrélation entre la complexité d'un produit et le nombre de fautes. Les objectifs de sûreté de fonctionnement sont donc plus difficiles à atteindre et la démonstration de sûreté de fonctionnement est plus complexe (Cauffriez et al. 2004) (Brissaud et al.,2010). Trois facteurs, qui influent sur la complexité, peuvent être identifiés dans une architecture de diagnostic distribué (Benard et al.,2008):

- complexité de taille : une architecture de diagnostic distribué est composée de nombreux éléments : sous-systèmes, capteurs, actionneurs, contrôleurs (pour le diagnostic) et réseau de communication. Plus le nombre de composants augmente (la taille augmente), plus la complexité de l'architecture augmente.
- complexité stochastique : le fonctionnement et le dysfonctionnement des composants de l'architecture de diagnostic distribué est caractérisé par des variables aléatoires ; le comportement résultant (le comportement stochastique de l'architecture de diagnostic distribué) est difficile à analyser
- complexité fonctionnelle : l'architecture de diagnostic utilise de nombreuses fonctions ; toutes les fonctions ne sont pas identiques et certaines sont rétromettantes.

D'un point de vue sûreté de fonctionnement, il est nécessaire d'insister sur la présence du réseau de communication. En effet, (Ghostine et al.,2006) (Koutsoukos et al.,2010) (Thiriet,2004) soulignent que le réseau ne doit pas seulement être considéré comme un sous système individuel mais comme un élément central, dont la défaillance peut affecter la mission globale du système. Un réseau de communication est un système à part entière, caractérisé par des modes de défaillances qui lui sont propres (Papadopoulos et al.,2006). D'autant plus que les réseaux de communication peuvent fonctionner dans un environnement extrême (poussière, vibrations, température…) (Wahl, et al., .2010) (FprEN50159,2010). Pour ces raisons, les réseaux de communication doivent être pris en compte. Les travaux de la littérature sur ces différents éléments vont maintenant être présentés.

3. Travaux sur l'évaluation de FMD des architectures de diagnostic

Les travaux existants sur l'évaluation de FMD d'architectures de diagnostic, peuvent être divisés en deux catégories :

- d'une part, les travaux sur l'évaluation FMD de systèmes distribués, appliqués à plusieurs domaines, dont le diagnostic,
- d'autre part, des travaux sur l'évaluation de FMD du diagnostic.

Les travaux recensés vont maintenant être présentés.

3.1. Travaux sur l'évaluation de FMD des systèmes distribués

Un réseau de communication présente plusieurs modes de défaillance (Papadopoulos et al.,2006) (FprEN50159,2010). Pour modéliser les modes de défaillances, deux grandes approches existent dans la littérature des systèmes distribués (Barger,2003) :

1 les approches systèmes, qui établissent le modèle complet du système distribué y compris le réseau de communication,
2 les approches centrées réseau, qui ne modélisent que le réseau de communication.

Cette section commence par détailler les approches systèmes, puis introduit les approches centrées réseau.

3.1.1. Approches systèmes

Dans (Vannier & Dersin,2006), les auteurs proposent un modèle pour l'évaluation de FMD de l'architecture distribuée d'un système de signalisation, utilisant des réseaux de communication câblés et des réseaux de communication sans fil. L'étude se décompose en deux parties. Une étude qualitative par AMDEC est d'abord réalisée afin de comprendre les états de marche et de panne du système et d'analyser les modes de défaillance et leurs effets. Une étude quantitative est ensuite réalisée en deux étapes. Les taux de défaillance du réseau de communication sont estimés à partir de l'architecture du système, qui est modélisée sous forme de bloc diagrammes de fiabilité. Puis, une modélisation par graphes de Markov est réalisée pour évaluer la disponibilité du réseau de communication.

(Galdun et al.,2008) évaluent plusieurs architectures distribuées de commande d'un mini-hélicoptère commandé en réseau. Les auteurs étudient l'influence de la fiabilité de composants en redondance partagée sur la fiabilité du système étudié. Ce type de redondance, qui diffère des types de redondances classiques (redondance active, redondance passive), est caractérisé par des composants qui ne sont pas redondants (dans un premier temps), mais qui sont capables de changer de mission en cas d'urgence (Wysocki et al.,2004). Lorsqu'un composant défaillant réalise plusieurs missions, le temps d'éxécution s'allonge et provoque un retard, qui peut déstabiliser le système. En supposant que le retard peut être compensé, le composant ne défaille pas immédiatement mais la fiabilité est réduite et modélisée par un facteur de réduction. Les architectures redondantes sont modélisées par Réseaux de Petri. La simulation de Monte Carlo permet d'obtenir et de comparer la fiabilité instantannée de chaque architecture.

(Aza-Vallina et al.,2011) présente une nouvelle méthode pour obtenir l'expression analytique de la fiabilité de transmission de données entre deux nœuds (capteurs, actionneurs, contrôleurs…) d'un système en réseau. Les composants sont supposés pouvoir défaillir de plusieurs manières : bavardage intempestif, défaillance silencieuse (de l'anglais "fail-silent") et défaillance se propageant aux nœuds adjacents. L'expression analytique de la fiabilité de chaque nœud est d'abord obtenue en modélisant les modes de défaillance retenus par graphes de markov. La fiabilité de la transmission est ensuite exprimée en analysant les combinaisons des états de tous les composants (nœuds et liens) et en ne retenant que les combinaisons d'états permis. L'originalité de cette approche est de prendre en compte les défaillances de propagation, où la défaillance d'un composant peut empêcher les composants adjacents de communiquer, même si l'autre n'est pas défaillant.

(Claesson,2002) vise la conception d'un système de commande distribué. Pour ce faire, plusieurs architectures (centralisées, décentralisées, distribuées) sont choisies. Le réseau de communication est supposé être un réseau de diffusion. Les échanges d'information sont chiffrés, afin de connaître la bande passante nécessaire dans le pire des cas pour réaliser la fonction critique. La modélisation par graphes de Markov permet alors d'obtenir l'expression analytique de la fiabilité des nœuds complexes (par exemple les nœuds en redondance active). L'expression de la fiabilité d'une

architecture est ensuite obtenue en réalisant des combinaisons séries/parallèle. Le taux de défaillance du bus est quantifié à partir du taux de défaillance des connecteurs.

3.1.2. Approches centrées réseau

(Barger,2003) étudie les systèmes à réseaux, composés de capteurs et actionneurs intelligents organisés autour d'un réseau de communication. Chaque composant est modélisé en Réseaux de Petri colorés avec un grand niveau de détail (algorithme de commande du régulateur, tampons d'émission sur le réseau…). En sortie, le modèle proposé permet d'obtenir par simulation la fiabilité ainsi que les variables continues du processus (par exemple, le niveau d'eau d'un réservoir). La démarche permet également d'estimer *" le taux de défaillance du système global sous les conditions que les modes de fonctionnement et des taux de défaillance des composants soient connus a priori "* (Barger,2003).

Dans (Navet et al.,2000), les auteurs prennent en compte les erreurs de transmission pour la conception de systèmes embarqués distribués. Le concept de " probabilité de pire temps de réponse des messages ", noté WCDFP (de l'anglais " worst-case deadline failure probability ") est étudié sur un réseau CAN. Le WCDFP est en fait un indicateur de sûreté de fonctionnement, qui peut aider le concepteur à fixer les périodes et priorités des messages. Pour évaluer le WCDFP, une méthode est proposée pour identifier le seuil sous lequel le temps de réponse du pire cas est satisfait. De plus un modèle d'erreur flexible, suivant un processus généralisé de Poisson est proposé.

(Zimmermann & Hommel,2005) étudie un système de télécommunication ferroviaire, composé d'équipements fixes (au sol) et d'équipements mobiles (à bord du train). Un modèle comportemental du système de télécommunication, basé sur les Réseaux de Petri stochastiques, est d'abord proposé. Celui-ci se concentre sur les erreurs de transmission, les pertes de connexion et les transferts intercellulaires. Le modèle est ensuite simplifié par le biais d'une analyse numérique. Enfin, celui-ci est intégré à un modèle d'échange d'informations avec le sol. En sortie, les résultats du modèle illustrent l'influence de la fiabilité du système de communication sur l'exploitation du train.

Pour le domaine spécifique du ferroviaire, la norme (FprEN50159,2010) spécifie les exigences pour les systèmes de communication pour la sécurité entre des systèmes de sécurité pour obtenir le niveau de SIL requis. La norme propose un modèle binaire pour un système de transmission de données, à base de graphe de Markov. Trois modes de défaillances sont modélisés : la défaillance du matériel de transmission, l'erreur bit et l'occurrence d'une faute sur le code de sécurité.

3.2.Travaux sur l'évaluation de FMD du diagnostic

Les travaux de la littérature sur l'évaluation FMD du diagnostic vont maintenant être présentés. La première sous-section présente les modes de défaillance d'un système de diagnostic, tandis que la seconde sous-section présente l'utilisation de ces modes de défaillance dans la littérature.

3.2.1. Modes de défaillance d'un système de diagnostic

Les systèmes de diagnostic peuvent être caractérisés par plusieurs propriétés, telles que :

- la détectabilité (Nyberg,2002), qui caractérise, dans le cas de l'approche FDI, la possibilité de concevoir un générateur de résidus sensible à une défaillance découplée des perturbations.

- la robustesse (Patton,1997), dont l'objectif est de maximiser la détectabilité tout en minimisant les effets des incertitudes et des perturbations lors de la réalisation du diagnostic.

D'un point de vue sûreté de fonctionnement, ces propriétés sont habituellement étudiées par l'intermédiaire de deux modes de défaillance (Kumamoto,2007):

- la fausse alarme (de l'anglais "false alarm"): le système de diagnostic génère une alarme ou un diagnostic alors que le processus est dans l'état de bon fonctionnement
- l'absence d'alarme (de l'anglais "inactive alarm") : le système de diagnostic ne génère pas d'alarme ni de diagnostic alors que le processus est dans l'état de panne.

En fonction des hypothèses de l'étude FMD, l'occurrence de ces évènements peut conduire à l'état de panne ou de fonctionnement dégradé du système de diagnostic lui-même, ou du système de diagnostic ainsi que du processus.

3.2.2. Travaux sur l'évaluation de FMD du diagnostic

(Dersin & Péronne,2007) étudie l'influence de la testabilité sur la fiabilité de systèmes en redondance active. Pour ce faire, les systèmes redondants sont modélisés par graphes de Markov, ce qui permet d'obtenir l'expression asymptotique de la fiabilité en fonction de la couverture du diagnostic. Une comparaison de politiques de maintenance est finalement proposée à partir de la fiabilité atteinte et du coût global.

Dans (Volovoi,2012), un composant à un mode de défaillance est couplé à un système de diagnostic. Les fausses alarmes et l'absence de détection sont modélisés par des états à part entière dans un graphe de Markov. Pour plus de flexibilité, une seconde modélisation à base de Réseaux de Petri colorés est ensuite réalisée. Plusieurs alternatives sont comparées grâce aux résultats en sortie : nombre de défaillances, nombre de réparations et coût.

(Myers & Rauzy,2008) étudient la couverture, c'est-à-dire la capacité d'un système à isoler et confiner les défaillances des systèmes redondants. L'expression analytique de la couverture est exprimée dans le cas de systèmes m parmi n. L'expression est ensuite implémentée dans des arbres de décision binaire. Au final, la défiabilité est calculée sur un cas industriel.

3.3.Synthèse

La revue des travaux réalisés sur les systèmes distribués et les systèmes de diagnostic a permis d'observer que :

- les systèmes de diagnostic sont des systèmes dynamiques et des systèmes à états. Un système de diagnostic peut évoluer dans des états de bon fonctionnement, de défaillance détectée ou de défaillance non détectée. De même, il peut être réparé après une défaillance.
- les architectures de diagnostic hiérarchisé et les architectures de diagnostic distribué mettent en évidence n couples ($n \in \mathbb{N}^*$) "sous-système et système de diagnostic local" qui peuvent être soit dépendants, soit indépendants.
- pour des raisons économiques ou techniques, les n couples du système distribué peuvent être amenés à partager des ressources communes (réseau de communication, équipe de réparateurs, calculateur central, base de données…) (Herzog,2002).

- Les méthodes de sûreté de fonctionnement utilisées pour évaluer la FMD des systèmes sous diagnostic et les systèmes d'automatisation à intelligence distribuée sont essentiellement des méthodes dynamiques : les chaînes de Markov ou les Réseaux de Petri.

Conclusion

Ce chapitre a d'abord permis de présenter la FMD, qui fait partie de la sûreté de fonctionnement, et les méthodes de la littérature pour réaliser une évaluation FMD. Les notions de base sur le diagnostic et les architectures de diagnostic, qui constituent un point de départ de cette thèse, ont ensuite été rappelées. Enfin, quelques travaux sur l'évaluation des architectures de diagnostic ont été présentés. Les travaux recensés peuvent être classés en deux catégories : les travaux sur le diagnostic d'une part et les travaux sur les systèmes distribués d'autre part.

Maintenant que les principales notions théoriques ont été abordées, le chapitre suivant détaille la problématique de thèse.

Chapitre 2 : Optimisation de la maintenance par l'amélioration du diagnostic

Chapitre 2 : Optimisation de la maintenance par l'amélioration du diagnostic

Introduction

Le premier chapitre a permis de présenter les notions de base en sûreté de fonctionnement, les architectures de diagnostic de la littérature et quelques travaux réalisés sur les architectures de diagnostic. La partie 1 introduit le contexte général et les objectifs de cette thèse, à savoir l'évaluation d'architectures de diagnostic dans le transport ferroviaire. La partie 2 présente les architectures de diagnostic existantes dans le transport ferroviaire. La partie 3 présente, dans le contexte des architectures de diagnostic pour le transport ferroviaire, la situation actuelle et ses limites ainsi que les solutions envisagées. La partie 4 détaille la problématique d'évaluation d'architectures de diagnostic dans le transport ferroviaire. Enfin, la partie 5 présente les verrous scientifiques identifiés en termes de systèmes distribués, de diagnostic et de sûreté de fonctionnement.

1. Contexte général et objectifs

Dans le transport ferroviaire, le coût global de possession du matériel roulant constitue un facteur de compétitivité important (CCE,2004). En effet, la mise en concurrence pousse de plus en plus les exploitants à vouloir acquérir des matériels roulants en prenant en compte le coût global de possession LCC (de l'anglais « Life Cycle Cost »), incluant le coût de maintenance pendant la vie du matériel roulant (Schweiger,2009). A ce titre, il existe une demande forte en maintenance plus efficace et moins coûteuse, au lieu du modèle historique de maintenance préventive organisée sur le territoire national.

Les constructeurs de matériel ferroviaire sont concernés en premier lieu par ces fortes exigences sur l'optimisation de la maintenance. Pour le constructeur de matériel ferroviaire, la spécification, la conception et le développement de systèmes de transport de plus en plus complexe prenant en compte ces exigences, est un défi. En effet, la conception d'un train doit prendre en compte les spécifications fonctionnelles tout en réduisant le LCC (Dersin,2009) mais aussi les exigences de FMD (Fiabilité, Maintenabilité, Disponibilité). Pour optimiser la maintenance, une approche consiste à améliorer le diagnostic (Marquez et al.,2008)(Utne et al.,2012). Dans ce cadre, Bombardier Transport conduit actuellement plusieurs projets de recherche (Cauffriez et al.,2013)(Bombardier,2010) (Gandibleux et al.,2011). Cette thèse est réalisée dans le cadre du projet SURFER (pour SURveillance active FERroviaire) financé par le FUI (Fonds Unique Interministériel), qui vise le développement d'une architecture de diagnostic efficace (ISO13374-1,2003) pour optimiser la maintenance. Un train est considéré comme un système complexe, composé d'un ensemble de systèmes en interaction, appelés "systèmes élémentaires" (par exemple, les portes, les freins…). L'objectif de SURFER, conduit par Bombardier Transport, est de développer quatre points relatifs :

- Lors de défaillances progressives, le diagnostic prédictif doit permettre d'anticiper les défaillances sur les systèmes élémentaires pouvant affecter la mission du train, permettant aux équipes de maintenance de préparer une intervention anticipée.
- Lors de défaillances avérées sur les systèmes élémentaires, le diagnostic curatif doit permettre de mieux les localiser géographiquement et temporellement, permettant de diminuer le temps d'immobilisation ou d'intervention.
- La surveillance continue et la traçabilité des évènements (défaillances bénignes, défaillances graves, réparations…) doit permettre de comptabiliser les états du système élémentaire sur le long terme. Ces données doivent alimenter les bases de retour d'expérience afin de consolider les futurs modèles de fiabilité prévisionnelle.
- Le retour d'expérience doit permettre d'obtenir les lois de dégradation des composants des systèmes élémentaires, afin d'optimiser dynamiquement les plans de maintenance en prenant en compte l'état du système élémentaire, pour une flotte entière.

Le développement de cette nouvelle architecture de diagnostic offre de nouvelles possibilités mais engendre cependant de nouvelles contraintes notamment en matière de sûreté de fonctionnement. La complexité induite par l'intégration des systèmes intelligents rend difficile la quantification du niveau de sûreté de fonctionnement.

Selon le principe GAMAB (Globalement Au Moins Aussi Bon) présenté en introduction, l'architecture de diagnostic développée doit être non-intrusive. Cette exigence de non-intrusivité du système de diagnostic se justifie par la défaillance en exploitation de ce dernier, dont l'occurrence peut conduire à des évènements redoutés de gravité significative. L'occurrence d'une défaillance sur un train retarde dans sa mission non seulement le train défaillant (desserte des stations) mais propage également un retard sur tous les trains suivants de la ligne (Corman, D'Ariano, & Hansen,2012). De plus, l'augmentation du trafic voyageur en Europe ces dernières années (ATOC,2007)(Eurostat,2010) et une possible saturation des lignes, oblige les exploitants de matériel roulant à atteindre un niveau de disponibilité toujours plus élevé. Pour ces raisons, la conception d'une nouvelle architecture de diagnostic est un défi. Ceci a conduit à cette thèse, qui vise à s'assurer que la nouvelle architecture de diagnostic est globalement au moins aussi bonne que l'architecture existante. Cette thèse se situe à l'intersection de trois domaines (Figure 10): la sûreté de fonctionnement, le diagnostic et les systèmes distribués.

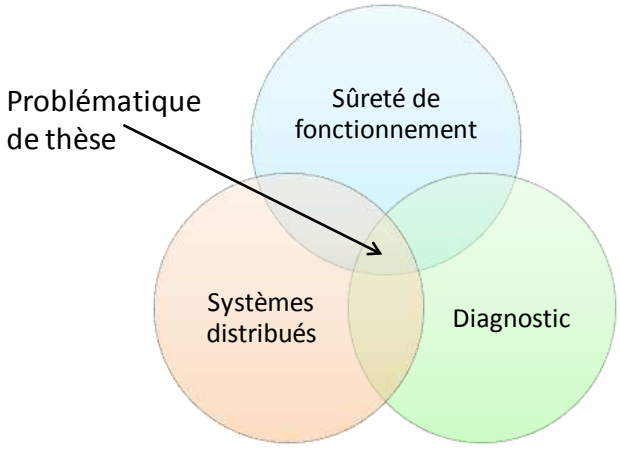


Figure 10 : Problématique de thèse, située à l'intersection de la sûreté de fonctionnement, du diagnostic et des systèmes distribués

Il s'agit donc d'apporter des solutions nouvelles de diagnostic et de maintenance. Le diagnostic prédictif, le diagnostic curatif et un meilleur retour d'expérience doivent permettre au constructeur d'atteindre plus facilement les objectifs de disponibilité. Ces objectifs de disponibilité conditionnent la sortie de la période de garantie, pendant laquelle l'occurrence d'une défaillance sur un train en exploitation est habituellement liée à des pénalités financières (Umiliacchi et al.,2011). A noter que les coûts de maintenance corrective sont à la charge du constructeur durant la période de garantie. D'autre part, l'optimisation dynamique du plan de maintenance permet à l'exploitant d'optimiser le coût de maintenance et donc d'optimiser le LCC.

Un état de l'art des architectures de diagnostic est présenté, afin de bien situer la situation actuelle, ses limites et les solutions apportées par le projet FUI SURFER.

2. Présentation des architectures dans le transport ferroviaire

De nombreux brevets attestent de l'attrait pour industrie sur les sujets de diagnostic et d'optimisation de maintenance (Wesling et al.,1993) (Worcester,2003) (Smedley & Steijger,2004) (Whittaker,2009)(Fries et al.,2009).

Cependant, plusieurs difficultés peuvent être rencontrées lors de l'application de la maintenance conditionnelle sur un système de transport, comme un véhicule ferroviaire. Deux approches fondamentales peuvent être distinguées (Bengtsson,2002) (Alanen et al.,2006):

- le diagnostic débarqué : cette approche consiste à collecter les données en temps réel dans le véhicule et à réaliser le diagnostic dans un centre de maintenance distant.
- le diagnostic embarqué : l'analyse des données et le diagnostic sont embarqués et seule une information de plus haut niveau quitte le véhicule.

Chaque approche est plus ou moins performante en termes de classification, réactivité et robustesse. D'un point de vue fonctionnel, ces différentes architectures peuvent être classées sur trois axes (embarquabilité, type d'architecture (centralisée, décentralisée…), organisation) (Le Mortellec et al.,2013). Il est possible de distinguer :

- le diagnostic distant centralisé (Figure 11a), noté RCD (de l'anglais "Remote Centralized Diagnosis"), où un diagnostic global est débarqué au centre de maintenance,
- le diagnostic embarqué centralisé (Figure 11b), où un diagnostic global est embarqué dans le train et envoie un diagnostic global au centre de maintenance,
- le diagnostic embarqué décentralisé (Figure 11c), qui repose sur des diagnostics locaux embarqués assignés à chaque système élémentaire et un diagnostic global débarqué au centre de maintenance, qui réalise la synthèse des diagnostics locaux générés,
- le diagnostic embarqué distribué coopérant (Figure 11d), noté EDCD (de l'anglais "Embedded Decentralized and Cooperative Diagnosis"), qui repose sur des diagnostics locaux et un diagnostic global embarqués dans le train ; ceux-ci s'échangent des informations pendant la réalisation du diagnostic. Enfin, le résultat du diagnostic global est envoyé au centre de maintenance.

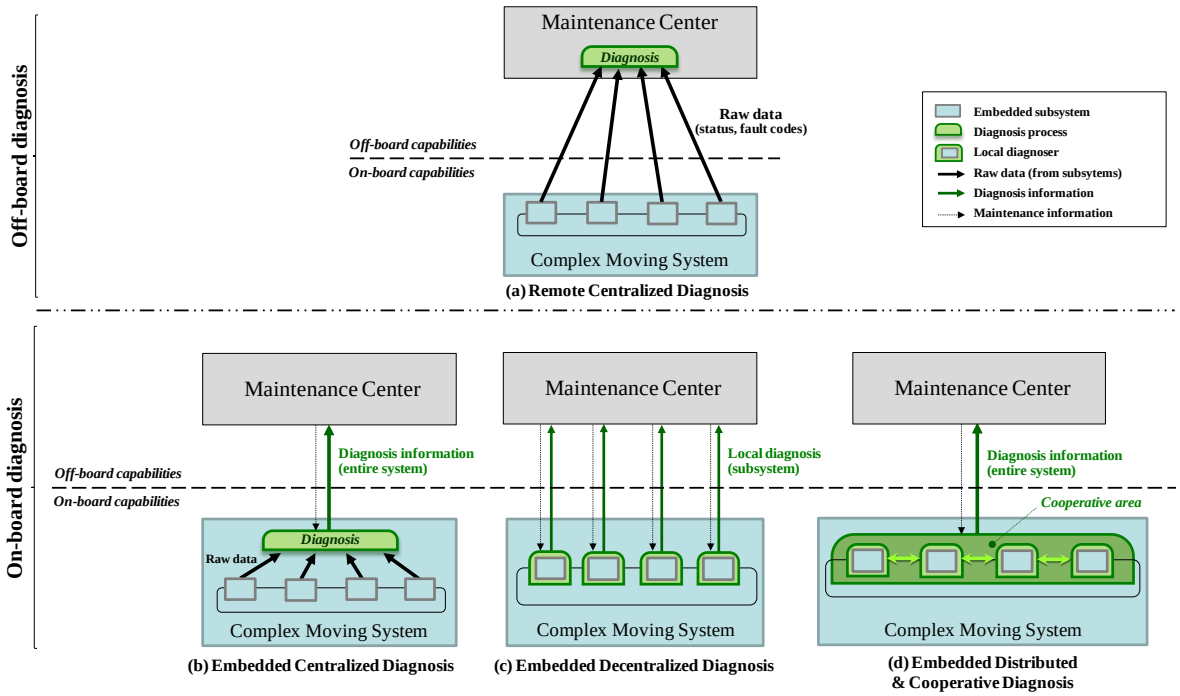


Figure 11 : Classification des architectures de diagnostic dans le transport ferroviaire

Par la suite, seules les architectures RCD et EDCD vont être abordées. Ce choix est motivé par les observations suivantes :

- L'architecture RCD est habituellement utilisée dans les systèmes de transport complexes (Umiliacchi et al,2011). L'architecture EDCD est actuellement étudiée et fait l'objet du projet FUI SURFER (Le Mortellec et al,2013) (Gandibleux et al.,2011).
- RCD et EDCD constituent deux extrêmes : RCD est une architecture centralisée où le diagnostic est débarqué, tandis que EDCD est une architecture distribuée où tous les diagnostics sont embarqués.

Les architectures RCD et EDCD sont maintenant détaillées tant sur les aspects fonctionnels que matériels. Pour ce faire, la Figure 12 sert de support et permet d'introduire la notation.

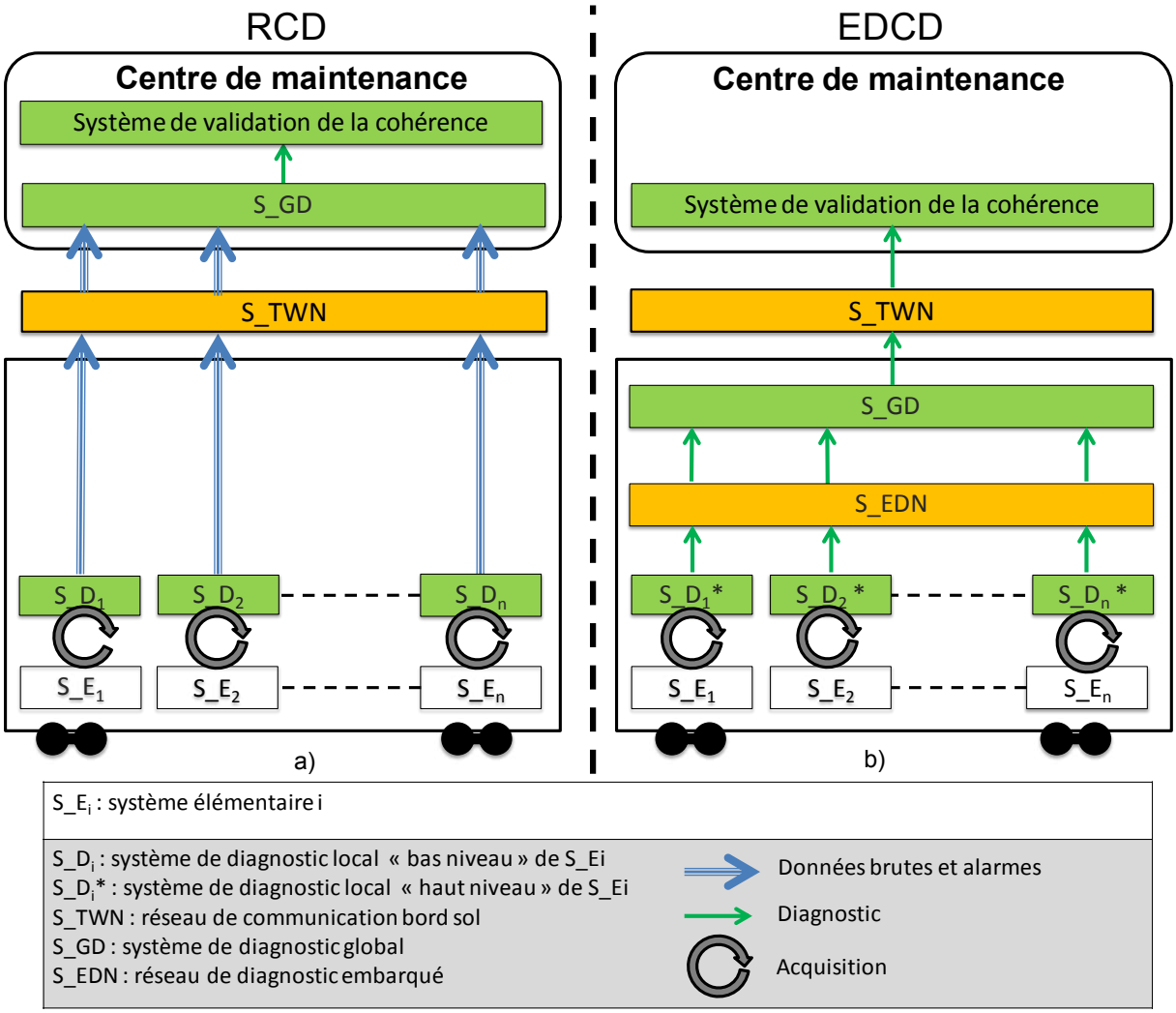


Figure 12 : Détail sur les architectures RCD et EDCD dans le transport ferroviaire

2.1.L'architecture RCD (" Remote Centralized Diagnosis ")

Dans l'architecture RCD (Figure 12a), un système de diagnostic "bas niveau" (voir sous-section 5.2.1), noté S_Di, génère des alarmes. Cette fonction correspond à la fonction surveillance (voir chapitre 1). Chaque S_Di obtient les données brutes des systèmes élémentaires (par exemple grâce à des capteurs). Les données brutes et les alarmes sont ensuite transmises par le S_Di au centre de maintenance distant. Un réseau de communication bord sol, noté S_TWN (de l'anglais "Train to Wayside communication Network"), réalise la transmission de données. Au sol, un système de diagnostic global, noté S_GD (de l'anglais "Global Diagnosis"), est responsable du traitement des données brutes obtenues. Ce dernier est l'entrée d'un système de validation de la cohérence, basé sur un opérateur humain, qui valide les alarmes et vérifie la cohérence des alarmes avec le contexte environnemental. Selon (Le Mortellec et al.,2013), le contexte environnemental permet de caractériser l'état d'un système. Il peut être, par exemple, de nature physique (présence de vibrations, d'interférences électromagnétiques).

L'architecture RCD a fait l'objet de plusieurs travaux dans le transport ferroviaire. Dans cette optique, le volet « Romain » (Remote Monitoring and Maintenance) du projet Traincom (Renner et Umiliacchi,2003) avait pour objectif de définir une architecture complète pour la surveillance à

distance et la maintenance des systèmes ferroviaires. Les résultats de Romain ont constitué le point de départ pour le projet européen EuRoMain (Shingler et Umiliacchi,2003) qui visait à définir et spécifier un système d'aide à la maintenance du système ferroviaire, permettant :

- de surveiller à distance et de diagnostiquer des systèmes à bord des trains,
- d'exploiter les données obtenues en temps réel en liaison avec la documentation technique,
- de récupérer ces données dans le format standard d'une base de données distribuée,
- de présenter les informations appropriées aux utilisateurs finaux, au moyen d'un ensemble complet d'outils.

Le projet InteGRail (Umiliacchi et al.,2006) vise quant à lui à introduire des concepts novateurs tels que la « lean Maintenance » et à étudier la coopération entre le matériel roulant et l'infrastructure, la coopération avec le système de gestion et l'automatisation des dépôts.

2.2.L'architecture EDCD (" Embedded Decentralized & Cooperative Diagnosis ")

La Figure 12b fournit une vue détaillée de l'architecture EDCD. Dans cette architecture, les systèmes de diagnostic sont principalement embarqués à l'intérieur du système de transport (Benedettini et al,2009). Les données brutes sont analysées pendant la circulation du train en service commercial par des systèmes de diagnostic de "haut niveau" (voir sous-section 5.2.2), notés S_Di*, qui génèrent des diagnostics (la cause probable de la (les) défaillance(s)) et génèrent des alarmes. Ces fonctions correspondent en fait aux fonctions surveillance et diagnostic (voir chapitre 1).

Les S_Di* envoient leurs résultats à un système de diagnostic global embarqué. Un réseau de diagnostic embarqué, noté S_EDN (de l'anglais "Embedded Diagnosis Network"), est nécessaire (Kootkar, 2008). Celui-ci permet de supporter les échanges de données entre les S_Di*. Une combinaison de différents diagnostics locaux est réalisée par le S_GD et, logiquement, un diagnostic plus robuste et plus précis est envoyé au centre de maintenance distant (Byington et al,2003) (Dievart et al,2010).

De la même manière que dans l'architecture RCD, la transmission de données vers le centre de maintenance est supportée par S_TWN. Le diagnostic raffiné de S_GD est également validé par un opérateur humain.

Des travaux en cours à la Direction de la Recherche de la SNCF s'intéressent à cette approche prometteuse (SNCF,2009). De plus, les données fournies par un système GPS permettent de relier certains symptômes à des conditions extérieures au véhicule, issues du contexte environnemental (Tanarro et Fuerte,2011). C'est cette approche qui est actuellement développée dans le cadre du projet FUI SURFER.

3. Situation actuelle, limites et solutions envisagées

Cette partie expose la situation actuelle et ses limites, et les solutions envisagées. Ces solutions sont apportées par les partenaires du projet FUI SURFER, qui sont présentés dans la section 3.1. Puis la situation actuelle, ses limites et les solutions envisagées sont successivement présentées aux sous sections suivantes.

3.1.Présentation des partenaires

Le projet FUI SURFER est un projet multipartenaire réunissant BOMBARDIER Transport, Prosyst, le laboratoire TEMPO, l'IFSTTAR et HIOLLE INDUSTRIES, soutenus par les pôles de compétitivité I-Trans et Advancity. Chaque partenaire travaille sur un périmètre défini. Le laboratoire TEMPO, BOMBARDIER Transport et Prosyst sont brièvement introduits ci-dessous. L'IFSTTAR, HIOLLE INDUSTRIES et les pôles de compétitivité I-Trans et Advancity sont présentés en Annexe 2, car leurs travaux n'entrent pas directement dans notre problématique de recherche.

3.1.1. BOMBARDIER Transport

BOMBARDIER Transport France, situé à Crespin, fait partie de BOMBARDIER Transport, chef de file mondial en solutions de transport sur rail et services connexes. La gamme de véhicules sur rail de Bombardier Transport est étendue (métros, véhicules légers sur rail, ou de locomotives et trains à grande vitesse). Grâce au succès sur les projets antérieurs, tels que l'Autorail à Grande Capacité, BOMBARDIER Transport à Crespin est devenu le site de référence en sûreté de fonctionnement au sein de BOMBARDIER Transport.

Pour faire face aux limites des technologies utilisées traditionnellement, le site de Crespin cherche aujourd'hui à évoluer vers la maîtrise du diagnostic embarqué. Il renforce ainsi sa position de chef de file mondial dans le transport ferroviaire en mettant en œuvre des solutions innovantes et moins coûteuses, et le projet FUI SURFER doit y contribuer fortement.

3.1.2. Prosyst

Prosyst est une PME (Petite et Moyennes Entreprise) active dans le domaine des automatismes industriels. Cette activité se traduit par la vente de produits et de services. Les savoir-faire suivants de Prosyst contribuent au projet :

- Surveillance et datation des évolutions de variables d'un système (capteurs/actionneurs, variables d'état …),
- Stockage et traitement des évolutions, par des modèles d'analyse autonomes et évolutifs,
- Diagnostic des défaillances par comparaison au comportement nominal d'un système (via l'exécution en temps réel d'un modèle structurel à événements discrets)

Prosyst apporte également ses compétences en développement logiciel.

3.1.3. TEMPO

Le laboratoire TEMPO (Thermique, Ecoulement, Mécanique, Matériaux, Mise en Forme, PrOduction) est une unité de recherche (EA 4542) à l'Université de Valenciennes et du Hainaut-Cambrésis (UVHC). Les chercheurs impliqués dans le projet FUI SURFER appartiennent tous à l'équipe « Production Services Information » PSI de TEMPO. L'activité de recherche menée au sein de l'équipe PSI s'articule autour de trois principaux thèmes scientifiques :

I. Les systèmes d'aide à la conception de produits intelligents et de systèmes d'information,
II. La modélisation et l'optimisation de la sûreté de fonctionnement et de la maintenance,
III. La conception, l'optimisation et le pilotage de systèmes complexes.

Le croisement des thèmes de recherche I et II, dans le cadre du projet FUI SURFER, constitue une opportunité originale non seulement d'un point de vue applicatif, celui de la surveillance et du diagnostic embarqués de matériel roulant, mais aussi scientifique puisque les développements théoriques réalisés se situent à la croisée de deux grands domaines scientifiques : la sûreté de fonctionnement et les systèmes intelligents. Il donne la possibilité à plusieurs chercheurs de collaborer au travers de l'encadrement de deux thèses, qui sont articulées de la manière suivante :

- La première thèse, nommée thèse Prosyst-TEMPO, se déroule en collaboration avec la société Prosyst. La thèse Prosyst-TEMPO a pour mission de spécifier et modéliser l'architecture distribuée de diagnostic : fonctions, données et traitement locaux. Les modèles élaborés sont utilisés par la société Prosyst pour réaliser les différents systèmes intelligents et procéder à leur intégration dans le train. Ils intègrent les outils développés par l'IFSTTAR (traitement, surveillance et modélisation des signaux) en vue d'élaborer un diagnostic prédictif, conformément aux spécifications de surveillance et de diagnostic embarqués qui sont fixées en phase de conception.
- La seconde thèse, nommée thèse Bombardier-TEMPO, se déroule en collaboration avec BOMBARDIER Transport. Il s'agit de la présente thèse, qui a pour objet d'élaborer une méthodologie pour évaluer l'impact de l'architecture de diagnostic développée dans SURFER sur un matériel roulant. Cette thèse prend en entrée les modèles d'architectures développés dans la première thèse (thèse Prosyst-TEMPO). La problématique de la présente thèse (la thèse Bombardier-TEMPO) est détaillée dans la prochaine section.

3.2.Situation actuelle et limites

L'architecture aujourd'hui utilisée par les constructeurs de matériel ferroviaire, est une architecture de diagnostic type RCD. D'autre part, la méthode de diagnostic utilisée est principalement basée sur des équations booléennes, qui se rapprochent des systèmes experts (voir chapitre 1). Celle-ci permet de tirer partie des capacités de calcul débarqués mais présente plusieurs limites :

- D'importantes quantités de données brutes sont envoyées au S_GD localisé au centre de maintenance. L'architecture RCD implique des contraintes de transmission (telles que, les erreurs de transmission de données, les pertes de données, les retards de transmission, et une bande passante limitée). L'architecture RCD implique un délai important entre l'occurrence de la défaillance et le diagnostic adéquat. De plus, le personnel de maintenance a souvent des difficultés à trouver la cause exacte d'une défaillance dans cette masse de données, ce qui implique un temps de traitement des données non négligeable (Khol & Bauer,2010).
- Le diagnostic est conçu au niveau système et prend peu en compte les interactions entre les systèmes élémentaires et le contexte environnemental associé aux défaillances. Les alarmes ne sont pas validées puisque le contexte environnemental n'est pas géré correctement. Cette notion peut être illustrée concrètement sur un accès voyageur ferroviaire. (Cauffriez et al.,2013) ont démontré que ce système élémentaire est soumis à des contraintes externes lors de l'exploitation du train (dévers de la voie, poids des voyageurs dans le véhicule ou sur les marches lors de la montée/descente, obstacles lors des mouvements d'ouverture/fermeture, vandalisme…). Par exemple, si un frottement anormal est détecté sur

un accès voyageur, les composants internes seront suspectés et un diagnostic sera généré. Cependant, si le même frottement est détecté sur un autre accès voyageur, alors les frottements peuvent probablement être expliqués par le dévers de la voie.

- Les solutions développées sont spécifiques et sont peu réutilisables d'un projet à l'autre.
- De nombreuses défaillances "non reproductibles" sont subies, de l'anglais "Cannot Duplicate Failure" ou "No Fault Found" (Söderholm,2007). Dans une telle situation, une défaillance peut être détectée et localisée sur une entité. Cependant, quand l'entité est testée à un niveau inférieur, alors la détection et la localisation peuvent échouer. Ce phénomène peut avoir plusieurs causes, comme par exemple les défaillances intermittentes (cas des interfaces électriques) ou la complexité élevée de la conception du système. Ce phénomène a un impact négatif sur les coûts et la sûreté de fonctionnement (Söderholm,2007).
- L'architecture d'un train est rendue complexe. En effet, des techniques de tolérance aux fautes (voir chapitre 1), telles que la redondance, sont mises en œuvre pour que le système élémentaire atteigne les objectifs de disponibilité.

Le projet FUI SURFER propose des solutions scientifiques et technologiques aux limites de l'architecture existante. Ces solutions sont détaillées dans la section suivante.

3.3.Solutions apportées par le projet FUI SURFER

Pour surmonter les difficultés liées à la solution existante basée sur RCD, SURFER vise à développer l'architecture EDCD de diagnostics correctifs par la mise en œuvre de modèles de diagnostic embarqués distribués, de diagnostics prédictifs, de maintenance conditionnelle et d'optimisation de la maintenance. Les aspects théoriques de cette approche sont détaillés ci-dessous.

3.3.1. Diagnostic correctif et approche automatique par le modèle

L'approche de diagnostic aujourdhui utilisée, repose principalement sur des alarmes à base d'équations booléennes (franchissement de seuils). Selon les notions introduites au chapitre 1, il ne s'agit pas d'une fonction de diagnostic (identification des causes d'une défaillance), mais d'une fonction de surveillance (détection d'un écart par rapport à un comportement nominal). Il est néanmoins possible d'essayer d'associer ces alarmes à une défaillance.

Les approches de diagnostic (ne pas détecter un écart mais identifier la cause de l'écart) font appel à diverses méthodes (méthodes à base de modèle, méthodes à base de connaissance, etc.) qui ne sont pas implémentées aujourd'hui chez Bombardier Transport.

La société Prosyst a conçu et validé un outil industriel, nommé "diagnostic automatique", utilisant une méthode à base de modèle et une surveillance non intrusive des signaux (en entrée et en sortie) et repose sur l'exécution en temps réel d'un modèle à événements discrets basé sur la structure des équipements à surveiller (Prosyst,2008). Cet outil a été appliqué au diagnostic de lignes de production complexes, pour l'identification de composants défaillants (ou suspects) en cas de pannes. Le schéma ci-dessous en résume le principe (Figure 13).

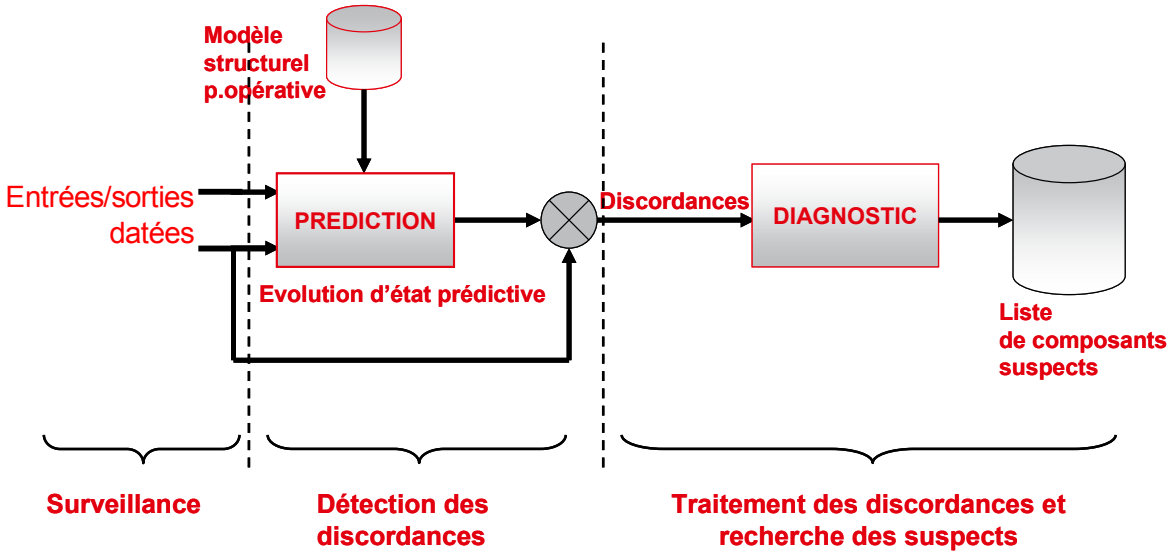


Figure 13 : Diagnostic automatique d'après (Prosyst,2008).

Une discordance correspond à un écart entre le comportement attendu et le comportement observé. Il s'agit, par exemple, de l'absence d'un front montant sur un capteur dans l'intervalle de temps fixé en conception. La connaissance, par le modèle, de tous les équipements électriques et électromécaniques intervenant dans la boucle actionneur->capteurs concernée, permet - par des processus de « suspicion/disculpation » exécutés en temps réel - de converger vers le plus petit ensemble de composants suspects à l'origine du défaut. L'ensemble de composants suspects correspond au diagnostic.

3.3.2. Enrichissement des diagnostics par l'utilisation d'entités intelligentes coopérantes

L'utilisation de capacités de traitement embarquées est rendue possible notamment par les évolutions technologiques relatives aux « capteurs intelligents » (CIAME,2009). Dans le projet FUI SURFER, ces capacités de traitement, de mémorisation et communication sont utilisées afin d'enrichir le diagnostic.

Pour ce faire, une architecture de diagnostic coopérant par la méthode du diagnostic automatique est proposée (Le Mortellec et al.,2013). L'architecture proposée se base sur la décomposition d'un système complexe en sous-systèmes et est composée de plusieurs niveaux de diagnostic. A chaque niveau de décomposition se trouve un système à diagnostiquer, un contexte environnemental et une méthode de diagnostic. Afin d'améliorer la confiance sur le diagnostic et de réduire le nombre de fausses alarmes, un diagnostic utilise le contexte environnemental de son niveau et peut aussi échanger des informations avec les diagnostics situés au même niveau, au niveau supérieur ou au niveau inférieur de l'architecture.

Cette problématique est l'objet de la thèse Prosyst-TEMPO du projet FUI SURFER, réalisée en partenariat entre la société Prosyst et TEMPO, qui a pour mission de spécifier et modéliser l'architecture distribuée de diagnostic, mettant en œuvre des mécanismes de coopération.

3.3.3. Diagnostic prédictif et maintenance conditionnelle

Certaines défaillances (sur les systèmes mécaniques par exemple) ont lieu suite à un phénomène de dégradation progressif tel que l'usure, le déréglage ou le vieillissement (Cauffriez et al.,2013). Il est possible, en observant cette dégradation à intervalles réguliers, d'évaluer sa vitesse d'évolution et de déterminer le moment à partir duquel l'état de dégradation est trop important. Dans le projet FUI SURFER, c'est ce qui est appelé "diagnostic prédictif". Si suite à ce diagnostic prédictif, une tâche de maintenance est déclenchée, alors il s'agit d'une réparation par maintenance conditionnelle.

Le développement du diagnostic prédictif est réalisé par l'IFSTTAR.

3.3.4. Optimisation de la maintenance

Dans la pratique, plusieurs stratégies de maintenance peuvent cohabiter (par exemple, la maintenance conditionnelle, la maintenance systématique, la maintenance corrective), pour atteindre des objectifs de disponibilité et de coût. Afin d'optimiser la maintenance, plusieurs approches existent (Zwingelstein,1996)(Zille,2009).

Au cours de ces dernières années, l'IFSTTAR (Institut Français des Sciences et Technologies des Transports, de l'Aménagement et des Réseaux, présenté en Annexe 2) a proposé une approche générique pour l'optimisation des paramètres de maintenance de systèmes complexes (multi-composants, éventuellement en interaction). Cette approche, nommée VirMaLab (Atelier Virtuel de Maintenance), est illustrée sur la Figure 14 (Bouillaut et al.,2011). Toutes les parties de la modélisation s'appuient sur la théorie des modèles graphiques probabilistes ou réseaux bayesiens dynamiques qui quantifient, par exemple, la probabilité qu'un composant soit dans un état donné.

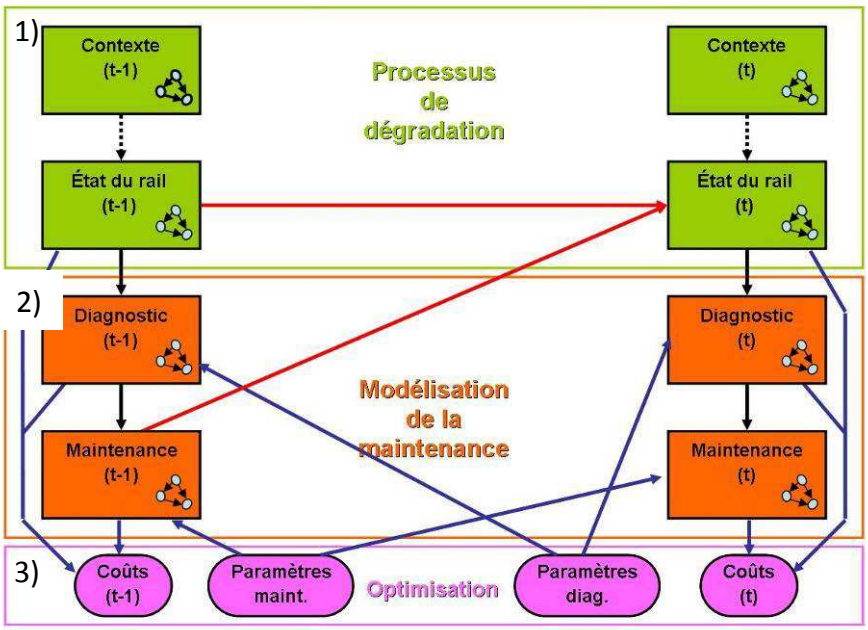


Figure 14 : Approche VirMaLab pour l'optimisation des paramètres de maintenance (Donat,2009)

Le bloc 1 (Figure 14) porte sur la modélisation du processus de dégradation du système élémentaire. Elle peut tenir compte de l'influence de variables contextuelles sur la dégradation et peut considérer plusieurs composants ayant leur propre mode de dégradation (pour une porte par exemple, les actionneurs, les guides et transmissions mécaniques…).

Le bloc 2 (Figure 14) de la modélisation s'intéresse aux systèmes de diagnostic et intègre les paramètres du diagnostic et de la maintenance (périodicité, taux de couverture...).

L'objectif final est d'évaluer et comparer ces différentes politiques en fonction des besoins de l'utilisateur (disponibilité, sécurité, coûts, …) ; le bloc 3 (Figure 14) du modèle consiste alors à intégrer les coûts (de fonctionnement, d'arrêt inopiné, de maintenance, …) caractérisant le système.

Le développement du modèle d'optimisation de la maintenance est également réalisé par l'IFSTTAR.

4. Présentation de la problématique de thèse

Le choix de l'architecture de diagnostic d'un train peut s'orienter vers une architecture de type RCD ou vers une architecture de type EDCD. Si l'architecture RCD est choisie, le risque est alors de perdre le système élémentaire en ligne (du fait des limites de l'architecture), ou d'envisager une redondance du système élémentaire en question. L'intérêt d'une méthodologie d'évaluation des architectures pour argumenter le choix de passer de l'architecture RCD à EDCD apparaît donc nécessaire.

Selon le principe évoqué précédemment, l'architecture EDCD doit être globalement au moins aussi bonne que l'architecture RCD (voir chapitre 1). Cependant, le développement de cette nouvelle architecture de diagnostic (type EDCD) offre de nouvelles possibilités mais engendre également de nouvelles contraintes notamment en matière de sûreté de fonctionnement. La complexité induite par l'intégration des systèmes intelligents et des réseaux de communication, inhérents à une architecture type EDCD, rend difficile la quantification du niveau de sûreté de fonctionnement atteignable, d'autant que les contraintes liées à l'environnement sont fortes. Afin de vérifier si l'architecture EDCD est globalement au moins aussi bonne que l'architecture RCD, il est nécessaire de comparer l'architecture EDCD à l'architecture RCD sur le train.

Cette problématique est à l'origine de ce sujet de thèse, qui vise à justifier l'intérêt d'ajouter une architecture EDCD dans un train. Pour ce faire, il convient de :

- modéliser les architectures de diagnostic afin d'évaluer leurs attributs FMD,
- quantifier la FMD de l'architecture EDCD et la FMD de l'architecture RCD,
- et comparer les bénéfices et pertes du nouveau système par rapport au système existant et s'assurer que le nouveau système répond au principe GAMAB.

Pour atteindre ces objectifs, cette thèse utilise en entrée :

- la formalisation de l'architecture de diagnostic existante (type RCD), qui est déjà implémentée dans les trains,
- la formalisation de l'architecture de diagnostic de type EDCD, qui est la sortie de la thèse Prosyst-TEMPO (Le Mortellec et al,2013) (Le Mortellec et al.,2012). Les thèses Prosyst-TEMPO et Bombardier-TEMPO s'éxécutant en parallèle, la modélisation et l'évaluation de

l'architecture de diagnostic EDCD n'a pu démarrer qu'une fois la formalisation de l'architecture EDCD achevée.

- les informations issues du retour d'expérience en sûreté de fonctionnement de Bombardier Transport (taux de défaillance, taux de réparation…).

5. Verrous scientifiques liés aux systèmes distribués, au diagnostic et à la sûreté de fonctionnement

Plusieurs verrous scientifiques inhérents aux architectures de diagnostic ont été ienditifiés. Ceux-ci concernent les systèmes distribués, le diagnostic et la sûreté de fonctionnement.

5.1. Systèmes distribués

Un train est un système mobile sur un réseau ferré et est habituellement affecté à un centre de maintenance (ou dépôt) statique. Lorsqu'une défaillance se produit en exploitation, l'agent de conduite utilise un réseau de télécommunication pour signaler la panne à distance au centre de maintenance. De plus, un train est caractérisée par une architecture distribuée et il existe généralement au moins un réseau de communication dans le train, afin que les différents systèmes élémentaires communiquent (Berbineau,2002)(Wahl,2004).

Comme cela est indiqué au chapitre 1, la présence des réseaux de communication apporte des contraintes sur le bon fonctionnement de l'architecture globale : la perte du réseau de communication dans un système distribué peut conduire à la perte de mission du système global. Dans un premier temps, la sous-section 5.1.1 détaille la qualité de service, qui caractérise le bon fonctionnement des réseaux de communication. Puis, les menaces pour un réseau de communication et les défenses faces à ces menaces sont présentées.

5.1.1. Qualité de service

La qualité de service d'un réseau est définie dans (E.800,2008) comme " l'*ensemble des caractéristiques d'un service de télécommunication qui lui permettent de satisfaire aux besoins explicites et aux besoins implicites de l'utilisateur du service*". La qualité de service peut être exprimée du point de vue du client ou du fournisseur.

En fonction de l'application, la qualité de service peut être exprimée et mesurée de plusieurs manières (Thomesse,2002)(Rahoual & Siarry,2006) (E.800,2008), par exemple :

- la disponibilité du réseau de communication, qui est la probabilité que le réseau de communication ne soit pas défaillant à t,
- le taux d'erreur résiduel, qui est le rapport entre le nombre de messages perdus ou mal transmis et le nombre total de messages émis au cours d'une période considérée,
- le temps de transit, qui mesure le temps écoulé entre le moment où l'utilisateur du service de transport envoie un message et celui où l'entité de transport réceptrice le reçoit.

La sous-section 5.1.2 liste brièvement différentes menaces récensées pour la qualité de service et les techniques pour surmonter ces menaces.

5.1.2. Menaces et défenses

Dans les réseaux industriels, les messages transmis doivent être intègres et le réseau doit pouvoir garantir l'authenticité, l'intégrité et la promptitude (Ciutat,2010).

Pour les applications ferroviaires, la norme (FprEN50159,2010) a identifié les menaces inhérentes aux réseaux industriels, et les défenses pour les réseaux industriels (Tableau 4). Les menaces comprennent (Ciutat,2010) par exemple :

- la perte : le message a été envoyé mais il n'a pas été reçu (il a été détruit ou refusé),
- l'ordre incorrect : les messages sont envoyés selon une séquence initiale, mais sont reçus dans un autre ordre.

Pour réduire le risque lié à ces deux menaces, les défenses suivantes peuvent être utilisées :

- le numéro de séquence : chaque message envoyé reçoit un nombre appelé numéro de séquence. Le récepteur peut ainsi vérifier que le numéro du message reçu correspond au numéro attendu,
- l'horodatage : chaque message contient une date qui permet de savoir à quelle date il a été envoyé.

		Défenses							
		Numéro de séquence	Horodatage	Surveillance du temps imparti	Identification des sourceset des destinations	Accusé de réception	Procédure d'identification	Code de sécurité	Techniques cryptographiques
Menaces	Répétition	x	x						
	Perte	x							
	Insertion	x			x	x	x		
	Ordre incorrect	x	x						
	Altération des données							x	x
	Retard		x	x					
	Usurpateur					x	x		x

Tableau 4 : Matrice des menaces et défenses, adapté de (FprEN50159,2010)

5.1.3. Conflit d'objectifs : objectif global vs. objectifs locaux

Dans un système distribué, l'atteinte de l'objectif du système global est basée sur la collaboration et le travail collectif des systèmes locaux autonomes (Dievart, 2010). L'atteinte de l'objectif du système global peut être incertaine, car les algorithmes sensés améliorer la performance du système global exigent la plupart du temps une synchronisation entre systèmes locaux. Ceci entre en conflit avec les principes d'autonomie locale et d'information globale minimale (Prabhu & Duffie,1996). De plus, il est difficile de prédire le comportement de ces systèmes, qui peut sembler chaotique, plus particulièrement lorsque des règles heuristiques sont utilisées pour la prise de décision locale (Prabhu & Duffie,1996).

Ce conflit d'objectifs peut également être observé dans les architectures de diagnostic distribué, entre l'objectif local d'un système de diagnostic local et l'objectif global d'un système de diagnostic global. Dans les architectures de diagnostic distribué, le diagnostic global génère un diagnostic pour

le processus complet (voir chapitre 1) à partir des diagnostics locaux. Or, une propriété désirée d'un diagnostic est qu'il soit minimal (voir chapitre 1). L'inconvénient est que, si les diagnostics locaux sont minimaux, alors ils peuvent ne pas être minimaux pour le système distribué complet (Biteus et al.,2011). Le diagnostic global minimal est donc préféré. Cependant, un inconvénient lors de l'utilisation de diagnostics globaux minimaux est qu'ils peuvent inclure des composants inutiles, c'est-à-dire des composants non défaillants. L'inclusion de ces composants implique une utilisation importante de mémoire et de puissance de calcul et a donc des coûts inutiles (Biteus et al.,2011).

5.2.Diagnostic

Dans notre travail, nous faisons référence à deux notions sur les systèmes de diagnostic : le diagnostic local bas niveau et le diagnostic local haut niveau. Ces notions sont définies ci-dessous.

5.2.1. Notion de diagnostic local "bas niveau"

Le "diagnostic local bas niveau" réalise la fonction surveillance. C'est le type de diagnostic mis en œuvre dans l'architecture RCD. Il est qualifié de "bas niveau" dans la mesure où la sortie est une information de bas niveau, c'est-à-dire un ensemble de données brutes et des alarmes.

La méthode utilisée se base sur les équations booléennes. La fonction de surveillance génère une ou plusieurs alarmes, lorsqu'une équation booléenne a la valeur VRAI. Il s'agit par exemple du franchissement d'un seuil sur une grandeur continue (température, vitesse, etc.). Les alarmes sont habituellement accompagnées des valeurs atteintes par les grandeurs continues.

5.2.2. Notion de diagnostic local "haut niveau"

Le "diagnostic local haut niveau" est le type de diagnostic mis en œuvre dans l'architecture type EDCD, développée dans le cadre du projet FUI SURFER. Il est qualifié de "haut niveau" dans la mesure où la sortie est une information de haut niveau, c'est-à-dire un diagnostic.

La méthode de diagnostic utilisée est le diagnostic à base de modèle. Cette approche consiste à comparer le comportement observé du système et son comportement "prédit", résultat de l'inférence d'un modèle explicite du système (De Kleer and Williams,1987). Le diagnostic automatique, utilisé pour le diagnostic curatif SURFER, se base sur les notions de discordance (dans la fonction surveillance) et de liste de suspect (dans la fonction diagnostic) (Willaeys,2008) :

- La fonction de surveillance génère une ou plusieurs alarmes, appelées discordances, lorsque la valeur d'une variable caractéristique observée sur le système est différente de celle prédite par le modèle. Il s'agit, par exemple, de l'absence d'un front montant sur un capteur dans l'intervalle de temps fixé en conception.
- La fonction de diagnostic traite la ou les discordances et permet - par des processus de « suspicion/disculpation » exécutés en temps réel - de générer une liste réduite de "variables suspectes", c'est-à-dire les variables qui pourraient avoir généré la discordance. L'ensemble de variables suspectes correspond au diagnostic.

5.3.Sûreté de fonctionnement

Un système de transport complexe, tel un train, est un système automatisé. Ce type de système prend une part croissante dans l'industrie (Antoni,2009)(Ciutat,2010). Cependant, il est délicat

d'évaluer le niveau de sûreté de fonctionnement de fonctions sur un système automatisé pour plusieurs raisons.

L'approche habituelle en sûreté de fonctionnement considère d'un côté le matériel et d'un autre côté le logiciel (Thiriet,2004)(Borrel,1996).

La sûreté de fonctionnement du logiciel peut être vue comme un domaine spécifique (Villemeur,1991). En effet, le matériel tombe en panne car il est sensible aux fautes physiques ; tandis que le logiciel ne vieillit pas (Gaudoin & Ledoux,2007) et n'est réellement sensible qu'à des fautes de conception (d'origine humaine) présentes dès son origine (ISDF,2000). Or, les logiciels sont caractérisés par une grande complexité, qui conduit à un risque plus élevé d'erreurs de spécification et de conception. De plus, les effets des erreurs de conception ne peuvent pas toujours être palliés par les techniques habituelles de conception tolérante aux fautes (redondance, programmation défensive, diversification) (Antoni,2009). En effet, une erreur de spécification, activée par une combinaison particulière d'entrées, peut affecter toutes les sorties du système redondé, quelque soit le nombre d'unités en redondance.

Or, les systèmes automatisés sont caractérisés par des interactions entre le logiciel et le matériel (Fota et al.,1999). De nouvelles difficultés liées à l'évaluation de sûreté de fonctionnement de tels systèmes apparaissent (Antoni,2009) : nouveaux modes de défaillance, vieillissement, augmentation de la complexité. Il est donc nécessaire de combiner les modélisations des composants matériels et logiciels (Villemeur,1991).

Enfin, le développement de systèmes automatisés s'appuie de plus en plus (Arlat,2000)(Clark et al.,2004) sur les COTS (de l'anglais "commercial off-the-shelf"). L'utilisation de ce type de composants a plusieurs avantages (Arlat,2000)(Redmill,2004) tels que la réduction du coût d'achat et l'incorporation rapide des progrès technologiques. Cependant, les COTS ont également plusieurs inconvénients. Par exemple, les composants disponibles ne sont pas parfaitement adaptés au besoin et comportent des fonctionnalités non-désirées, qui peuvent être sources de défaillance.

5.4. Synthèse et caractérisation de la complexité des architectures de diagnostic

Ci-dessous, le Tableau 5 synthétise et permet de comparer les caractéristiques principales des architectures retenues : l'architecture RCD et l'architecture EDCD.

La partie 3 a permis de lister les limites liées à l'architecture RCD. Une quantité élevée de données est transmise au centre de maintenance. De plus, les alarmes ne sont pas validées et de nombreuses fausses alarmes sont générées. Les S_D génèrent beaucoup de données, ce qui implique un temps important pour les interpréter au centre de maintenance. A titre d'exemple, une quantité de données de plusieurs Gigaoctets peut être générée par jour par train ; cette quantité croît rapidement lorsqu'il s'agit d'étudier une flotte de trains (plusieurs centaines de trains). Cependant, l'architecture RCD est peu complexe à coté de l'architecture EDCD.

Dans l'architecture EDCD, les données brutes analysées pendant l'exploitation du train réduisent les coûts de communication sur S_TWN. La coopération parmi les systèmes de diagnostic embarqués empêche les mauvaises détections et les mauvais diagnostics. En effet, le contexte environnemental ainsi que l'état des systèmes voisins (par exemple, état d'un autre système similaire, profil de

mission) peut être géré plus facilement, car les diagnostics locaux s'échangent des informations (Le Mortellec et al.,2013). Par conséquent, l'architecture EDCD empêche l'occurrence d'alarmes non validées et fournit un diagnostic pertinent au centre de maintenance distant (Dievart,2010). L'architecture EDCD permet donc plus de réactivité.

Cependant, l'architecture EDCD compte deux réseaux de communication tandis que l'architecture RCD n'en compte qu'un. D'autre part, un S_Di* (architecture EDCD) réalise deux fonctions (surveillance et diagnostic), tandis qu'un S_Di (architecture RCD) ne réalise qu'une fonction (surveillance). Un S_Di* en EDCD est donc plus sophistiqué (il a plus de fonctions) qu'un S_Di en RCD. La taille d'un système étant lié à sa complexité (voir partie 1), l'architecture EDCD est plus complexe que l'architecture RCD.

Cette observation sur la complexité est confirmée par la conception innovante et l'utilisation des nouvelles technologies comme les capteurs/actionneurs intelligents dans l'architecture EDCD (voir chapitre 1). De plus, le réseau de communication est un point central. Cette dernière observation prend tout son sens dans le transport ferroviaire, parce que les réseaux de communication ferroviaires fonctionnent dans un environnement soumis à des contraintes importantes (FprEN50159, 2010) (Wahl,2004). D'une part, l'environnement ferroviaire implique des températures de fonctionnement, qui varient de -25°C à +85°C (EN50155, 2007) et une pollution électromagnétique importante (EN50121, 2006) en provenance du train (convertisseurs de puissance, équipements électroniques des passagers). D'autre part, l'application ferroviaire comprend des reconfigurations du train en exploitation (Wahl,2004) et conduit à des modifications de topologie du réseau.

Paramètre	Nombre de réseaux de communication	Quantité de données transmise au centre de maintenance	Alarmes envoyées au centre de maintenance	Temps pour interpréter les données au centre de maintenance	Complexité de l'architecture de diagnostic
architecture RCD	1	Elevée	Non-validées	Elevé	Faible
architecture EDCD	2	Faible	Validées	Faible	Elevée

Tableau 5 : tableau comparatif des architectures RCD et EDCD

Conclusion

Ce chapitre a d'abord permis d'introduire le contexte général de cette thèse, à savoir le projet FUI SURFER, qui vise à optimiser la maintenance par l'amélioration du diagnostic. Puis, les architectures de diagnostic du transport ferroviaire ont été présentées afin d'exposer les solutions existantes et leurs limites, ainsi que les solutions apportées par les partenaires du projet FUI SURFER. La problématique de thèse, qui consiste à évaluer des architectures de diagnostic d'un point de vue sûreté de fonctionnement proposées dans SURFER, a ensuite été détaillée. Enfin, la partie 5 a identifié les verrous scientifiques liés aux systèmes distribués, au diagnostic et à la sûreté de fonctionnement. La sûreté de fonctionnement des systèmes distribués et des systèmes automatisés est difficile à traiter. De plus, le réseau de communication occupe une place importante dans les systèmes distribués. Enfin, nous avons caractérisé la complexité des architectures de diagnostic RCD et EDCD.

Ces observations soulèvent le défi de la conception de l'architecture de diagnostic retenue dans SURFER.

Dans le chapitre 3, une méthodologie pour évaluer les architectures de diagnostic d'un point de vue FMD est proposée.

Chapitre 3 : Proposition de modèles et validation

Chapitre 3 : Proposition de modèles et validation

Introduction

Ce chapitre présente notre travail de recherche en réponse à la problématique de thèse, qui consiste à évaluer des architectures de diagnostic d'un point de vue FMD (Fiabilité, Maintenabilité, Disponibilité).

Pour ce faire, la partie 1 détaille notre justification du choix d'une méthode d'évaluation de FMD et le formalisme retenu, à savoir les Réseaux de Petri Colorés (RdPC). Puis, la partie 2 liste les hypothèses retenues et présente les modèles RdPC proposés pour les architectures de diagnostic. Enfin, la partie 3 se focalise sur la validation par simulation des modèles proposés.

1. Choix d'une méthode de modélisation et d'évaluation de FMD

Dans un premier temps, nous justifions dans cette partie notre choix d'une méthode d'évaluation de FMD. Puis le formalisme retenu (Réseaux de Petri Colorés) est présenté.

1.1. Justification du choix de modélisation et d'évaluation de FMD

L'état de l'art proposé sur l'évaluation de FMD des architectures de diagnostic utilisées dans le transport ferroviaire (voir chapitre 1, partie 3) a permis de remarquer que :

- Les architectures de diagnostic RCD et EDCD sont des systèmes dynamiques et multi-états.
- Les architectures de diagnostic RCD et EDCD sont constituées à leur base de n couples (S_E_i et S_D_i / S_D_i*) identiques, partageant des ressources communes (le réseau de communication bord sol, le système de diagnostic global).
- Les méthodes utilisées (chapitre 1, partie 3) pour évaluer la FMD de ces architectures de diagnostic sont essentiellement des méthodes dynamiques (chaînes de Markov et Réseaux de Petri).

Ces observations nous ont amenés à nous intéresser aux méthodes dynamiques et plus particulièrement aux Réseaux de Petri.

Les Réseaux de Petri permettent de représenter les systèmes dynamiquement grâce à l'évolution des jetons dans les places (Barger,2003). Ils sont donc adaptés pour représenter les architectures de diagnostic RCD et EDCD, qui sont des systèmes dynamiques.

Les systèmes de diagnostic étant des systèmes multi-états (Amari et al.,2008) (Volovoi,2012), les Réseaux de Petri sont également adaptés pour les modéliser. Enfin, les Réseaux de Petri sont adaptés pour représenter le diagnostic et les stratégies de maintenance (Zille, 2009)(Dersin & Péronne,2007).

Les Réseaux de Petri ont une capacité à modéliser de nombreux types de systèmes, par exemple les systèmes à évènements discrets, les systèmes hybrides… (Cordier et al.,1997) (Barger,2003) (Boiteau et al.,2006). Ils permettent de modéliser des phénomènes complexes comme le partage de

ressources, l'exclusion mutuelle, le parallélisme. Les nombreuses extensions dont ils font l'objet leur donnent un grand pouvoir d'expression (David & Alla, 2005). Ils sont donc adaptés pour modéliser les réseaux de communication et le système de diagnostic global des architectures de diagnostic.

Sous certaines conditions, une chaîne de Markov peut être convertie en Réseaux de Petri Stochastiques (David & Alla, 2005). Les modèles de Markov recensés dans la littérature pourraient donc être traduits et évalués en Réseaux de Petri.

Concernant leur évaluation, les Réseaux de Petri couplés à la simulation de Monte Carlo permettent de traiter de grands modèles. De plus, (Niel & Craye, 2002) précise que " *la vitesse de calcul des ordinateurs actuels rend l'utilisation de la simulation de Monte Carlo de plus en plus efficace et la critique de temps de calcul excessifs est de moins en moins fondée* ".

Les Réseaux de Pétri colorés intègrent les temporisations stochastiques et intègrent la notion de couleur (Jensen,2007). Ces derniers sont utilisés pour modéliser les réseaux de communication (Diaz, 2001)(Barger,2003)(Bereznyuk et al.,2007)(Jensen,2007).

Enfin, il existe de nombreux logiciels pour créer, éditer, analyser et simuler les Réseaux de Petri, dont : GRIF (http://grif-workshop.fr), CPN Tools (http://cpntools.org), TimeNET (http://www.tu-ilmenau.de/sse/timenet), Möbius (https://www.mobius.illinois.edu).

Pour toutes ces raisons, les Réseaux de Petri Colorés (RdPC)(Jensen, 1994) couplés à la simulation de Monte Carlo ont finalement été retenus dans cette thèse pour l'évaluation de FMD des architectures de diagnostic.

1.2. Présentation des Réseaux de Petri Colorés

Cette section présente les Réseaux de Petri Colorés (Jensen, 1994), qui sont une extension des Réseaux de Petri (Petri, 1962). La première sous-section rappelle les notions de base sur les Réseaux de Petri. Puis, la deuxième sous-section présente les principales extensions dont ils ont fait l'objet. La dernière sous-section présente une des techniques de résolution habituellement utilisée en sûreté de fonctionnement, à savoir la simulation.

1.2.1. Notions de base

Un réseau de Petri (ou RdP) est un graphe (Figure 15) composé de (Diaz, 2001):

- un ensemble de places, représentées graphiquement par des cercles,
- un ensemble de transitions, représentées graphiquement par des barres,
- un ensemble d'arcs, représentées graphiquement par des flèches, qui relient les places aux transitions et les transitions aux places,
- un ensemble de poids, associés aux arcs,
- une distribution de jetons dans les places.

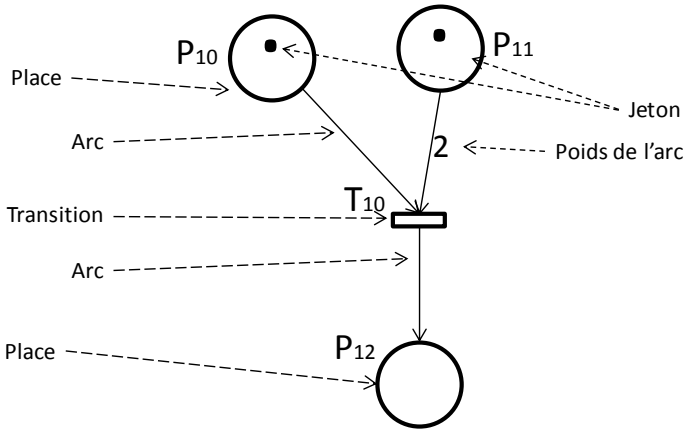


Figure 15 : un Réseau de Petri

L'état global d'un RdP peut se définir par un ensemble de places, qui sont soit marquées (c'est-à-dire lorsqu'elles contiennent un ou plusieurs jetons) soit non marquées (c'est-à-dire lorsqu'elles ne contiennent pas de jeton). La distribution des jetons dans les places est appelée marquage (Diaz, 2001). Le marquage d'un RdP est défini à un moment donné.

Les arcs illustrent les possibilités d'évolution. L'évolution de l'entité modélisée (une fonction, un système) est à l'image de l'évolution du marquage, lui-même provoqué par le franchissement de transitions (David & Alla, 2005). Le RdP peut évoluer lorsque le nombre de jetons dans chaque place d'entrée d'une transition est supérieur ou égal au poids de l'arc qui relie la place à la transition. La transition est alors dite "franchissable". Un arc reliant la place P_1 à la transition T_1, de poids p, signifie que T_1 est franchissable lorsque P1 contiendra au moins p jetons (David & Alla, 2005).

Un conflit structurel existe lorsqu'une place est l'entrée d'au moins deux transitions (David & Alla, 2005). Plusieurs types de résolution existent pour résoudre ces conflits dans les Réseaux de Petri (David & Alla, 2005):

- La priorité. Ce type de résolution est déterministe : lorsqu'un conflit existe entre deux transitions, la priorité est donnée à une transition bien définie.
- Le choix probabiliste. Dans ce type de résolution, une probabilité est assignée à chaque transition. Quand les deux transitions sont franchissables, un nombre est tiré au hasard, de telle sorte que chaque transition est franchie avec la probabilité définie.
- Le franchissement alternatif. Dans ce type de résolution déterministe, des places supplémentaires sont ajoutées, afin qu'une seule des transitions en conflit puisse être franchissable. De plus, la syntaxe est telle que les transitions en conflit sont franchies l'une après l'autre.

1.2.2. Extensions

Depuis leur introduction (Petri, 1962), les RdP ont été dotés de nombreuses extensions (David & Alla, 2005). Les principales extensions vont maintenant être présentées.

1.2.2.1. Réseaux de Petri Temporisés

Les Réseaux de Petri Temporisés permettent d'exprimer le temps. Dans un RdP temporisé, le temps peut être associé aux places (RdP P temporisé) ou aux transitions (RdP T temporisé). Cependant, (David & Alla, 2005) précise qu'il est naturel d'associer la durée d'une opération (ou la durée d'un

état) à une place et d'associer le temps d'attente d'un évènement à une transition (qui est franchie sur occurrence de l'évènement). Nous choisissons donc de présenter uniquement les RdP T temporisé.

Dans un RdP T temporisé, une temporisation de durée d_i est associée à chaque transition T_i . La transition T_i est franchissable lorsque ses conditions de franchissement sont vraies et que la temporisation d_i associée à T_i est écoulée, sauf en cas de conflit (David & Alla, 2005).

1.2.2.2. Réseaux de Petri Stochastiques

Les Réseaux de Petri Stochastiques permettent d'exprimer des probabilités. Un RdP stochastique peut être considéré comme un RdP temporisé, dans lequel les temps ont des valeurs stochastiques (David & Alla, 2005). Dans le RdP Figure 16, une fois que la transition est franchissable, la transition est franchie quand la temporisation associée est écoulée : la temporisation, qui est ici répartie selon une distribution exponentielle, est représentée par son paramètre λ.

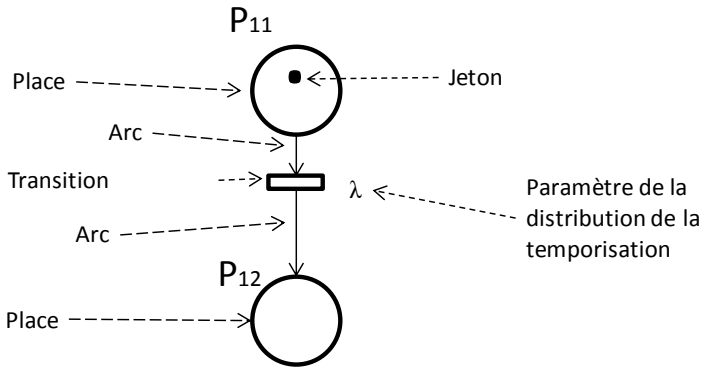


Figure 16 : un RdP stochastique

1.2.2.3. Réseaux de Petri Stochastiques Généralisés

Les RdP Stochastiques Généralisés sont semblables aux RdP stochastiques, mais incluent des transitions immédiates, en plus des transitions associées à des variables aléatoires. C'est-à-dire lorsqu'une transition est franchissable, celle-ci est franchie immédiatement, en un délai nul (Vernez et al.,2003). Une transition immédiate est habituellement représentée sans paramètre.

1.2.2.4. Réseaux de Petri Colorés

Un Réseau de Petri Coloré est composé de places, d'arcs, de transitions et de jetons (Jensen, 1994), auxquels différentes notions sont ajoutées. Ces notions sur les Réseaux de Petri Colorés sont illustrées à la Figure 17.

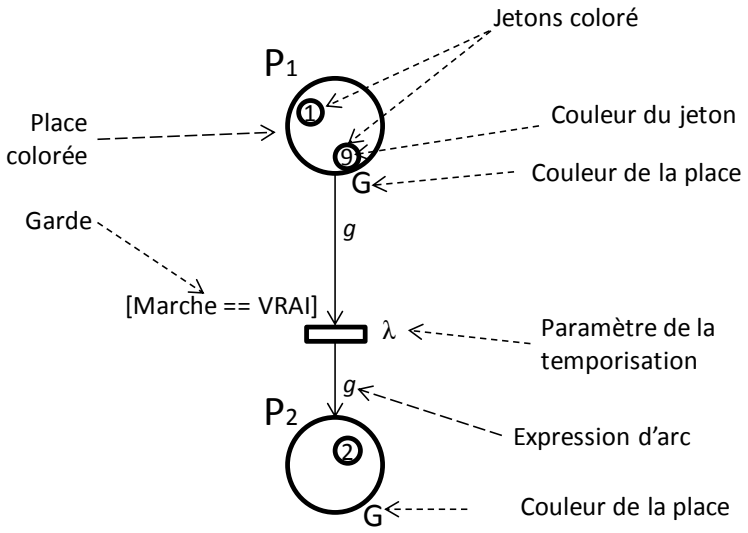


Figure 17 : un Réseau de Petri Coloré

- Notion de couleur dans les Réseaux de Petri Colorés

Une caractéristique importante ajoutée dans les Réseaux de Petri Coloré est la notion de couleur (David & Alla, 2005). Pour des raisons historiques, la notion de couleur fait référence à la valeur associée à un jeton. De même, la notion de domaine couleur fait référence au type de données (Jensen, 1994). Par exemple, l'ensemble des entiers naturels (ℕ) est défini comme un domaine de couleur, tandis que les valeurs 1, 5 ou 52 peuvent être définies comme des couleurs proprement dites. Cette notion métaphorique permet de différencier les uns des autres les jetons des Réseaux de Petri Coloré (les jetons sont "colorés"), contrairement aux Réseaux de Petri "bas niveau", qui ne permettent pas de distinguer les jetons (les jetons sont "noirs") (Jensen, 1994).

- Notion de place dans les Réseaux de Petri Colorés

Une place d'un Réseau de Petri Coloré est une place à laquelle est associée un domaine de couleur. Une place ne peut contenir que des jetons qui appartiennent à une couleur ou un domaine de couleur. Par convention, la couleur de la place est indiquée à proximité de la place, en majuscule.

- Notion de transition dans les Réseaux de Petri Colorés

Les évènements dans un Réseau de Petri Coloré sont représentés au moyen de transitions. Dans un Réseau de Petri Coloré, une transition a les caractéristiques supplémentaires suivantes (Jensen, 1994)(Jensen et al.,2007): une garde (de l'anglais "guard"), un segment de code (de l'anglais "code segment") et une temporisation (de l'anglais "time inscription delay").

  - Une garde de transition est une expression booléenne (de variables), qui permet de limiter la validation de la transition aux cas où l'expression booléenne prend la valeur "VRAI". Par convention, la garde de la transition est indiquée à proximité de la place, entre crochets " [] ".
  - Un segment de code de transition est une portion de code, qui est exécutée chaque fois que la transition est franchie (Jensen et al.,2007). Le code permet par exemple

de modifier l'information d'un jeton coloré : pour un jeton coloré (c'est-à-dire un jeton associé à une valeur) en entrée de la transition, un autre jeton coloré en sortie est créé (c'est-à-dire un jeton associé à une autre valeur).

- Une temporisation de transition en Réseaux de Petri Colorés peut être nulle, déterministe ou stochastique. En fait, elle correspond à une temporisation de transition en Réseaux de Petri Stochastiques Généralisés (voir sous-section 1.2.2.3). Par convention, nous représentons la temporisation de transition de la même manière que dans les Réseaux de Petri Stochastiques Généralisés.

- Notion d'arc dans les Réseaux de Petri Colorés

Un arc, en Réseau de Petri Coloré, est associé à une expression d'arc, qui permet de modifier le nombre de jetons et les valeurs des jetons (Jensen, 1994). Une expression d'arc peut contenir (Barger,2003):

- Une valeur : pour que le jeton puisse passer, il faut que l'expression d'arc contienne cette valeur, sinon le passage lui est interdit.
- Une variable : la variable est fixée à une valeur particulière, et le même principe que précédemment s'applique. Cependant, la valeur de la variable ne change pas pendant tout le franchissement de la transition.
- Une fonction : elle permet de réaliser des opérations sur les jetons. Il peut s'agir d'une fonction simple (fonction identité) ou plus complexe (expression incluant des tests conditionnels par exemple).

1.2.3. Résolution par simulation

La modélisation d'un système en Réseaux de Petri permet une meilleure compréhension de ce système. Ce modèle peut en plus être analysé de façon automatique par plusieurs méthodes (Diaz, 2001) (Niel & Craye, 2002) (Antoni, 2009) : l'analyse des invariants, le graphe de marquage, la simulation.

Dans notre cas, les RdP sont utilisés pour leur capacité à modéliser les systèmes et sont résolus par simulation. La plupart des propriétés nécessaires (par exemple l'absence de conflit, l'invariance…) ne sont donc pas utilisées (Niel & Craye, 2002). Le principe de la simulation est basé sur (Niel & Craye, 2002) :

- la modélisation des parties fonctionnelle et dysfonctionnelle du système à étudier,
- l'animation du modèle par tirage de nombres au hasard pour réaliser des histoires possibles du système,
- l'obtention de résultats statistiques.

2. Proposition d'un modèle

Cette partie a pour but de présenter les modèles des architectures RCD et EDCD, qui ont été proposés dans (Gandibleux et al.,2013). Ci-dessous, les hypothèses fixées pour la modélisation sont listées dans la première section. Les modèles RdPC des architectures de diagnostic sont proposés

dans la deuxième section. Enfin, les modèles complets des architectures RCD et EDCD sont proposés dans la troisième section.

2.1. Hypothèses

Pour la suite de notre travail, les hypothèses suivantes sont fixées :

i. Le système élémentaire i (S_E_i) est supposé binaire : il peut être soit dans l'état de marche, soit dans l'état de panne et est dans l'état de marche à l'instant initial.
ii. Le système de diagnostic (S_D_i / S_D_i*) est supposé ne jamais être dans un état de panne permanent et est supposé être dans l'état de marche à l'instant initial. Le terme permanent fait référence à un état de panne, depuis lequel plus aucune réparation n'est possible. En effet, quand un S_D_i subit une défaillance permanente, plus aucune alarme n'est émise.
iii. De la même manière, le réseau de communication bord sol (S_TWN) et le réseau de communication embarqué pour le diagnostic (S_EDN) sont supposés ne jamais être dans un état de panne permanent, car ce mode de défaillance conduit à une défaillance complète de l'architecture de diagnostic.
iv. En cas de fonctionnement du système de diagnostic (S_D_i / S_D_i*), la défaillance de S_E_i est détectée. Cependant, S_D_i / S_D_i* peut défaillir et générer des fausses alarmes.
v. A l'instant initial, r réparateurs sont disponibles pour n systèmes élémentaires (r<n).
vi. Une fois que la réparation est terminée, S_E_i et S_D_i sont supposés être dans l'état de marche.
vii. Le système de diagnostic global S_GD traite toutes les alarmes qui n'ont pas été validées. La notion d'alarme validée fait référence à une alarme générée par S_D_i alors que S_Ei est défaillant. Cependant, S_GD peut émettre une demande de réparation (succès) ou ne pas émettre de demande de réparation (échec).

Le comportement résultant de ces hypothèses peut maintenant être modélisé.

2.2. Modèles des architectures de diagnostic

Cette section est dédiée à la modélisation des architectures de diagnostic RCD et EDCD. Les modèles RdPC des architectures RCD et EDCD sont composés de plusieurs RdPC interconnectés. Chaque RdPC décrit le comportement d'une entité spécifique : les réseaux de communication S_TWN et/ou S_EDN, les systèmes élémentaires S_E_i, les systèmes de diagnostic S_D_i / S_D_i*, le système de diagnostic global S_GD et la maintenance.

Les Réseaux de Petri Colorés reposent sur un formalisme très strict (voir sous-section 1.2.2.4). Cependant, afin de faciliter la compréhension du lecteur, les expressions d'arc et couleurs de place ne sont pas affichées dans les modèles. Les interconnexions entre les RdPC sont mises en valeur par des places et des arcs en pointillés. Dans les RdPC, l'indice i indique le ième système élémentaire S_E_i et son système de diagnostic associé, noté S_D_i ou S_D_i*.

Etant donné que les architectures reposent sur des réseaux de communication (S_TWN et/ou S_EDN), la modélisation en RdPC de ces réseaux est d'abord détaillée, dans la sous-section ci-dessous. Puis les modèles des architectures de diagnostic RCD et EDCD sont présentés dans les sous-sections suivantes.

2.2.1. Modèle d'un réseau de communication

Plusieurs modèles pour les réseaux de communication ont été proposés dans la littérature (voir chapitre 1). Les réseaux de communication embarqués dans les trains, comme S_EDN, reposent sur

des technologies spécifiques au transport ferroviaire, comme par exemple le réseau MVB "Multifunction Vehicle Bus" (IEC61375,2012), ou des technologies plus généralement utilisées dans l'industrie, comme par exemple le réseau Profibus (Wahl et al.,2004).

Quelque soit le type de réseau de communication, des protocoles existent pour détecter les messages qui ont été transmis en erreur : par exemple, le contrôle de la parité ou les codes à redondance cyclique (Rahoual & Siarry, 2006)(Ciame,2009). Cependant, ces protocoles de détection ne sont pas parfaits. Il est donc possible qu'un message soit transmis avec une ou plusieurs erreurs non détectée(s) par les protocoles de détection.

Dans notre travail, nous caractérisons cette erreur par la notion d'erreur résiduelle. Nous la définissons par le rapport entre le nombre de bits altérés en dépit des protocoles de détection/correction des erreurs sur le nombre total de bits transmis :

$$\mathrm{p_{RE}} = \frac{nombre\ de\ bits\ altérés\ en\ dépit\ des\ protocoles\ de\ détection/correction}{nombre\ total\ de\ bits\ transmis} \quad (8)$$

Dans notre travail, selon l'hypothèse (iii), la modélisation du réseau de communication prend en compte les défaillances temporaires et les erreurs résiduelles. De plus, nous supposons que, lorsqu'une erreur résiduelle se produit, elle est détectée dans tous les cas et aucune retransmission du message erroné n'est réalisée par le réseau de communication.

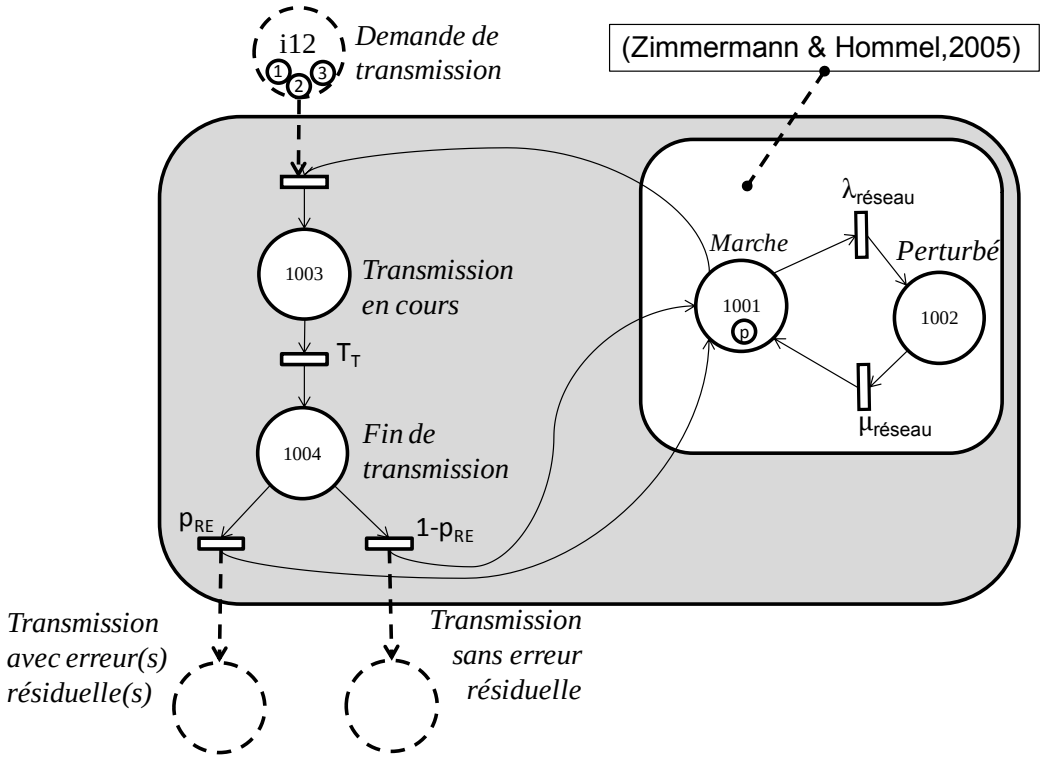
Pour modéliser un réseau de communication temps réel, (Zimmermann & Hommel,2005) propose un Réseau de Petri à 2 places et identifie empiriquement les lois de probabilité exponentielles de défaillance temporaire (paramètre $\lambda_{réseau}$) et de reprise après celles-ci (paramètre $\mu_{réseau}$). Inspiré de ce travail, la Figure 18 comporte deux principaux états: l'état de marche (place 1001) et l'état perturbé (place 1002). Le jeton du Réseau de Petri évolue de la place 1001 à la place 1002 lorsqu'une défaillance temporaire se produit (par exemple, due à des perturbations électromagnétiques). La place 1001 est à nouveau marquée après un certain temps, modélisé par le taux de reprise $\mu_{réseau}$.

A ce modèle est ajoutée la partie grisée de la Figure 18, décrivant le processus de transmission:

- La transmission démarre quand une requête de transmission est émise (place i12) et que le réseau de communication est dans l'état de marche (place 1001).
- La transmission est modélisée par les places 1003 et 1004 avec un temps de transmission T_T qui est lié à la taille du message n exprimée en bit et au débit du réseau de communication Q en bit/s. T_T est défini par :

$$T_T = \frac{n\ (bit)}{\mathrm{Q\ (bit/s)}} \quad (9)$$

- Le modèle permet également de prendre en compte la notion d'erreur résiduelle. Cette possibilité est modélisée par deux transitions avales et par la probabilité p_{RE} qu'un message soit affecté par une erreur résiduelle. Il convient de s'assurer que la somme des probabilités, associées aux différentes alternatives, soit égale à 1. Ici, deux alternatives sont possibles : occurrence de l'évènement ou absence d'évènement. Pour respecter cette égalité, la probabilité associée à la transition "Transmissions avec erreur(s) résiduelle(s)" est donc p_{RE} et la probabilité associée à la transition "Transmissions sans erreur résiduelle" est le complément, soit $1-p_{RE}$.



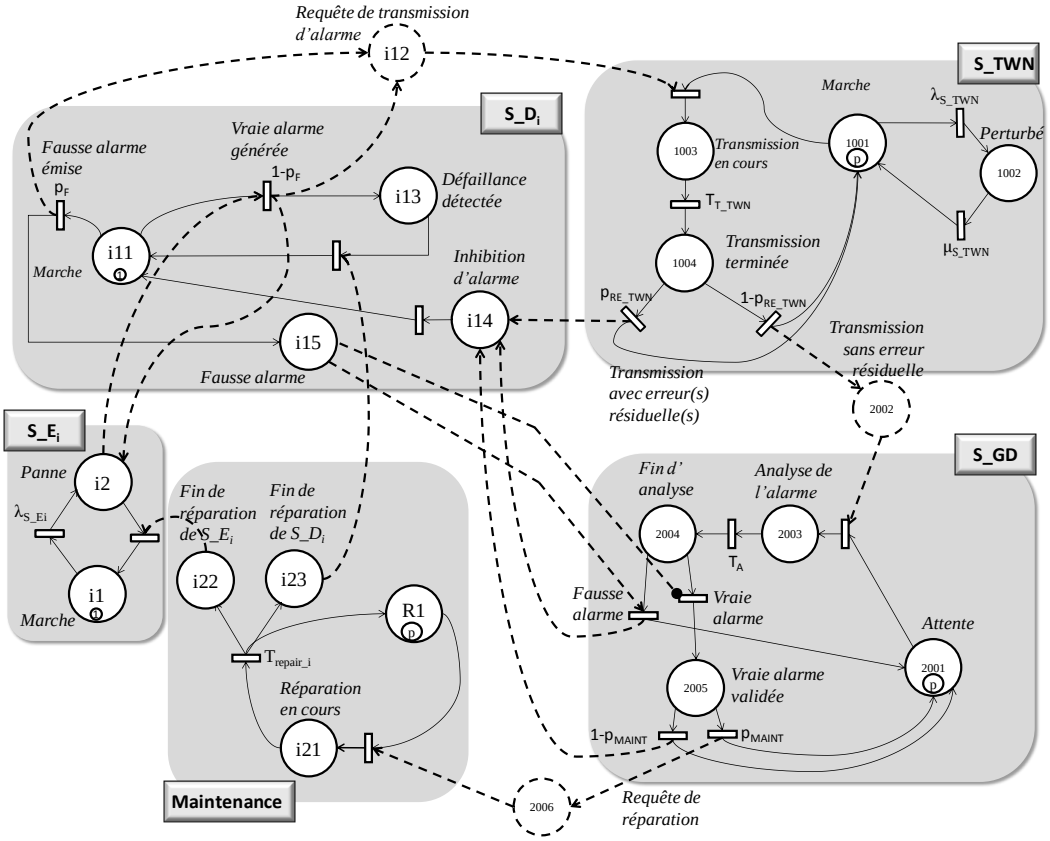
Légende
$\lambda_{réseau}$: Taux de défaillance du réseau de communication
$\mu_{réseau}$: Taux de reprise du réseau de communication
p_{RE} : Probabilité qu'un message soit affecté par une erreur résiduelle
T_T : Temps de transmission

Figure 18 : Modèle RdPC d'un réseau de communication

Il convient de remarquer que, étant donné que le réseau de communication est une ressource commune, il doit être capable de gérer tous les jetons colorés, correspondant aux différents messages de S_D_i ou S_D_i*. Un conflit peut se produire lorsque plusieurs demandes de transmission sont en attente et que le réseau de communication est dans l'état de marche (la place 1001 contient un jeton). Dans nos travaux, nous avons choisi de résoudre ces conflits par priorité, en donnant la priorité au jeton avec l'index i le plus petit.

2.2.2. Modèle de l'architecture RCD

Le modèle RdPC générique de l'architecture RCD est composé de plusieurs RdPC interconnectés (zones grises). Le modèle RdPC est générique dans le sens où il peut convenir pour n couples S_Ei et S_D_i / S_D_i*. A des fins d'illustrations, le modèle RdPC est présenté pour n=1 (Figure 19). Pour une architecture RCD donnée, il existe un seul RdPC pour le réseau de communication bord sol S_TWN, un seul RdPC pour le système de diagnostic global S_GD et un seul RdPC pour la maintenance, tandis que les systèmes élémentaires S_E_i et systèmes de diagnostic S_D_i peuvent être instanciés n fois. Cette instanciation des couples S_Ei et S_Di / S_D_i* est réalisée en mettant n jetons dans la place i1 et n jetons dans la place i11.



Legende	
λ_{S_Ei} : taux de défaillance du système élémentaire i (S_Ei) T_{repair_i} : temps de réparation du couple (S_E_i / S_D_i) p_F : probabibité que S_Di défaille T_{T_TWN}: temps pour transmettre un message d'alarme du S_Di vers le S_GD (au centre de maintenance) T_A : temps d'analyse d'une alarme P_{MAINT} : probabilité de déclencher une opération de maintenance	λ_{S_TWN} : taux de défaillance de S_TWN μ_{S_TWN} : taux de reprise de S_TWN p_{RE_TWN} : probabilité qu'un message sur S_TWN soit affecté par une erreur résiduelle

Figure 19 : modèle RdPC de l'architecture RCD

Le RdPC proposé pour décrire le comportement d'un S_Ei a deux places, correspondant respectivement aux états de marche et de panne (Figure 19). Le jeton i représente S_E_i. La transition depuis l'état de marche vers l'état de panne (i2) suit une loi de distribution caractérisée par le taux de défaillance λ_{S_Ei}. La transition depuis l'état de panne vers l'état de marche (i1) est régie par un jeton dans la place i22, modélisant la fin de réparation à l'issue de la chaîne de diagnostic et de réparation.

Le comportement de S_D_i est modélisé par un Réseau de Petri coloré qui caractérise la bonne détection, lorsque la défaillance de S_E_i est détectée (place i13), la mauvaise détection, en cas de fausse alarme (place i15) et l'inhibition d'alarme (place i14). Cette place i14 modélise l'inhibition, c'est-à-dire la non-transmission d'une demande d'alarme soit en cas de transmission erronée (place 1004), soit en cas de fausse alarme (place 2004), soit lorsqu'une opération de maintenance n'est pas déclenchée (place 2005). Cette inhibition est nécessaire afin de réarmer le S_Di qui a généré l'alarme ou le diagnostic de S_Ei. Après inhibition d'une alarme, S_D_i retourne dans l'état initial (place i11). S_D_i est initialement dans l'état de marche (place i11). L'évolution de S_D_i vers l'état de défaillance détectée ou de fausse alarme est modélisée par deux transitions aux probabilités complémentaires :

- S_D_i évolue vers l'état de vraie alarme avec la probabilité 1-pF (place i13) et émet une requête de transmission d'alarme.
- Sinon, $S\_ D_i$ génère des fausses alarmes avec la probabilité pF (place i15) et émet dans ce cas une requête de transmission de fausse alarme.

La modélisation de S_TWN est similaire à celle présentée à la sous-section 2.2.1, mis à part que les paramètres T_{T_TWN}, λ_{S_TWN}, et μ_{S_TWN} sont ceux du réseau de communication bord sol (S_TWN).

Le comportement de S_GD est modélisé par un Réseau de Petri coloré à quatre places. Le S_GD est en d'attente dans l'état initial (place 2001) et évolue dans l'état d'analyse (place 2003) quand une alarme est reçue (place 2002). Le temps nécessaire pour analyser l'alarme est modélisé par la durée T_A. A la fin de l'analyse, deux alternatives sont possibles (place 2004) :

- Si l'alarme est considérée comme "fausse", alors elle est inhibée (place i14).
- Si l'alarme est considérée comme "vraie" et validée (place 2005), alors deux alternatives sont possibles :
    - une demande une réparation est réalisée avec la probabilité p_{MAINT} car l'alarme est justifiée (place 2006).
    - l'alarme est inhibée avec la probabilité $1\text{-}p_{MAINT}$ si l'intervention est jugée non-prioritaire (place i14).

Une fois que le choix entre ces alternatives a été réalisé, S_GD retourne dans l'état d'attente (place 2001).

La maintenance est modélisée par un RdPC à quatre places. Quand une réparation est demandée (place 2006) et qu'un réparateur est disponible (place R1), alors la réparation démarre (place i21)

pour un couple S_E_i / S_D_i défaillant. La durée de réparation est modélisée par le temps T_{repair_i}. Les places i22 et i23 correspondent respectivement à la fin de réparation de S_E_i et S_D_i. Si plusieurs S_E_i sont simultanément en attente de réparation (la place 2006 contient plusieurs jetons), alors il est possible de modéliser r réparateurs (place i21) par r jetons dans la place R1. A des fins d'illustration, la Figure 19 illustre le RdPC de maintenance pour r=1.

Le lecteur doit garder à l'esprit que des conflits peuvent exister, par exemple :

- entre les couples "S_E_i / S_D_i", lors de l'accès au réseau de communication (place 1003) et à un réparateur (place R1),
- lorsque plusieurs alarmes doivent être analysées (place 2002) et que le S_GD est en attente.

De la même manière que précédemment, pour résoudre ces conflits, la priorité est donnée à l'index i le plus petit. De même, S_TWN, S_GD et les r réparateurs sont des ressources communes (marque p) et définis dans la couleur unité, qui est la couleur de base (Jensen,2007). Les S_E_i et S_D_i sont définis dans le domaine de couleur entier naturel ($\mathbb{N}$), où la marque i représente le système i.

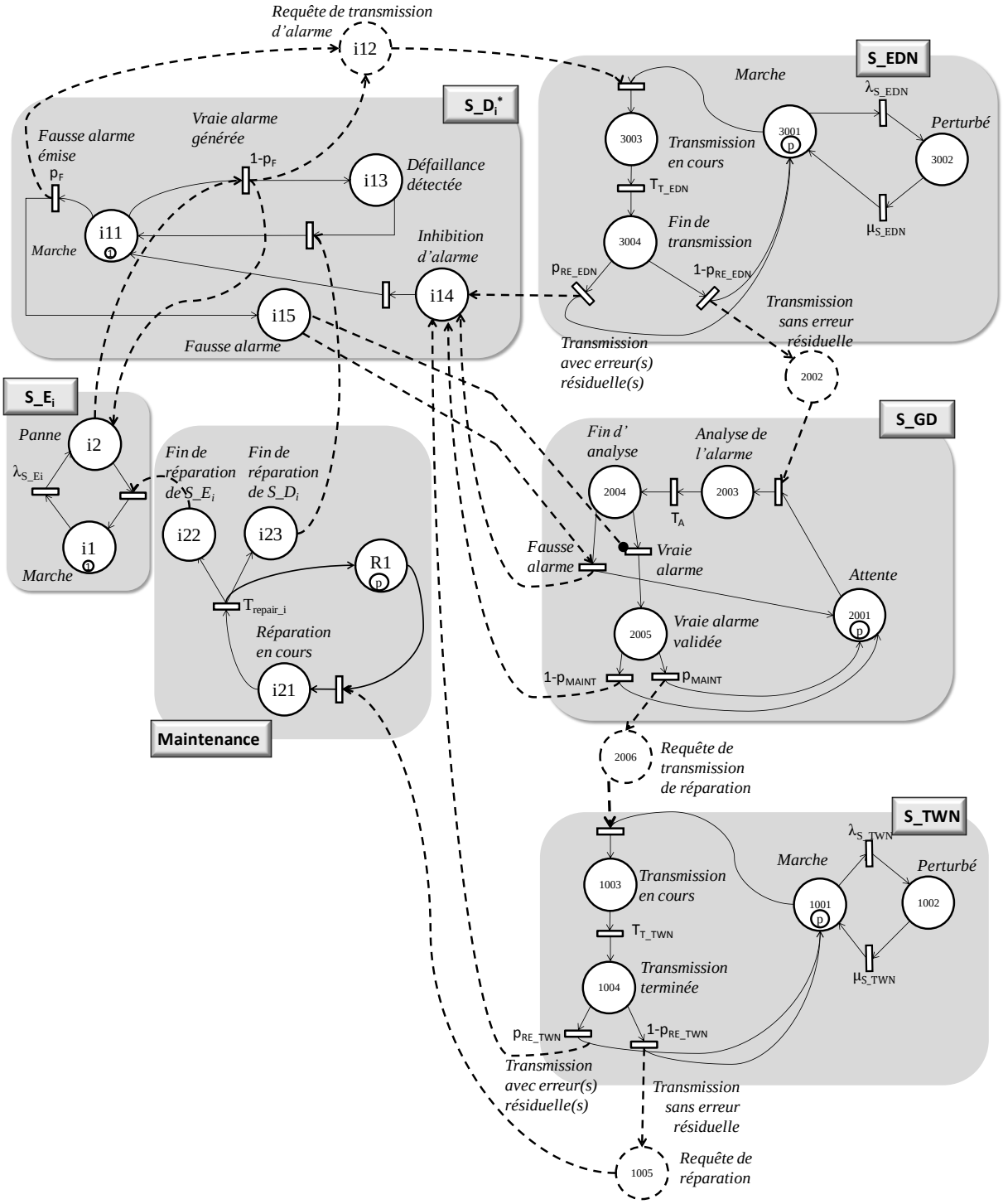
2.2.3. Modèle de l'architecture EDCD

Le modèle de l'architecture EDCD est similaire au modèle de l'architecture RCD. Trois principales différences existent :

- Les systèmes de diagnostic embarqués S_D_i* génèrent des diagnostics de haut niveau, c'est-à-dire la cause probable d'une défaillance.
- Le diagnostic global S_GD est embarqué et n'est pas localisé au centre de maintenance.
- Un réseau de communication supplémentaire (S_EDN) est utilisé pour échanger les messages dans le train, qui est modélisé par un seul RdPC similaire à S_TWN.

Le principe d'instanciation des couples "S_E_i / S_D_i*" est similaire à l'architecture RCD : chaque S_E_i est couplé à S_D_i*.

La Figure 20 fournit les RdPC interconnectés, modélisant l'architecture EDCD.



Légende

λ_{S_Ei} : taux de défaillance du système élémentaire i (S_Ei) T_{repair_i} : temps de réparation du couple (S_E_i / S_D_i) p_F : probabilité que S_Di* défaille T_{T_TWN}: temps pour transmettre un message d'alarme du S_GD au centre de maintenance T_{T_EDN} : temps pour transmettre un message d'alarme de S_Di* à S_GD T_A : temps d'analyse d'une alarme P_{MAINT} : probabilité de déclencher une opération de maintenance	λ_{S_TWN} : taux de défaillance de S_TWN μ_{S_TWN} : taux de reprise de S_TWN p_{RE_TWN} : probabilité qu'un message sur S_TWN soit affecté par une erreur résiduelle λ_{S_EDN} : taux de défaillance de S_EDN μ_{S_EDN} : taux de reprise de S_EDN p_{RE_EDN} : probabilité qu'un message sur S_EDN soit affecté par une erreur résiduelle

Figure 20 : modèle RdPC de l'architecture EDCD

3. Validation

Cette partie propose de valider théoriquement les modèles proposés en comparant l'architecture RCD à l'architecture EDCD. Pour ce faire, le protocole de validation consiste à considérer un cas optimiste et un cas pessimiste. Puis, les résultats sont générés en sortie des modèles afin de valider le comportement attendu en fonction des valeurs fixées en entrée.

3.1.Définition d'un protocole de validation

Dans le protocole de validation retenu, les architectures RCD et EDCD sont simulées. Pour obtenir une sollicitation identique en entrée des architectures, les temps avant défaillance des systèmes élémentaires S_E sont tirés a priori, dans le logiciel MATLAB, selon la distribution de défaillance retenue. Puis, un vecteur, constitué de tous ces temps avant défaillance, est mis en entrée du logiciel de simulation des Réseaux de Pétri. A chaque S_Ei en architecture RCD et en architecture EDCD est associé un ensemble de temps identiques.

Pour comparer l'architecture RCD à l'architecture EDCD, un ensemble de critères (Tableau 6) est utilisé. Les mesures implémentées pour la FMD (le MTTF, la MDT et A(t)) sont définies au chapitre 1. Neuf critères supplémentaires sont introduits :

- le nombre d'erreurs résiduelles sur les réseaux de communication, noté N_{RE} (pour "Number of Residual Errors"),
- le temps cumulé d'analyse des fausses alarmes, noté CTFA (pour "Cumulative Time Spent on analyzing False Alarms"), qui permet de mesurer le temps "perdu" à analyser des alarmes, dans le sens où il ne permet ni de réparer un S_Ei ni d'améliorer un attribut de l'architecture,
- le temps cumulé d'analyse des vraies alarmes, noté CTTA (pour "Cumulative Time spent on analyzing True Alarms"), qui permet de mesurer le temps consacré à raison à analyser des alarmes, dans le sens où ces vraies alarmes sont émises après qu'un S_E_i soit défaillant,
- le temps cumulé d'analyse de toutes les alarmes, noté CTAA (pour "Cumulative Time spent on analyzing All Alarms"), qui permet de mesurer le temps consacré à analyser toutes les alarmes : les fausses alarmes et les vraies alarmes. Ainsi, il est possible d'écrire que CTAA est la somme du temps cumulé passé à analyser les fausses alarmes (CTFA) et du temps cumulé passé à analyser les vraies alarmes (CTTA).
- le Pourcentage de Temps d'analyse passé à analyser des Fausses Alarmes, noté PTFA, qui permet de mesurer la proportion de CTAA consacrée à l'analyse des fausses alarmes.
- le nombre de vraies alarmes, noté NTA (de l'anglais "Number of True Alarms"), qui mesure le nombre d'alarmes/diagnostics générés après qu'un S_E_i soit défaillant,
- le nombre de fausses alarmes, noté NFA (de l'anglais "Number of False Alarms"),
- le nombre total d'alarmes, noté NAA (de l'anglais "Number of All Alarms"), qui mesure le nombre de toutes les alarmes/diagnostics générés. Ainsi, NAA est la somme du nombre de vraies alarmes (NTA) et le nombre de fausses alarmes (NFA).
- la taille de l'architecture de diagnostic, qui mesure l'encombrement de l'architecture de diagnostic.

Critères de validation d'architecture pendant le temps de simulation	Mesure implémentée sur les RdPC
Fiabilité	MTTF
Maintenabilité	MDT
Disponibilité	A(t)
Mesure du nombre d'erreurs résiduelles sur les réseaux de communication	N_{RE}
Mesure du Temps Cumulé d'analyse des Fausses Alarmes	CTFA
Mesure du Temps Cumulé d'analyse des Vraies Alarmes	CTTA
Mesure du Temps Cumulé d'analyse de toutes les Alarmes	CTAA = CTTA + CTFA
Pourcentage de Temps d'analyse passé à analyser des Fausses Alarmes	$PTFA = \frac{\text{CTFA}}{\text{CTAA}} = \frac{\text{CTFA}}{\text{CTTA} + \text{CTFA}}$
Nombre de vraies alarmes	NTA
Nombre de fausses alarmes	NFA
Nombre total d'alarmes	NAA = NTA + NFA
Evaluation de taille de l'architecture de diagnostic	Nombre d'entités constituant l'architecture de diagnostic embarquées dans le train

Tableau 6 : critères de validation et mesures réalisées sur les RdPC

Deux logiciels (CPN Tools et GRIF) ont été utilisés pour implémenter les modèles RdPC des architectures de diagnostic. GRIF ne supportant pas les Réseaux de Petri colorés, les modèles proposés ont donc été convertis en Réseaux de Petri stochastiques. Cette conversion est possible, car les RdPC proposés ont un nombre fini d'ensemble de couleurs (David & Alla,2005). Les résultats fournis par les deux logiciels ont une erreur relative de moyenne 11% et d'écart type 0.2.

3.2.Simulation et résultats

Le premier cas théorique de validation consiste à simuler un couple "S_E_i / S_D_i" pour l'architecture RCD et un couple "S_E_i / $S\_D_i^*$" pour l'architecture EDCD (n=1). Pour n=1, une architecture est supposée :

- fiable si tous les systèmes S_E, S_D (ou S_D*) et tous les réseaux de communication (S_TWN et S_EDN) sont dans l'état de bon fonctionnement,
- disponible si S_E et S_D sont tous les deux dans l'état de bon fonctionnement

Le second cas théorique de validation est basé sur le même principe de validation en utilisant trois couples “S_E_i / S_D_i” respectivement “S_E_i / $S\_D_i^*$” (n=3). Pour n=3, une architecture est supposée :

- fiable si tous les couples "S_Ei et S_Di / S_Di* associés" et tous les réseaux de communication sont l'état de bon fonctionnement (S_TWN et S_EDN)
- disponible si au moins un couple parmi les trois “S_E_i / S_D_i” ou “S_E_i / $S\_D_i^*$” est dans l'état de bon fonctionnement

3.2.1. Premier cas théorique de validation

Deux campagnes de simulation ont été réalisées avec les entrées données dans le Tableau 7. La durée de simulation a été fixée à 8760h (soit 1 an), afin que les valeurs asymptotiques soit atteintes.

Pour les deux cas théoriques de validation, λ_{S_Ei} et T_{repair_i} sont fixés arbitrairement. Le taux de défaillance de S_E_i suit une distribution de weibull de paramètres de forme égal à 0.8, de paramètre d'échelle égal à 500 et de paramètre de temps égal à 0. Le temps de réparation pour le couple “S_E_i / S_D_i” ou “S_E_i / $S\_D_i^*$” (T_{repair_i}) suit une loi de distribution log normale de moyenne 50h de facteur d'erreur égal à 3. Les paramètres des architectures de diagnostic sont ensuite définis dans deux cas :

- La simulation 1, qui se place dans un cas optimiste, et qui suppose que l'architecture de diagnostic est "parfaite":
  - S_D_i ne génère aucune fausse alarme (pF=0),
  - Les temps de transmission sont fixés à des valeurs nulles (T_{T_TWN}=T_{T_EDN}=0),
  - Les réseaux de communication ne sont jamais perturbés (λ_{S_TWN}=λ_{S_EDN}=$10^{-10}h^{-1}$ afin que les perturbations n'aient jamais lieu durant la simulation et donc il n'y a pas d'erreur résiduelle P_{RE_TWN}=P_{RE_EDN}=0),
  - le temps T_A pour analyser une alarme est supposé nul,
  - la probabilité de déclencher une opération de maintenance est fixée à 1 (p_{MAINT}=1),

- La simulation 2, qui se place dans un cas pessimiste, et qui suppose que l'architecture de diagnostic est "mauvaise" :
  - S_D_i génère des fausses alarmes (pF=0.6),
  - Les temps de transmission sont fixés à des valeurs importantes (T_{T_TWN}=T_{T_EDN}=0.2h),
  - Le réseau de communication S_TWN est souvent perturbé (λ_{S_TWN}=$3.10^{-2}h^{-1}$ de telle manière que les perturbations ont lieu souvent pendant la durée de simulation avec des erreurs résiduelles p_{RE_TWN}=0.3). Etant donné que l'architecture EDCD implique un nouveau réseau de communication S_EDN, ce réseau est supposé être un réseau local industriel qui n'est jamais perturbé (λ_{S_EDN}=$10^{-10}h^{-1}$) mais où des erreurs résiduelles apparaissent (p_{RE_EDN}=0.3). Ceci afin de ne pas étudier l'influence du réseau sur l'architecture,
  - la probabilité de déclencher une opération de maintenance est fixée à 0.2 (p_{MAINT}=0.2),

	Entrées		Simulation 1: cas optimiste	Simulation 2: cas pessimiste
	Paramètre	**Type de distribution**	**Valeur**	**Valeur**
architecture RCD	λ_{S_Ei}	exponentielle	Paramètre de forme : 0.8 Paramètre d'échelle : 500 Paramètre de temps : 0	Paramètre de forme : 0.8 Paramètre d'échelle : 500 Paramètre de temps : 0
	λ_{S_TWN}	exponentielle	$10^{-10}h^{-1}$	$3.10^{-2}h^{-1}$
	μ_{S_TWN}	exponentielle	-	$10h^{-1}$
	p_{RE_TWN}	-	0	3.10^{-1}
	T_{T_TWN}	déterministe	0h	0.2h
	p_F	-	0	$6.\ 10^{-1}$
	T_A	déterministe	0h	0h
	p_{MAINT}	-	1	0.2
	T_{repair_i}	exponentielle	Moyenne : 50 h Facteur d'erreur : 3	Moyenne : 50 h Facteur d'erreur : 3
architecture EDCD	λ_{S_Ei}	exponentielle	Paramètre de forme : 0.8 Paramètre d'échelle : 500 Paramètre de temps : 0	Paramètre de forme : 0.8 Paramètre d'échelle : 500 Paramètre de temps : 0
	λ_{S_EDN}	exponentielle	$10^{-10}h^{-1}$	$10^{-10}h^{-1}$
	μ_{S_EDN}	exponentielle	-	$10h^{-1}$
	p_{RE_EDN}	-	0	3.10^{-1}
	T_{T_EDN}	déterministe	0h	0.2h
	λ_{S_TWN}	exponentielle	$10^{-10}h^{-1}$	$3.10^{-2}h^{-1}$
	μ_{S_TWN}	exponentielle	-	$10h^{-1}$
	p_{RE_TWN}	-	0	3.10^{-1}
	T_{T_TWN}	déterministe	0h	0.2h
	p_F	-	0	6.10^{-1}
	T_A	déterministe	0h	0h
	p_{MAINT}	-	1	0.2
	T_{repair_i}	exponentielle	Moyenne : 50 h Facteur d'erreur : 3	Moyenne : 50 h Facteur d'erreur : 3

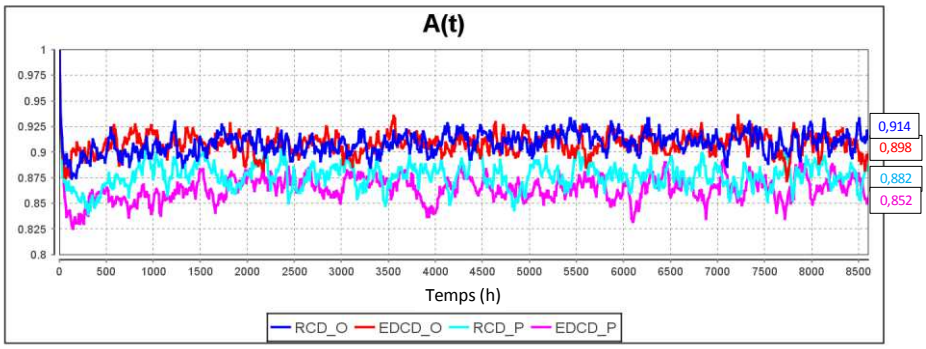
Tableau 7 : Paramètres et valeurs en entrée des modèles pour les cas optimiste et pessimiste

Pour les résultats des cas théoriques de validation, l'affichage des résultats sous forme d'histogramme est préférée (Figure 21 et Figure 22).

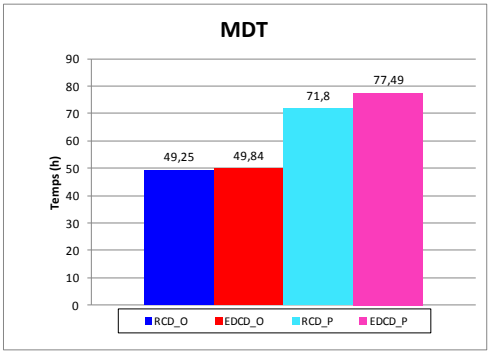
- Résultats

La Figure 21 illustre les résultats de simulation pour les cas pessimiste (x_P) et optimiste (x_O). En ce qui concerne la disponibilité, la valeur asymptotique converge pour les deux cas respectivement vers 0.914 pour RCD_O, 0.898 pour EDCD_O, 0.882 pour RCD_P et 0.852 pour EDCD_P (Figure 21a).

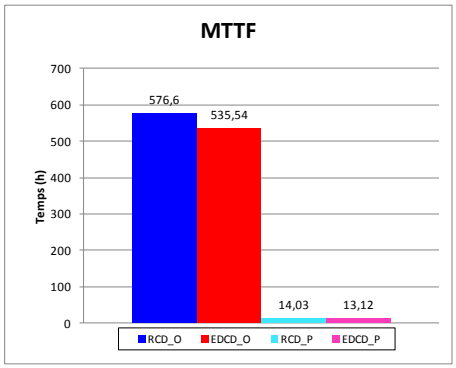
Quant à la MDT, sa valeur atteint 49.25h et 49.84h pour RCD et EDCD dans le cas optimiste et sa valeur atteint 71.8h et 77.49h pour le cas pessimiste (Figure 21b).



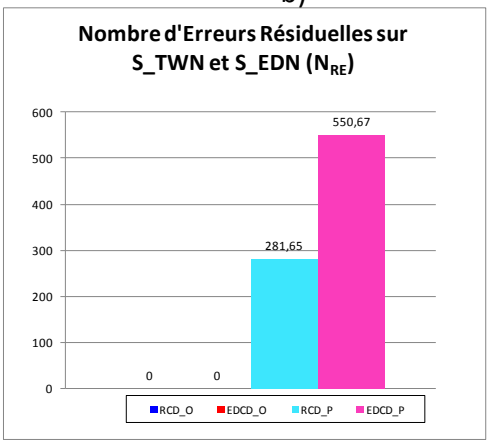
a)



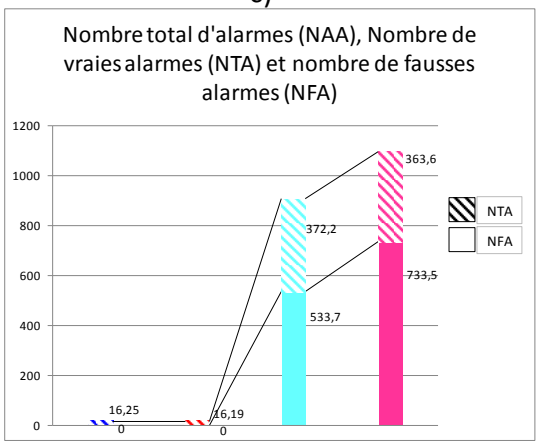
b)



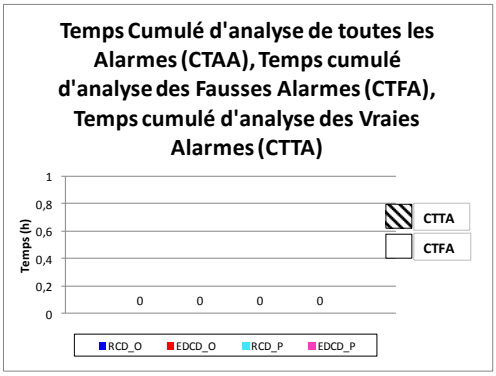
c)



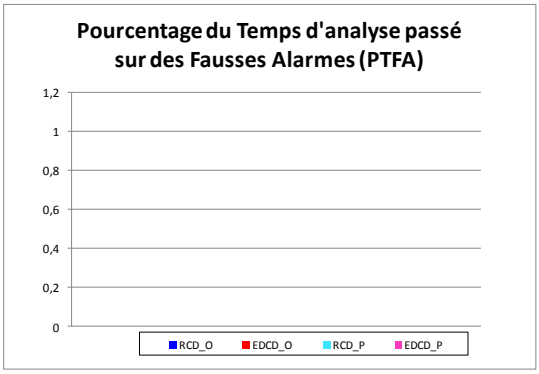
d)



e)



f)



g)

RCD_O : RCD, cas optimiste
EDCD_O : EDCD, cas optimiste
RCD_P : RCD, cas pessimiste
EDCD_P : EDCD, cas pessimiste

Figure 21 : Résultats de simulation pour les cas pessimiste et optimiste (n=1)

Le MTTF prend respectivement une valeur asymptotique de 576.6h et 535.34h pour RCD et EDCD dans le cas optimiste, tandis que le MTTF est respectivement égal à 14.03h et 13.22h pour RCD et EDCD dans le cas pessimiste (Figure 21c).

Le résultat pour l'indicateur N_{RE} (Figure 21d) prouve que le comportement du modèle est le comportement attendu : une valeur nulle pour le cas optimiste, puisque p_{RE_EDN} et p_{RE_TWN} sont fixés à la valeur 0. Pour le cas pessimiste, l'architecture EDCD atteint une valeur de 550.67 (Figure 21d), ce qui est environ le double de l'architecture RCD dans le cas pessimiste, puisque l' architecture EDCD intègre deux réseaux de communication et est de ce fait plus sensible aux erreurs de transmission.

Le nombre de fausses alarmes est nul (indicateur NFA) pour RCD_O et EDCD_O car pF est fixé à 0 (Figure 21e). Les indicateurs de temps cumulé d'analyse de fausses alarmes (CTFA) et de vraies alarmes (CTTA) sont aussi nuls (Figure 21f), du fait de la valeur d'entrée de T_A (égale à 0).

Le Pourcentage de Temps d'analyse passé à analyser des Fausses Alarmes ne peut être calculé (Figure 21g) dans tous les cas, car le Temps Cumulé d'analyse des Fausses Alarmes CTFA et le Temps Cumulé d'analyse des Vraies Alarmes CTTA n'ont pas été pris en compte en entrée du modèle (Figure 21f).

- Interprétation

L'objectif de cette étude est de valider l'aspect stochastique du modèle.

Dans le cas optimiste, les valeurs de tous les indicateurs décrivent des architectures performantes : disponibilité et fiabilités élevées (Figure 21a à c), pas d'erreur résiduelle (Figure 21d) ni de fausse alarme (Figure 21e et f). Les architectures RCD et EDCD sont très proches sur tous les indicateurs (Figure 21a à g). Ce résultat permet de valider le modèle pour ces valeurs d'entrée, car les défaillances dues aux réseaux communication (S_TWN et S_EDN) et aux systèmes de diagnostic (S_D/S_D*) ont été "désactivées".

Ces résultats de sortie permettent donc de valider le modèle et l'implantation dans les logiciels de simulation, dans le cas optimiste, pour ces valeurs d'entrée.

Dans le cas pessimiste, l'architecture EDCD est moins bonne que RCD sur tous les indicateurs (Figure 21a à g). En effet, un nombre important d'erreurs résiduelles a lieu en architecture EDCD (Figure 21d). Ce nombre, presque deux fois plus grand qu'en architecture RCD, implique davantage d'alarmes générées par le S_D (Figure 21e) et au final, davantage de temps perdu avant de commencer la réparation.

Ces résultats de sortie permettent donc de valider le modèle et l'implantation dans les logiciels de simulation, dans le cas pessimiste, pour ces valeurs d'entrée. Cette première simulation permet également de souligner que, en théorie dans le cas pessimiste, EDCD est moins réactive et implique davantage d'erreurs que RCD, du fait de la présence du second réseau de communication. Les résultats du cas pessimiste illustrent également que le réseau embarqué peut occuper une place

centrale : s'il est mauvais (probabilité d'erreur résiduelle élevée et taux de défaillance élevé), il peut conduire à une architecture EDCD aux performances réduites.

3.2.2. Second cas théorique de validation

En ce qui concerne le second cas théorique de validation, le même processus de validation est réalisé en utilisant trois couples "S_E_i / S_D_i" respectivement "S_E_i / $S\_D_i^*$" pour les architectures RCD et EDCD. De la même manière que précédemment, deux campagnes de simulation ont été réalisées pour une durée de 8760h avec les mêmes valeurs d'entrée (Tableau 7).

- Résultats

La Figure 22 donne les résultats de simulation pour les cas optimistes et pessimistes. En ce qui concerne la disponibilité (Figure 22a), la valeur asymptotique pour les deux cas converge respectivement vers 0.999 pour RCD_O, vers 0.997 pour EDCD_O, vers 0.964 pour RCD_P et vers 0.953 pour EDCD_P. En ce qui concerne la MDT (Figure 22b), sa valeur atteint 47.66h et 48.023h pour RCD et EDCD dans le cas optimiste et sa valeur atteint 57.44h et 72.5h pour le cas pessimiste.

Le MTTF prend respectivement une valeur asymptotique de 134.17h et 134.08h pour les cas optimistes RCD et EDCD, tandis que le MTTF est respectivement égal à 11.06h et 10.65h pour RCD et EDCD dans le cas pessimiste (Figure 22c).

De la même manière que pour le premier cas théorique de validation, étant donné que le but de cette étude est de valider l'aspect stochastique du modèle :

  - N_{RE} (Figure 22d) est nul pour le cas optimiste car p_{RE_EDN} et p_{RE_TWN} sont fixés à 0. Pour le cas pessimiste, la valeur de l'architecture EDCD (EDCD_P=662.98) est supérieure à l'architecture RCD (RCD_P=461.39) car EDCD a un second réseau de communication
  - les indicateurs NFA (Figure 22e) et CTFA (Figure 22f) sont égaux à 0 et PTFA ne peut être calculé (Figure 22g).

- Interprétation

Pour n=3, le modèle a le comportement attendu dans les cas optimistes et pessimistes et donne en sortie des résultats similaires aux résultats pour n=1 :

  - Les architectures RCD et EDCD sont très proches et performantes dans le cas optimiste (fiabilité et disponibilité élevées, aucune fausse alarme).
  - l'architecture EDCD est moins performante que l'architecture RCD dans le cas pessimiste.
  - Le réseau embarqué (S_EDN) occupe une place centrale dans l'architecture EDCD, car sa mauvaise performance (probabilité d'erreur résiduelle élevée et taux de défaillance élevé), peut diminuer les performances (fiabilité, disponibilité, nombre d'erreurs résiduelles) de l'architecture EDCD.
  - La faiblesse de l'architecture EDCD réside (en théorie) dans la présence de deux réseaux de communication, parce que l'indicateur N_{RE} est égal à 461.39 pour RCD_P, tandis qu'il atteint 662.98 pour EDCD_P (Figure 22d).

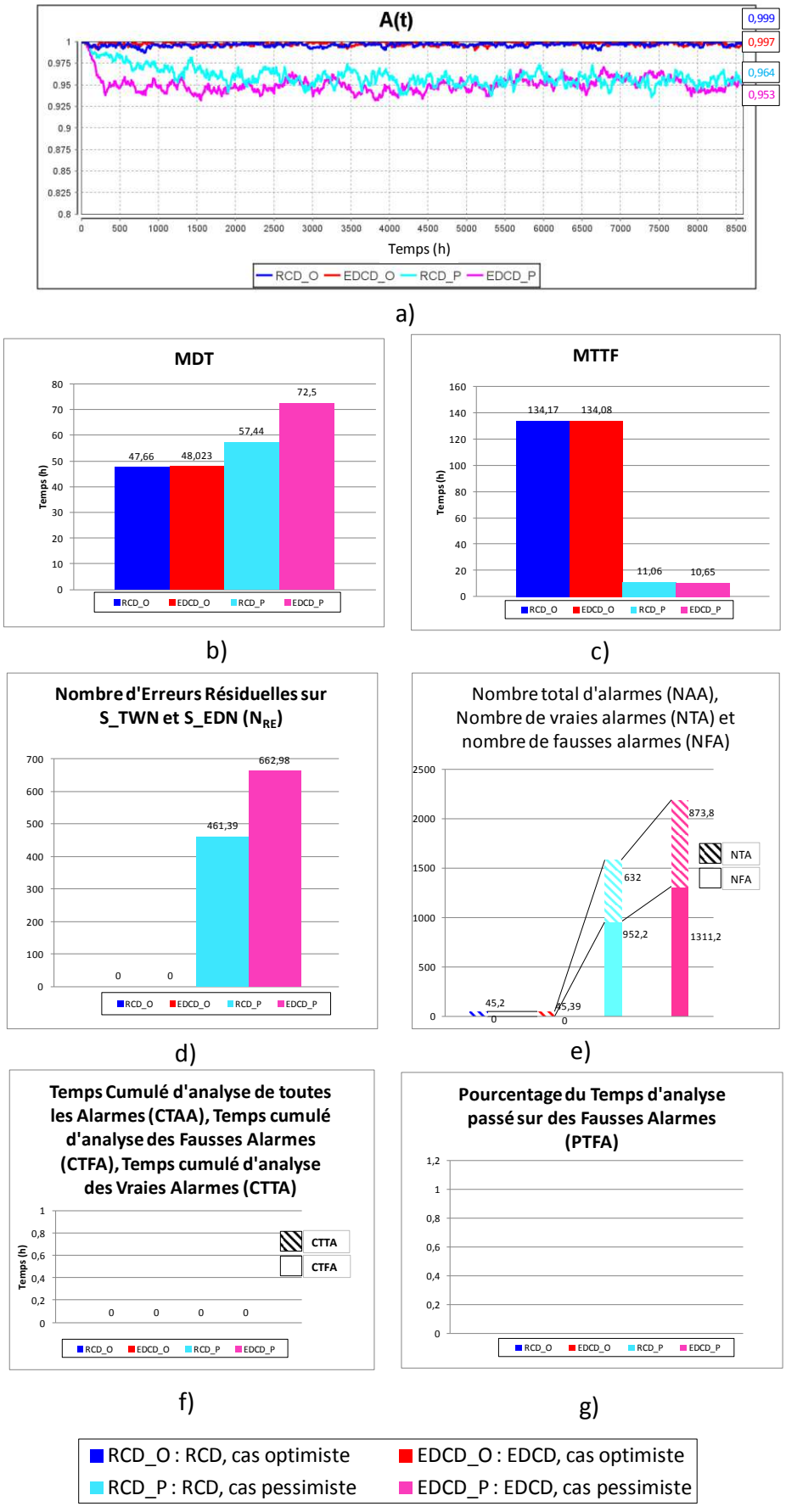


Figure 22 : Résultats de simulation pour les cas pessimiste et optimiste (n=3)

Conclusion

Ce chapitre a permis de présenter nos modèles et notre protocole d'évaluation de FMD pour la validation des modèles d'architectures de diagnostic présentées.

Dans un premier temps, notre choix d'une méthode d'évaluation de FMD a été présenté et justifié. Les caractéristiques des architectures de diagnostic (systèmes dynamiques et multi-états, partage de ressources communes) nous ont poussés à nous orienter vers les Réseaux de Petri Colorés (RdPC), que nous avons ensuite présentés. Parmi les méthodes de résolution, nous avons retenu la résolution par simulation, qui est généralement utilisée avec les Réseaux de Petri.

Dans un second temps, nous avons proposé des modèles RdPC pour les architectures RCD et EDCD du chapitre 2. Nous avons d'abord détaillé un modèle RdPC pour les réseaux de communication, qui occupent une place centrale dans ces architectures de diagnostic. Puis, nous avons proposé des modèles RdPC pour les architectures RCD et EDCD.

Un protocole, composé de critères d'évaluation des modèles et de cas de simulations (cas optimiste et cas pessimiste) a ensuite été présenté afin de valider ces modèles. De plus, les modèles RdPC ont été implémentés dans deux logiciels différents afin de s'assurer de l'absence d'erreurs de modélisation en comparant l'erreur entre les valeurs numériques atteintes par les critères et la cohérence des résultats.

Les modèles RdPC des architectures RCD et EDCD sont validés. Le chapitre suivant a pour objet de les exploiter et de les appliquer sur un cas réel ferroviaire.

Chapitre 4 : exploitation des modèles proposés

Chapitre 4 : exploitation des modèles proposés

Introduction

Ce chapitre a pour but d'exploiter les modèles RdPC (Réseaux de Pétri Colorés) proposés dans le chapitre précédent pour les architectures RCD et EDCD sur des cas réels.

Pour ce faire, la première partie présente l'application des modèles RdPC sur un cas réel proposé par Bombardier, où le système élémentaire retenu est un accès voyageurs. La distribution du taux de défaillance et la distribution des temps de réparation de ce système élémentaire sont d'abord estimées à partir du retour d'expérience, puis les paramètres des réseaux de communication et des systèmes de diagnostic sont quantifiés. Enfin, les résultats de l'architecture RCD sont comparés aux résultats de l'architecture EDCD, pour les paramètres d'entrée retenus.

La seconde partie de ce chapitre présente les études de sensibilité réalisées. Dans la première section, la sensibilité des architectures RCD et EDCD au taux de défaillance du réseau bord sol est présentée. Puis, la sensibilité de l'architecture EDCD au taux de défaillance du réseau embarqué pour le diagnostic est présentée. La sensibilité des architectures RCD et EDCD au temps de validation d'une alarme au système de diagnostic global est étudiée dans la troisième section. Enfin, les conclusions de ces trois études de sensibilité sont synthétisées dans la quatrième section.

1. Application sur un cas réel

Cette partie détaille l'application des modèles RdPC des architectures RCD et EDCD sur un cas réel proposé par Bombardier, où le système élémentaire est un accès voyageurs. Ce système élémentaire est présenté ci-dessous.

1.1.Présentation de l'accès voyageurs

Le système élémentaire étudié est un accès voyageurs (AV), situé à bord des matériels roulants (de type train périurbain) circulant sur le réseau ferré français de la région parisienne (Gandibleux et al.,2012b) (Turgis,2013). La localisation et la très forte urbanisation impliquent que le train soit soumis à une exploitation de type "métro", c'est-à-dire des arrêts fréquents et un flux important de passagers. Au final, l'accès voyageurs est soumis à une sollicitation accrue par rapport à un train de voyageurs de type train régional ou de type train à grande vitesse. Un train comporte plusieurs accès voyageurs (Figure 23), qui diffèrent s'ils sont montés sur les véhicules d'extrémité (équipés pour l'accessibilité des UFR (Unité en Fauteuil Roulant) et des PMR (Personne à Mobilité Réduite)), ou sur les véhicules intermédiaires (uniquement accès PMR).

L'accès voyageurs est composé de trois sous systèmes : un sous-système porte coulissante à deux vantaux, un sous-système marche mobile PMR (Personne à Mobilité Réduite) et un sous-système marche mobile UFR (Unité Fauteuil Roulant) (Figure 23).

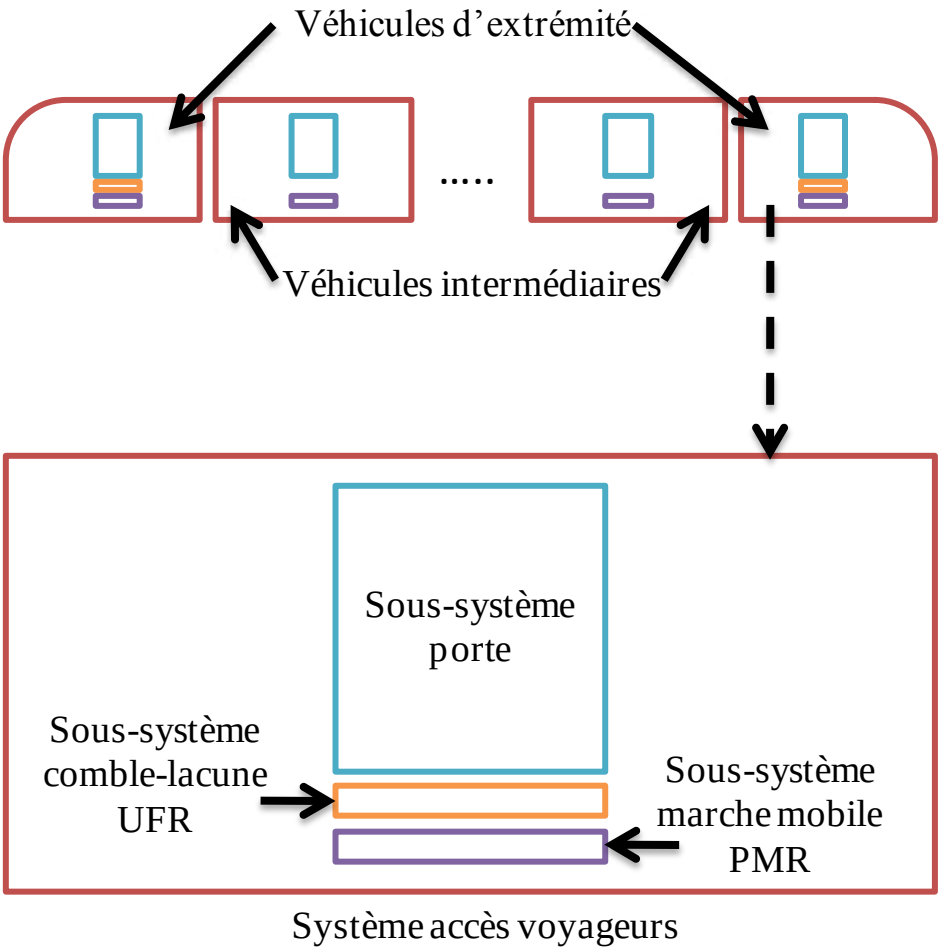
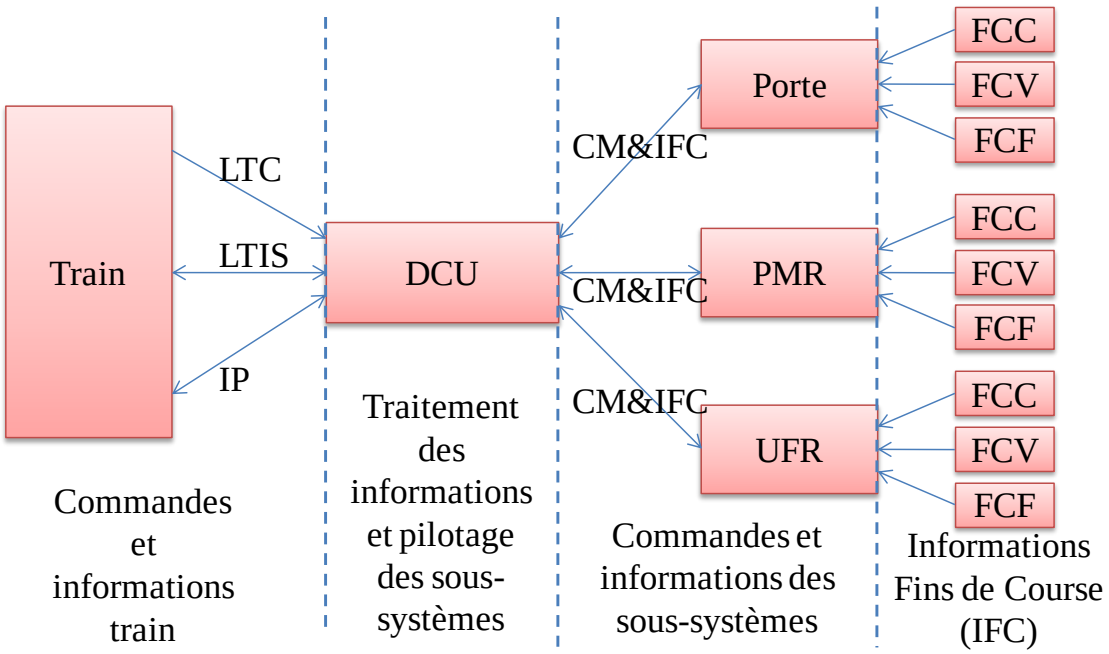


Figure 23 : **Disposition des sous-systèmes accès voyageurs sur les véhicules du train (Turgis,2013).**

Chaque sous-système est entraîné par des moteurs électriques. La demande d'ouverture est réalisée par un bouton poussoir et l'acquisition de l'état de la partie opérative est réalisée par des capteurs de fin de course (Figure 24). Les trois sous-systèmes (porte, marche mobile UFR et marche mobile PMR) sont pilotés par une unité électronique, appelée DCU, (de l'anglais "Door Control Unit"). Chaque accès voyageurs est ainsi équipé d'une DCU, qui assure l'interface entre les informations de pilotage envoyées depuis la cabine du conducteur et chaque sous-système (porte et marches mobiles) (Turgis,2013).



LTC : Ligne de train de commande	FCC : Fin de course de condamnation
LTIS : Ligne de train information de sécurité	FCV : Fin de course de verrouillage
IP : Connexion au réseau IP train	FCF : Fin de course de fermeture
	CM&IFC : Commande moteur et informations capteurs

Figure 24 : Diagramme de contrôle / commande des sous-systèmes accès voyageurs (Turgis,2013)

Le retour d'expérience issu de travaux de recherche précédents (Cauffriez et al.,2013)(Turgis et al.,2010) a permis de souligner la criticité de ce système élémentaire en termes de disponibilité. De ce fait, ce système élémentaire a également été retenu comme application pour le diagnostic dans le projet FUI SURFER (Gandibleux et al., 2011). Ce système élémentaire a été choisi pour l'application réelle de nos travaux.

1.2.Estimation des paramètres du système élémentaire d'accès voyageurs

Cette section présente l'estimation des lois de distributions de défaillance et de réparation d'un accès voyageurs, qui a été réalisée à partir des données disponibles grâce au retour d'expérience de Bombardier. Ce retour d'expérience comporte des informations, telles que la date de défaillance, la date de démarrage de l'opération de maintenance, le mode de défaillance, saisies à la main par le personnel de maintenance.

Les données disponibles concernent une population de 240 accès voyageurs. D'une part, ces systèmes élémentaires ont été mis en service chronologiquement les uns après les autres. D'autre part, le retour d'expérience étant élaboré à la main, les données ne sont pas toujours complètes et ne sont pas toujours valides. Par exemple, le mode de défaillance n'est pas toujours indiqué.

Pour nos travaux, le mode de défaillance le plus grave a été retenu. Celui-ci correspond à une perte de l'accès voyageurs pendant la mission du train. Ce mode de défaillance implique un retard de 5 minutes dans la mission du train (Gandibleux et al.,2012b).

Il est à noter que, étant donné leur nature confidentielle, les données de défaillance et de réparation présentées ci-dessous ne sont pas les données réelles mais se situent dans le même ordre de grandeur.

1.2.1. Estimation de la distribution de défaillance d'un accès voyageurs

Les données de défaillance proviennent de 240 accès voyageurs (AV), qui ont été progressivement mis en service. Les données ont été obtenues 18 mois après l'instant de mise en service en service du premier accès voyageurs ($t_{ser\ AV1}$), ce qui décrit une fenêtre d'observation de 18 mois sur l'ensemble de la population (Figure 25). Dans cette fenêtre d'observation, 91 accès voyageurs parmi les 240 ont connu leur première défaillance.

L'accès voyageur i entre en service à l'instant $t_{ser\ AVi}$ (Figure 25). Connaissant l'instant d'occurrence de la première défaillance de l'accès voyageurs i ($t_{def\ AVi}$), il est possible de calculer le temps avant la première défaillance de l'accès voyageurs i ($t_{tf\ AVi}$) par :

$$t_{tf\ AVi} = t_{def\ AVi} - t_{ser\ AVi} \tag{10}$$

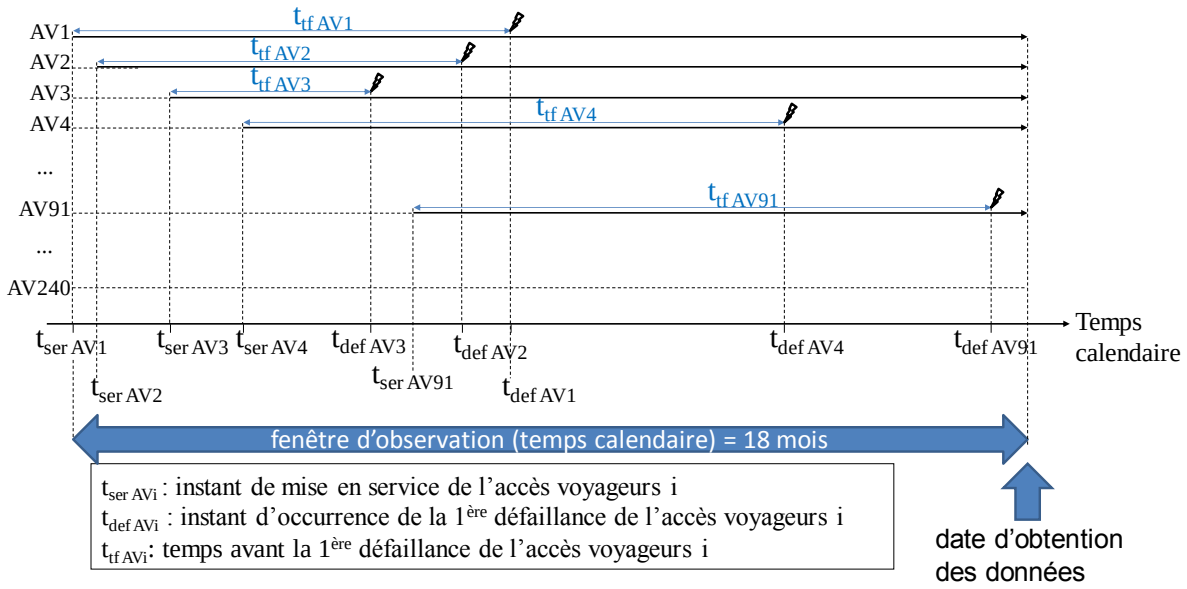


Figure 25 : Représentation graphique des données de défaillance des accès voyageurs avant hypothèse

Des modifications de conception peuvent avoir lieu entre l'instant de mise en service de l'AV1 ($t_{ser\ AV1}$) et l'AV240 ($t_{ser\ AV240}$). De plus, l'environnement extérieur (température, humidité), qui varie durant le temps calendaire considéré, est un des facteurs qui influencent le fonctionnement de l'AV (Turgis,2013). Les conditions de mesure des temps avant première défaillance peuvent donc varier d'un accès voyageur à l'autre. Enfin, la fenêtre d'observation constitue une partie de la phase de déverminage (ou phase de rodage) des accès voyageurs, car la fenêtre d'observation ne couvre que les 18 premiers mois de la vie de ces systèmes dont la durée de vie est prévue pour 40 ans.

Lorsque des processus de défaillances sont observés, plusieurs types d'essais existent (Procaccia et al.,2011). Les essais sont dits "censurés" lorsque ces essais se terminent après un temps t déterminé

(Procaccia et al.,2011). Dans notre travail, il s'agit de ce type d'essai, car la fenêtre d'observation est limitée par le temps d'observation disponible. Dans un premier temps, nous choisissons de ne pas prendre en compte l'effet de la censure sur les données, afin de simplifier l'estimation.

Dans ce cas, la distribution de défaillance d'un accès voyageurs peut être estimée en posant l'hypothèse d'une distribution de défaillance particulière et en traçant les données pour la distribution d'hypothèse (Kumamoto & Henley,1996). La proximité d'une droite avec les données indique alors si le modèle (la distribution de probabilité) représente raisonnablement les données (Kumamoto & Henley,1996).

Plusieurs distributions de probabilité (loi de Weibull, loi exponentielle, loi normale) ont été testées dans MATLAB pour représenter les données de défaillance. Par la méthode graphique, (Kumamoto & Henley,1996) précise que dans le cas d'une loi de Weibull, les données tracées dans le repère $\left[\ln(t) \quad \ln\left\{\ln\left(\frac{1}{1-F(t)}\right)\right\}\right]$ doivent former une ligne droite (Figure 26). Certains points, entourés en rouge, illustrent que la distribution de Weibull ne correspond pas parfaitement aux données et qu'une erreur existe, car ces points s'éloignent de la droite d'estimation.

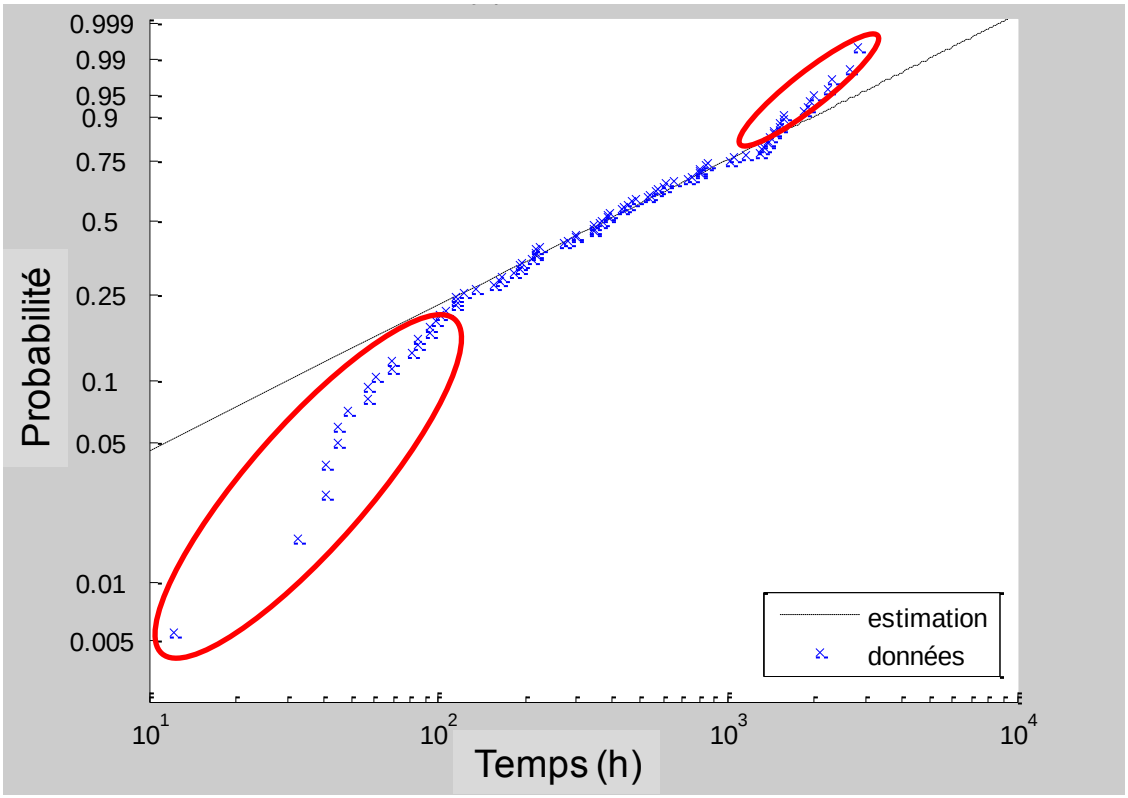


Figure 26 : Test des données de défaillance pour une distribution de Weibull

Pour estimer les paramètres des distributions de probabilité, plusieurs méthodes existent (méthode graphique, méthode par intervalle de confiance, méthode du maximum de vraisemblance) (Lyonnet,2006)(Procaccia et al.,2011) (voir annexe 1). Parmi ces méthodes, la méthode du maximum de vraisemblance a été utilisée pour estimer la valeur des paramètres, car elle peut être rapidement et facilement mise en œuvre dans le logiciel MATLAB. De plus, la méthode par intervalle de confiance a également été utilisée car elle permet de fixer un intervalle de confiance sur la précision des

paramètres estimés (voir annexe 1). Cette méthode peut aussi être mise en œuvre dans le logiciel MATLAB.

Le Tableau 8 présente, pour un intervalle de confiance à 90%, les résultats d'estimation des paramètres de la loi de Weibull : le paramètre de forme estimé ($\hat{\beta}$), la borne inférieure du paramètre de forme estimé ($\hat{\beta}_{inf}$), la borne supérieure du paramètre de forme estimé ($\hat{\beta}_{sup}$), le paramètre d'échelle estimé ($\hat{\eta}$), la borne inférieure du paramètre d'échelle estimé ($\hat{\eta}_{inf}$), la borne supérieure du paramètre d'échelle estimé ($\hat{\eta}_{sup}$). Pour simplifier les calculs, le paramètre de temps (γ) a été supposé nul comme indiqué dans (Kumamoto & Henley,1996).

Paramètre de forme	$\hat{\beta}_{inf}$	$\widehat{\boldsymbol{\beta}}$	$\hat{\beta}_{sup}$
	0.693796	**0.797816**	0.917431
Paramètre d'échelle	$\hat{\eta}_{inf}$	$\widehat{\boldsymbol{\eta}}$	$\hat{\eta}_{sup}$
	396.206	**497.367**	624.356

Tableau 8 : Résultats d'estimation des paramètres de la loi de Weibull pour les données présentées Figure 26

La distribution de Weibull a finalement été retenue pour deux raisons :

- D'une part le test des données de défaillance par la méthode graphique pour une distribution de Weibull est concluant avec MATLAB (Figure 26)
- D'autre part, les résultats d'estimation donnent β inférieur à 1. Ce résultat est représentatif de la réalité car les données proviennent de la phase de rodage, qui est caractérisée par un taux de défaillance décroissant (β inférieur à 1).

Au vu des résultats d'estimation, nous choisissons une distribution de Weibull de paramètres β=0.8 ; η=500 ; γ=0 pour la distribution de défaillance d'un accès voyageur.

1.2.2. Estimation de la distribution de réparation d'un accès voyageurs

Pour estimer la distribution des temps de réparation d'un accès voyageurs, les durées de toutes les réparations de tous les accès voyageurs sur la période de 18 mois ont été considérées. Un test a été réalisé par la méthode graphique (Figure 27). Parmi les distributions testées, la loi log normale a été retenue pour deux raisons :

- D'une part, parce que celle-ci peut convenir aux temps de réparation des accès voyageurs, car la plupart des points forment une droite, bien qu'une erreur existe (Figure 27).
- D'autre part, parce que la loi log normale est habituellement utilisée pour représenter les données de réparation (Villemeur,1991).

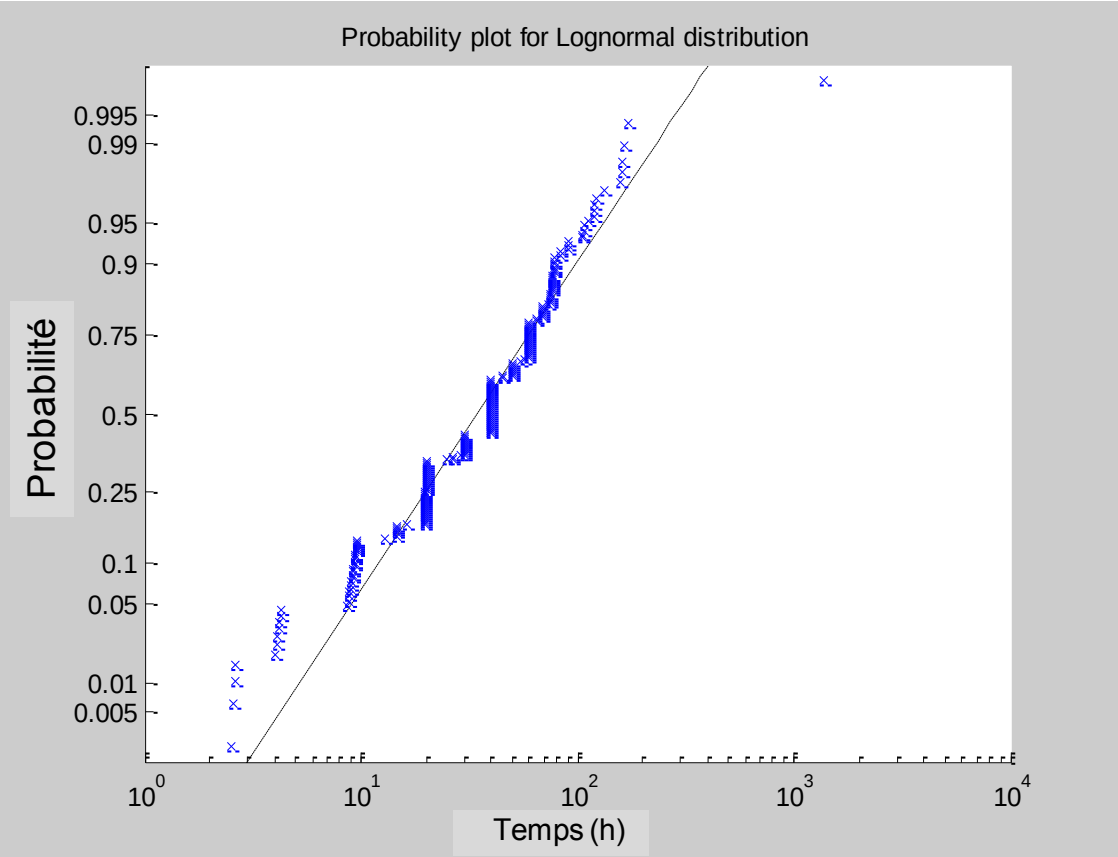


Figure 27 : Test des données de réparation pour une distribution log normale

De la même manière, les valeurs des paramètres sont estimées par la méthode du maximum de vraisemblance avec un intervalle de confiance (Procaccia et al.,2011). Le Tableau 9 présente, pour un intervalle de confiance à 90%, les résultats d'estimation des paramètres de la loi log normale : la moyenne estimée ($\hat{\mu}$), la borne inférieure de la moyenne estimée ($\hat{\mu}_{inf}$), la borne supérieure de la moyenne estimée ($\hat{\mu}_{sup}$), l'écart type estimé ($\hat{\sigma}$), la borne inférieure de l'écart type estimé ($\hat{\sigma}_{inf}$), la borne supérieure de l'écart type estimé ($\hat{\sigma}_{sup}$).

Moyenne	$\hat{\mu}_{inf}$	$\hat{\boldsymbol{\mu}}$	$\hat{\mu}_{sup}$
	3.498	**3.594**	3.690
Ecart type	$\hat{\sigma}_{inf}$	$\hat{\boldsymbol{\sigma}}$	$\hat{\sigma}_{sup}$
	0.729	**0.791**	0.865

Tableau 9 : Résultats d'estimation des paramètres de la loi log normale pour les données présentées Figure 27

Au vu des résultats d'estimation, une distribution log normale est retenue avec les paramètres μ=3,6 et σ=0.8. Par la suite, la distribution log normale sera caractérisée par (Villemeur,1991):

- la moyenne des temps de réparation, égale à $e^{(\mu+\frac{\sigma^2}{2})}$,

- et le facteur d'erreur, défini par $e^{1,645\sigma}$ pour un intervalle de confiance à 90%.

1.3.Quantification des paramètres des réseaux de communication

Les architectures de diagnostic RCD et EDCD comportent des réseaux de communication dont les paramètres sont quantifiés ci-dessous. La première sous-section traite les paramètres du réseau de communication bord sol S_TWN, tandis que la seconde sous-section traite les paramètres du réseau de communication embarqué pour le diagnostic S_EDN.

1.3.1. Réseau de communication bord sol (S_TWN)

Parmi les travaux recensés dans la littérature (chapitre 1), (Zimmermann & Hommel, 2005) étudie le réseau de communication bord sol GSM-R, qui est le GSM (Global System for Mobile communications) utilisé dans le transport ferroviaire. Les taux de transition vers l'état de bon fonctionnement et vers l'état perturbé sont approchés par une analyse numérique et démontrent un système très perturbé (λ_{S_TWN} = 0.02719 s^{-1} et μ_{S_TWN} = 3.236 s^{-1}). Par la suite, λ_{S_TWN} sera choisi dans l'ordre de grandeur supérieur, car la valeur élevée de λ_{S_TWN} = 0.02719 s^{-1} conduit à un effondrement des architectures de diagnostic.

La quantification du temps de transmission (T_{T_TWN}) sur le réseau de communication bord sol GSM-R pour RCD et pour EDCD est réalisée à partir de la taille du message, obtenue à partir des spécifications fonctionnelles de l'architecture RCD chez Bombardier, et le débit du réseau de communication, obtenu dans la spécification fonctionnelle du GSM-R (UIC, 2006).

La probabilité d'erreur résiduelle des bits pour S_TWN (p_{RE_TWN}) est calculable à partir de la formule suivante, proposée au chapitre 3 :

$$p_{RE} = \frac{nombre\ de\ bits\ altérés\ en\ dépit\ des\ protocoles\ de\ détection/correction}{nombre\ total\ de\ bits\ transmis} \quad (11)$$

Par la suite, une valeur de p_{RE_TWN} égale à 10^{-3} sera retenue pour l'étude.

1.3.2. Réseau de diagnostic embarqué (S_EDN)

Une démarche similaire est appliquée pour quantifier les paramètres du réseau de diagnostic embarqué S_EDN. Cependant, cette thèse se déroule pendant la phase de conception de l'architecture EDCD. Les paramètres de S_EDN ont donc été calculés à partir de prévisions sur la taille des messages et le choix de technologie du réseau de diagnostic embarqué.

La technologie choisie pour S_EDN est le réseau CAN (Controller Area Network) (ISO 11898-1,2003)(IEC61375, 2012). Le temps de transmission sur S_EDN (T_{T_EDN}) est donc déterminé à partir de la taille du message à transmettre par un système de diagnostic local haut niveau (S_Di*) et du débit du réseau CAN.

Pour le CAN, (CIA,2013) spécifie que la probabilité d'erreur résiduelle pour un message (ici p_{RE_EDN}) atteint 4,7.10^{-11}. Pour l'application réelle, nous choisissons une hypothèse moins optimiste (p_{RE_EDN} = 10^{-6}).

Les hypothèses sur les taux de défaillance et de reprise du réseau CAN sont fixées comme suit. Nous supposons qu'un réseau local industriel filaire comme le CAN est moins perturbé qu'un réseau de télécommunication de type GSM-R, donc λ_{S_EDN} = 10^{-5} h^{-1}. De même, le taux de reprise du réseau de

diagnostic embarqué est supposé au moins aussi bon voire meilleur que le taux de reprise du réseau de communication bord sol. Un choix pessimiste nous amène à fixer $\mu_{S\_TWN} = \mu_{S\_EDN}$.

1.4.Quantification des paramètres des systèmes de diagnostic

Le délai de validation d'une alarme / d'un diagnostic (T_A) au système de diagnostic global (S_GD) et la probabilité de déclencher une opération de maintenance (p_{MAINT}) sont quantifiés selon le retour d'expérience de Bombardier pour l'architecture RCD et selon des prévisions pour l'architecture EDCD.

En architecture RCD, le délai d'analyse et de validation d'une alarme peut atteindre 6h, tandis qu'en architecture EDCD, les premiers résultats de mise en œuvre du diagnostic haut niveau permettent de raccourcir T_A, qui peut atteindre au maximum 1h (Le Mortellec et al.,2013).

Concernant la probabilité de déclencher une opération de maintenance (p_{MAINT}), l'importante quantité de données brutes et d'alarmes à traiter dans l'architecture RCD provoque chez le personnel de maintenance des difficultés à localiser l'origine de la défaillance. De ce fait, une réparation n'est déclenchée que dans un cas sur deux (p_{MAINT} = 0.5). En architecture EDCD, la mise en œuvre du diagnostic haut niveau permet d'identifier la liste de composants à l'origine de la défaillance. La probabilité de déclencher une opération de maintenance est donc améliorée (p_{MAINT} = 0.9).

En architecture RCD, la probabilité de fausse alarme p_F des systèmes de diagnostic local (S_D), a été estimée à partir des informations du retour d'expérience. Le résultat exact ne pouvant être communiqué pour des raisons de confidentialité, p_F est fixée à une valeur représentative de la réalité (p_F=0.2). Du fait de l'expérimentation en cours depuis Juillet 2013 dans le cadre du projet FUI SURFER, il n'existe pas encore de retour d'expérience sur la mise en œuvre d'un système de diagnostic haut niveau (S_D_i*) en architecture EDCD. Cependant, l'architecture EDCD doit être globalement au moins aussi bonne que l'architecture RCD. Ces raisons nous ont conduites à fixer p_F en architecture EDCD à une valeur pessimiste, c'est-à-dire la même valeur qu'en architecture RCD.

1.5.Synthèse des données d'entrée

Les paramètres estimés et quantifiés précédemment sont synthétisés dans le Tableau 10. Ces données sont mises en entrées des modèles dans la section suivante.

	Paramètre	Type de distribution	Valeur
Architecture RCD	λ_{S_Ei}	weibull	Paramètre de forme : 0.8 Paramètre d'échelle : 500 Paramètre de temps : 0
	λ_{S_TWN}	exponentielle	$2.719\ 10^{-2}\ h^{-1}$
	μ_{S_TWN}	exponentielle	$3.3236\ h^{-1}$
	p_{RE_TWN}	-	10^{-3}
	T_{T_TWN}	déterministe	$8.33\ 10^{-3}$h
	p_F	-	0.2
	T_A	déterministe	6 h
	p_{MAINT}	-	0.5
	T_{repair_i}	log normale	Moyenne des temps de réparation : 50 h Facteur d'erreur : 3
Architecture EDCD	λ_{S_Ei}	weibull	Paramètre de forme : 0.8 Paramètre d'échelle : 500 Paramètre de temps : 0
	λ_{S_EDN}	exponentielle	$10^{-5}\ h^{-1}$
	μ_{S_EDN}	exponentielle	$3.3236\ h^{-1}$
	p_{RE_EDN}	-	10^{-6}
	T_{T_EDN}	déterministe	$5.333\ 10^{-5}$ h
	λ_{S_TWN}	exponentielle	$2.719\ 10^{-2}\ h^{-1}$
	μ_{S_TWN}	exponentielle	$3.3236\ h^{-1}$
	p_{RE_TWN}	-	10^{-3}
	T_{T_TWN}	déterministe	$8.33\ 10^{-3}$ h
	p_F	-	0.2
	T_A	déterministe	1 h
	p_{MAINT}	-	0.9
	T_{repair_i}	log normale	Moyenne des temps de réparation: 50 h Facteur d'erreur : 3

Tableau 10 : Paramètres et valeurs en entrée des modèles pour le cas réel

1.6.Simulations

Un système élémentaire (n=1) puis trois systèmes élémentaires S_Ei (n=3) en architecture RCD et EDCD ont été simulés. Ci-après, les résultats pour 1000 histoires sont présentés. La durée de chaque histoire est fixée à 8760h.

1.6.1. Un système élémentaire S_Ei (n=1)

Pour cette simulation, une architecture de diagnostic est considérée :

- fiable si le système élémentaire (S_E), le système de diagnostic local bas/haut niveau (S_D / S_D*) et tous les réseaux de communication sont dans l'état de bon fonctionnement,
- disponible si le système élémentaire (S_E) et le système de diagnostic local associé (S_D / S_D*) sont dans l'état de bon fonctionnement.

La Figure 28 illustre les résultats associés.

- Résultats

Pour ces valeurs spécifiques, l'architecture EDCD est plus disponible que l'architecture RCD (Figure 28a et b), car la disponibilité asymptotique des architectures RCD et EDCD atteint respectivement 0,890 et 0,912. De même, la MDT de l'architecture RCD (63,33h) est supérieure à la MDT de l'architecture EDCD (50,88h).

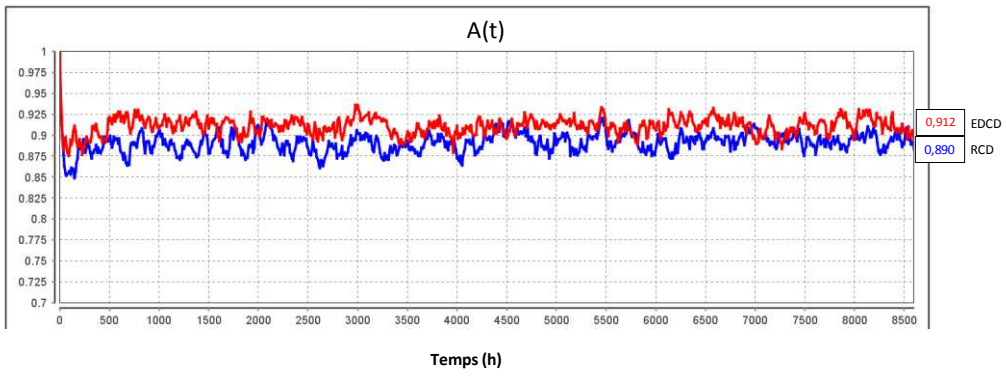
La fiabilité de l'architecture EDCD (MTTF=23,98h) est diminuée de 6,7% par rapport à la fiabilité de l'architecture RCD (MTTF=25,70h) (Figure 28c). Concernant l'indicateur N_{RE} (Figure 28d), l'architecture EDCD (N_{RE}=0,375) connait légèrement plus (0,001) d'erreurs résiduelles que l'architecture RCD (N_{RE}=0,374), mais cet indicateur n'est pas significatif car le nombre d'erreurs résiduelles est inférieur à 1.

Le nombre d'alarmes fausses (NFA) ou vraies (NTA) et les temps cumulé d'analyse des fausses alarmes (CTFA) et des vraies alarmes (CTTA) de l'architecture EDCD (Figure 28e et f) sont réduits de 44% par rapport à l'architecture RCD. De même, PTFA en architecture EDCD est réduit par rapport à l'architecture RCD (Figure 28g).

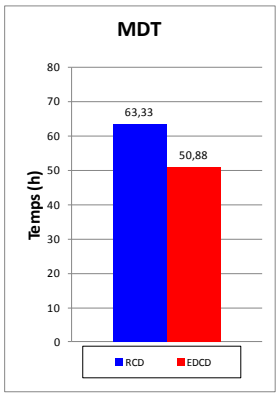
L'architecture EDCD traite 15,25 défaillances du S_E tandis que l'architecture RCD traite 14,98 défaillances du S_E sur la même durée de simulation. Pour ces valeurs, l'architecture EDCD est légèrement plus réactive que l'architecture RCD sur la même durée de simulation.

- Interprétation

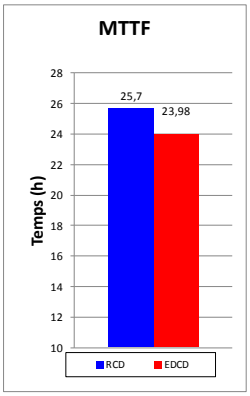
Il est possible de calculer le nombre moyen de vraies alarmes traitées par défaillance du système élémentaire S_E (Tableau 11). En architecture EDCD, ce nombre atteint 1,11, tandis qu'il atteint 2,03 en architecture RCD. L'architecture EDCD conduit donc à générer une quantité de données inférieure, par défaillance de S_E, par rapport à l'architecture RCD.



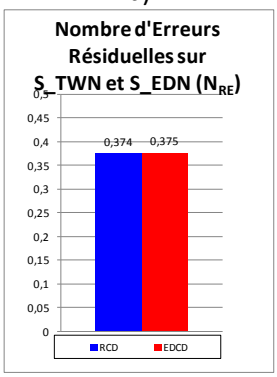
a)



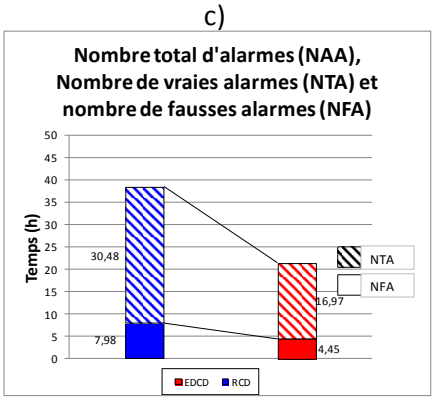
b)



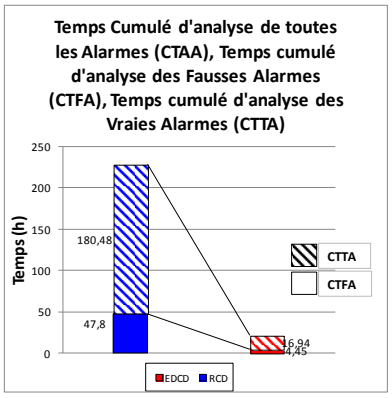
c)



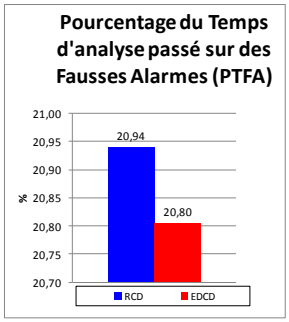
d)



e)



f)



g)

Figure 28 : Résultats de simulation pour le cas réel (n=1).

	Nombre de défaillances du S_E	Nombre de vraies alarmes traitées par l'architecture de diagnostic	Nombre moyen de vraies alarmes traitées par défaillances du S_E
Architecture RCD	14,98	30,48	30,48 / 14,98 = 2,03
Architecture EDCD	15,25	16,97	15,25 / 16,97 = 1,11

Tableau 11 : calcul du nombre moyen de vraies alarmes traitées par défaillance du système élémentaire S_E

En plus de générer moins de données par défaillance, l'architecture EDCD conduit à une meilleure répartition du temps cumulé d'analyse de toutes les alarmes (CTAA) que l'architecture RCD. Cette dernière interprétation est visible sur les temps cumulés CTFA et CTTA, et sur PTFA (Figure 28f et g) : CTFA et CTTA, et PTFA sont inférieurs en architecture EDCD par rapport à l'architecture RCD.

Cette interprétation ne pouvait être réalisée au chapitre 3, dans les cas théoriques de validation, car le délai de validation T_A était alors fixé à 0h.

1.6.2. Trois systèmes élémentaires S_Ei (n=3)

Pour cette simulation, une architecture de diagnostic est considérée :

- fiable si tous les systèmes élémentaires (S_E), tous les systèmes de diagnostic local bas/haut niveau (S_Di / S_Di*) et tous les réseaux de communication sont dans l'état de bon fonctionnement,
- disponible si au moins un couple système élémentaire (S_Ei) et le système de diagnostic local associé (S_Di / S_Di*) sont dans l'état de bon fonctionnement.

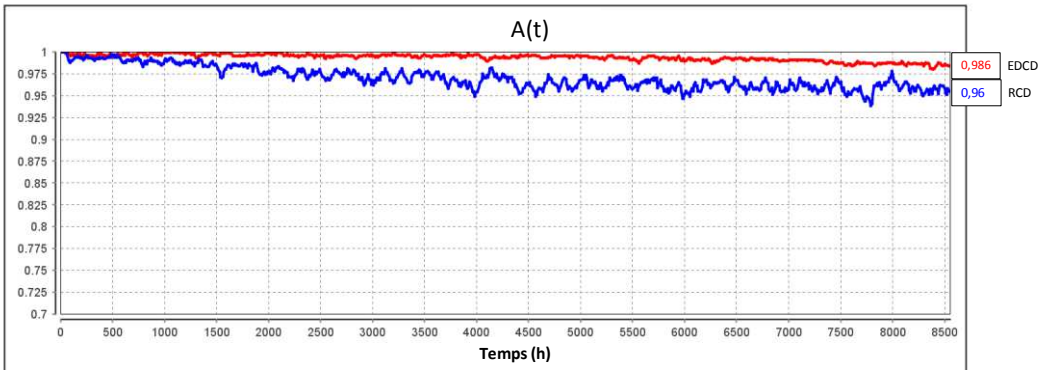
Les résultats sont illustrés Figure 29 et sont similaires aux résultats de la sous-section 1.6.1.

- Résultats

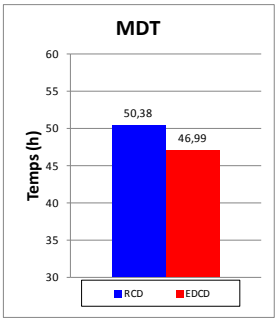
La phase transitoire des courbes de disponibilité est représentée Figure 29a. Cette Figure illustre que, pour ces valeurs spécifiques, la disponibilité de l'architecture EDCD atteint une valeur asymptotique de 0,986 et sa MDT (Figure 29b) atteint 46,99h. L'architecture RCD quant à elle atteint une valeur asymptotique de 0,960 et une MDT de 50,38h. L'architecture EDCD est donc plus disponible que l'architecture RCD.

Par ailleurs, la fiabilité de l'architecture EDCD est légèrement plus faible que la fiabilité de l'architecture RCD, parce que la valeur du MTTF pour EDCD est de 12,46h pour EDCD tandis que la valeur du MTTF pour RCD est égale à 13,7h (Figure 29c).

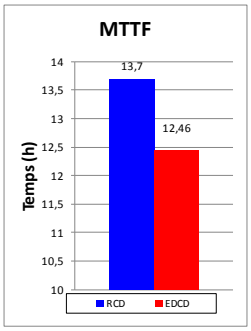
Concernant l'indicateur N_{RE} (Figure 29d), une augmentation du nombre d'erreurs résiduelles se produit en passant de l'architecture RCD (N_{RE} = 0,468) à l'architecture EDCD (N_{RE} = 0,965). Cependant N_{RE} reste inférieur à l'unité dans les deux cas.



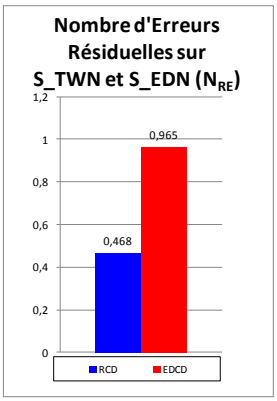
a)



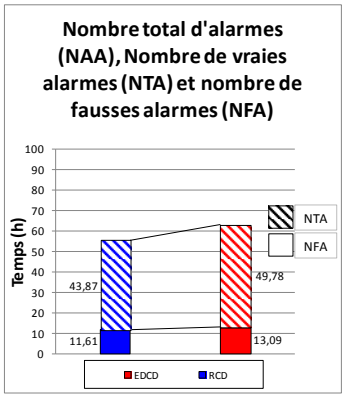
b)



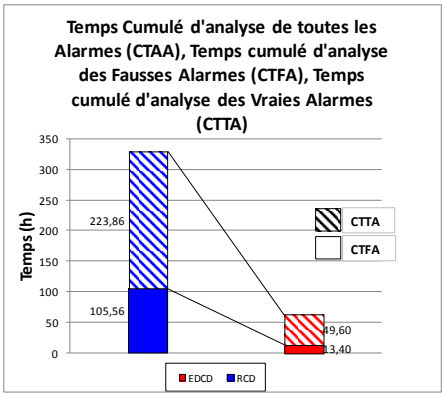
c)



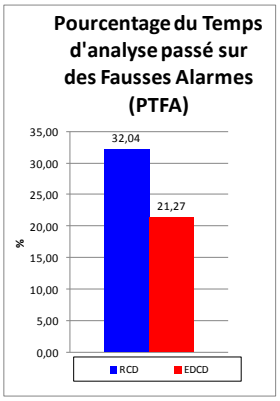
d)



e)



f)



g)

Figure 29 : Résultats de simulation pour le cas réel (n=3).

Le nombre d'alarmes fausses(NFA) ou vraies (NTA) de l'architecture EDCD (Figure 29e) est supérieur par rapport à l'architecture RCD. Cependant, le temps cumulé d'analyse des fausses alarmes (CTFA) et des vraies alarmes (CTTA) de l'architecture EDCD est inférieur par rapport à l'architecture RCD (Figure 29g).

- Interprétation

La faible perte de fiabilité (9%) de l'architecture EDCD par rapport à l'architecture RCD s'explique par l'ajout d'un second réseau de communication (S_EDN).

En architecture EDCD, au plus une erreur résiduelle a lieu pendant le temps de simulation (8760h) (Figure 29d). L'ajout d'un second réseau de communication provoque donc une augmentation du nombre d'erreurs résiduelles par rapport à l'architecture RCD. Cependant, les conséquences sur les performances de l'architecture EDCD sont limitées et le nombre d'erreurs résiduelles est inférieur à 1.

Les indicateurs CTTA, CTFA et PTFA confirment et illustrent que l'architecture EDCD conduit à une réduction de la durée moyenne d'indisponibilité MDT, parce que le concept de "diagnostic haut niveau" réduit la quantité de données à traiter et permet d'analyser plus vite ces dernières. T_A est donc réduit ce qui permet de réduire le temps cumulé passé à analyser des fausses alarmes. D'autre part, en fin de simulation, un compteur indique que l'architecture EDCD a traité en moyenne 44,72 défaillances de S_Ei, tandis que l'architecture RCD n'a traité que 22,69 défaillances sur la même durée de simulation.

2. Etudes de sensibilité

Cette partie présente les résultats et interprétations pour plusieurs études de sensibilité. Trois systèmes élémentaires sont considérés et les mêmes hypothèses de fiabilité et de disponibilité sont fixées.

Dans la première section, la sensibilité des architectures RCD et EDCD au taux de défaillance du réseau bord sol S_TWN est étudiée. Dans la deuxième section, la sensibilité de l'architecture EDCD au taux de défaillance du réseau embarqué pour le diagnostic S_EDN est présentée. Puis, la sensibilité des architectures RCD et EDCD au temps de validation d'une alarme au système de diagnostic global est étudiée dans la troisième section. Enfin, les conclusions de ces études de sensibilité sont synthétisées dans la quatrième section.

2.1. Sensibilité des architectures RCD et EDCD au taux de défaillance du réseau de communication bord sol (S_TWN)

Le manque de données sur le taux de défaillance du réseau de communication bord sol (S_TWN) (une seule valeur dans (Zimmermann & Hommel,2005)) nous a poussé à réaliser une étude de sensibilité des architectures RCD et EDCD à ce paramètre. Le taux de défaillance du réseau de communication bord sol est fixé successivement aux valeurs du Tableau 12. Les autres paramètres des modèles RdPC sont fixés aux valeurs synthétisées dans le Tableau 10. Il est également rappelé que, selon nos hypothèses de modélisation pour le réseau de communication, lorsqu'un message est affecté par une erreur résiduelle, le réseau de communication ne fait aucune retransmission.

Les résultats associés à ces entrées sont illustrés par la Figure 30.

Il convient de remarquer que les indicateurs de la Figure 30 prennent plusieurs valeurs pour l'étude de sensibilité à λ_{S_TWN}, avec $\lambda_{S\_TWN} \in [10^{-5} ; 10^{-1}]$. Pour cette raison, la représentation sous forme de courbe est préférée à la représentation sous forme d'histogramme dans la suite de notre travail.

Paramètre	Type de distribution	Valeurs				
λ_{S_TWN}	exponentielle	$10^{-5}\,h^{-1}$	$10^{-4}\,h^{-1}$	$10^{-3}\,h^{-1}$	$10^{-2}\,h^{-1}$	$10^{-1}\,h^{-1}$

Tableau 12 : Valeurs utilisées pour l'étude sensibilité à λ_{S_TWN}

- Résultats

Lorsque λ_{S_TWN} passe de $10^{-5}\,h^{-1}$ à $10^{-1}\,h^{-1}$ (Figure 30a), la disponibilité asymptotique de l'architecture EDCD est peu influencée (0,986 à 0,984), tandis que la disponibilité asymptotique de l'architecture RCD diminue de 0,965 à 0,958. Le fait de multiplier λ_{S_TWN} par 10 000 implique en sortie une diminution de la disponibilité asymptotique de 0,36% pour l'architecture EDCD et de 0,7 % pour l'architecture RCD. Cette observation est également illustrée par la MDT (Figure 30b), qui augmente de 46,00h à 47,59h pour EDCD et de 47,12h à 59,36h pour RCD lorsque λ_{S_TWN} passe de $10^{-5}\,h^{-1}$ à $10^{-1}\,h^{-1}$. La disponibilité des architectures RCD et EDCD diminue donc avec l'augmentation de λ_{S_TWN}.

Le MTTF de l'architecture RCD passe de 69,17h à 4,54h avec l'augmentation de λ_{S_TWN} de $10^{-5}\,h^{-1}$ à $10^{-1}\,h^{-1}$ (Figure 30c). Le MTTF de l'architecture EDCD passe de 66,66h à 4,47h avec l'augmentation de λ_{S_TWN} de $10^{-5}\,h^{-1}$ à $10^{-1}\,h^{-1}$ (Figure 30c). Dans chaque cas, l'augmentation de λ_{S_TWN} de $10^{-5}\,h^{-1}$ à $10^{-1}\,h^{-1}$ implique une perte de fiabilité de 93%.

L'augmentation du taux de défaillance du réseau de communication bord sol (S_TWN) ne conduit ni à une augmentation ni à une réduction des autres indicateurs (Figure 30d à g).

- Interprétation

  - Les résultats de cette étude de sensibilité illustrent comment la présence d'un réseau de communication bord sol de plus en plus perturbé conduit à une réduction de la fiabilité et de la disponibilité de l'architecture. Au contraire, un réseau bord sol très peu perturbé ($\lambda_{S\_TWN} = 10^{-5}\,h^{-1}$) conduit à une augmentation de la fiabilité et de la disponibilité.

  - L'augmentation de λ_{S_TWN} correspond à un état perturbé, où le réseau bord sol ne peut pas transmettre de message. Cela implique un temps d'attente supplémentaire avant qu'un message ne puisse être transmis et, au final, qu'une réparation puisse démarrer.

  - Toutefois, cette étude de sensibilité démontre que les résultats restent similaires aux résultats du cas réel Bombardier :
    - L'architecture EDCD est plus disponible que l'architecture RCD (Figure 30a).
    - L'architecture EDCD est moins fiable que l'architecture RCD (Figure 30c).
    - Le nombre d'erreurs résiduelles N_{RE}, pour les valeurs d'entrée de p_{RE_TWN} et p_{RE_EDN}, n'est pas significatif dans les deux cas : N_{RE} est sensiblement inférieur ou égal à l'unité (Figure 30d).

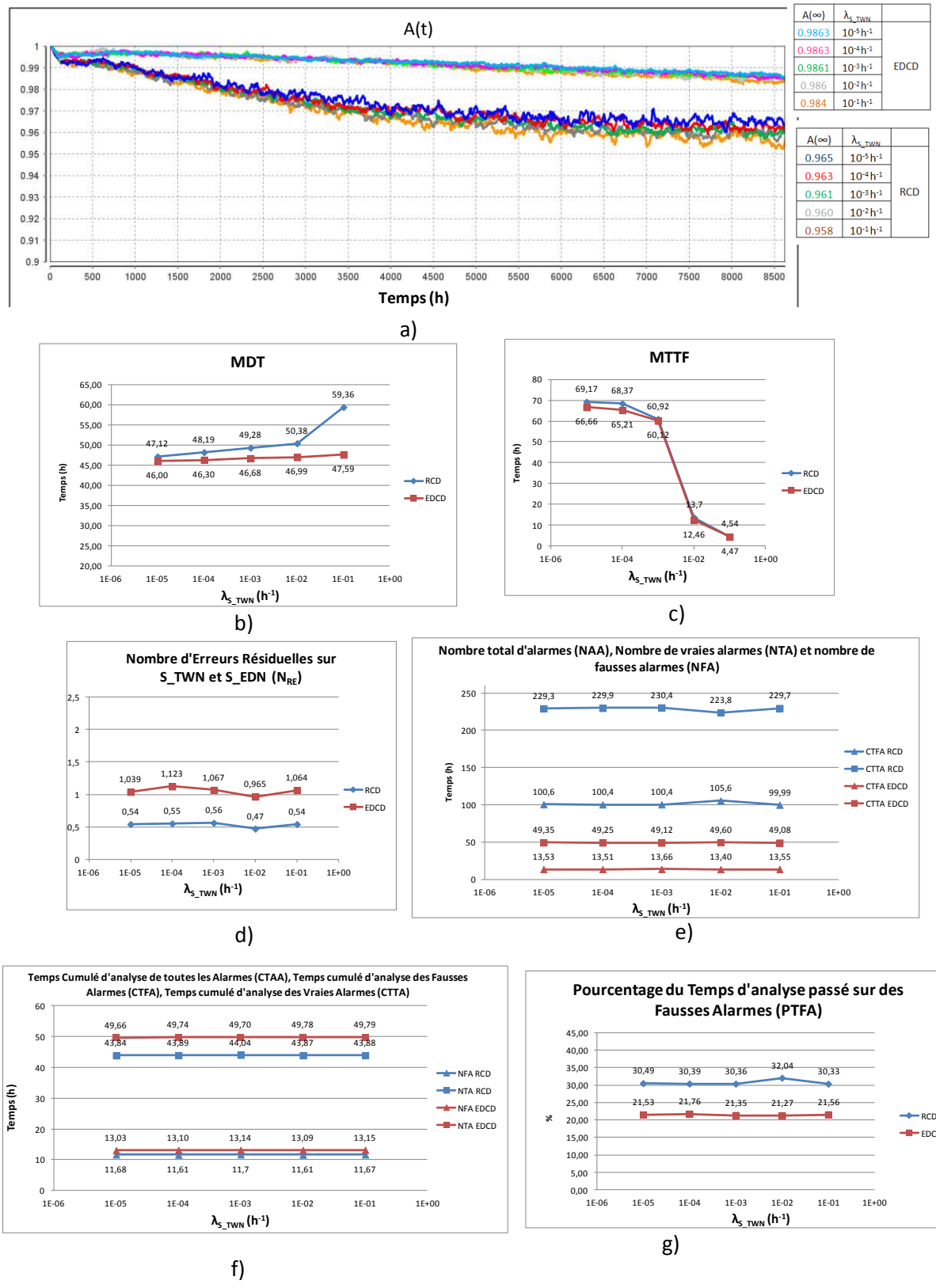


Figure 30 : Résultats de simulation pour l'étude de sensibilité au taux de défaillance du réseau de communication bord sol (n=3).

2.2.Sensibilité de l'architecture EDCD au taux de défaillance du réseau embarqué pour le diagnostic (S_EDN)

De la même manière que dans la section 2.1, le manque de données sur le taux de défaillance du réseau embarqué pour le diagnostic (λ_{S_EDN}) nous a poussés à réaliser une étude de sensibilité de l'architecture EDCD à ce paramètre.

Pour réaliser cette étude de sensibilité, la valeur du taux de défaillance du réseau embarqué pour le diagnostic (λ_{S_EDN}) est fixée successivement à des valeurs supérieures ou égales à $10^{-5}\,h^{-1}$ (Tableau 13), qui reflètent un réseau de communication de plus en plus perturbé. A noter que les valeurs des indicateurs restent sensiblement égales aux valeurs prises pour $\lambda_{S\_EDN}=10^{-5}\ h^{-1}$, lorsque λ_{S_EDN} est strictement inférieur à $10^{-5}\,h^{-1}$.

Paramètre	Type de distribution	Valeurs				
λ_{S_EDN}	exponentielle	$10^{-5}\,h^{-1}$	$10^{-4}\,h^{-1}$	$10^{-3}\,h^{-1}$	$10^{-2}\,h^{-1}$	$10^{-1}\,h^{-1}$

Tableau 13 : Valeurs utilisées pour l'étude sensibilité à λ_{S_EDN}

Les autres paramètres des modèles RdPC sont fixés aux valeurs synthétisées dans le Tableau 10. Les résultats associés à ces entrées sont illustrés à la Figure 31.

- Résultats

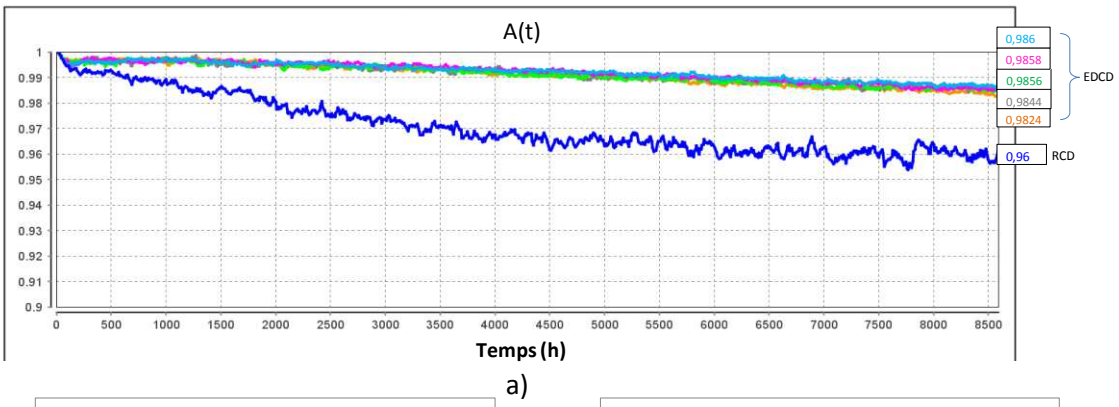
Lorsque λ_{S_EDN} passe de $10^{-5}\ h^{-1}$ à $10^{-1}\ h^{-1}$ (Figure 31a), la disponibilité asymptotique de l'architecture EDCD est peu influencée. En effet, il existe une faible diminution (de 0,986 à 0,982), qui ne représente qu'une perte de 0,3%. Cette observation est également illustrée par la MDT (Figure 31b), qui augmente de 46,99h à 47,70h lorsque λ_{S_EDN} passe de $10^{-5}\ h^{-1}$ à $10^{-1}\ h^{-1}$. La disponibilité de l'architecture EDCD diminue donc avec l'augmentation de λ_{S_EDN}.

Le MTTF de l'architecture EDCD passe de 12,46h à 3,65h avec l'augmentation de λ_{S_EDN} de $10^{-5}\,h^{-1}$ à $10^{-1}\ h^{-1}$ (Figure 31c). Ce résultat illustre comment la présence d'un réseau de communication de plus en plus perturbé conduit à une réduction de la fiabilité : multiplier λ_{S_EDN} par 10 000 implique une perte de fiabilité d'environ 71%.

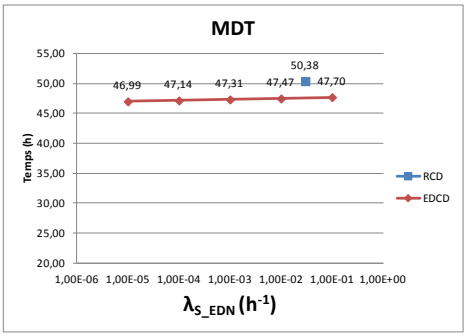
L'augmentation du taux de défaillance du réseau embarqué influence sensiblement l'indicateur N_{RE} (Figure 31d) : celui-ci reste égal à 1,038 en moyenne avec un écart type de 0,04 (Tableau 14), compte tenu des valeurs d'entrée.

Le nombre d'alarmes total (NAA), fausses(NFA) ou vraies (NTA) de l'architecture EDCD (Figure 31e) est supérieur par rapport à l'architecture RCD ; le temps cumulé d'analyse de toutes les alarmes (CTAA), des fausses alarmes (CTFA) et des vraies alarmes (CTTA) de l'architecture EDCD est inférieur à l'architecture RCD (Figure 31f).

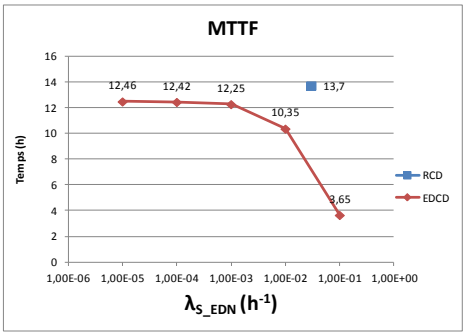
Le Pourcentage de Temps d'analyse passé à analyser des Fausses Alarmes (PTFA, Figure 31g) est plus faible en architecture EDCD qu'en en architecture RCD.



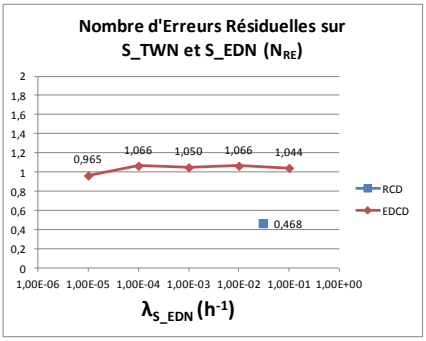
a)



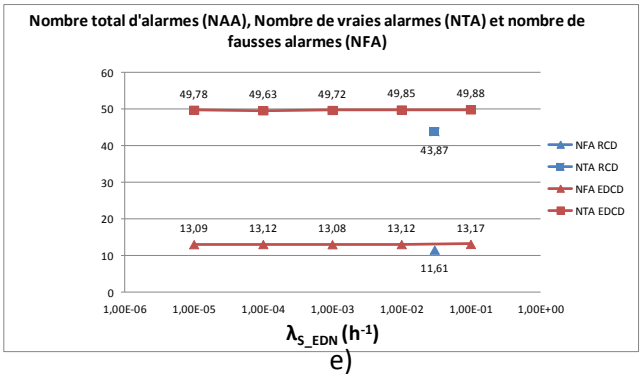
b)



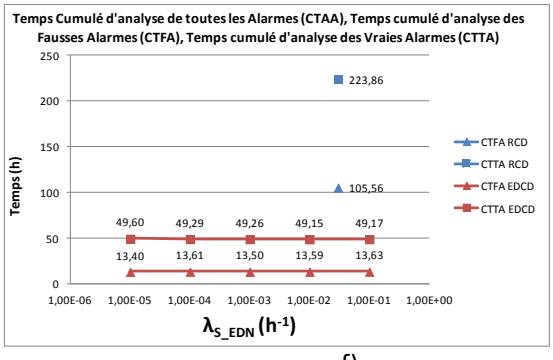
c)



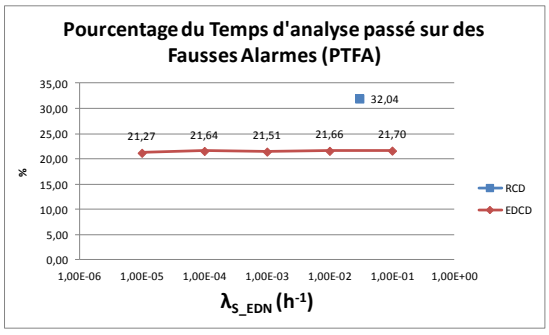
d)



e)



f)



g)

Figure 31 : Résultats de simulation pour l'étude de sensibilité au taux de défaillance du réseau de communication pour le diagnostic embarqué (n=3).

De même, l'augmentation du taux de défaillance du réseau embarqué n'influence pas les indicateurs de temps cumulé d'analyse des alarmes (CTFA, CTAA et CTA, Figure 31f), de nombre d'alarmes (NAA, NTA, et NFA, Figure 31e) et de pourcentage de temps passé à analyser des fausses alarmes (PTFA, Figure 31g). Les moyennes et écarts type des valeurs de ces indicateurs ont été calculés pour l'architecture EDCD et sont reportés au Tableau 14.

Indicateur	Moyenne	Ecart type
N_{RE}	1,038	0,0421
CTFA	13,546 h	0,0938
CTTA	49,292 h	0,1815
CTAA	62,837 h	0,1096
NFA	13,115	0,0329
NTA	49,772	0,1015
NAA	62,887	0,1218
PTFA	21,557	0,1739

Tableau 14 : Moyennes et écarts types des valeurs des indicateurs N_{RE} , CTFA, CTAA, CTA, NAA, NTA, NFA et PTFA pour l'étude de sensibilité de l'architecture EDCD à λ_{S_EDN}

- Interprétation

Pour les valeurs choisies, l'étude de sensibilité permet d'illustrer l'influence du taux de défaillance du réseau embarqué pour le diagnostic (λ_{S_EDN}) sur la FMD de l'architecture EDCD. Des conclusions similaires à l'étude de sensibilité précédente peuvent être tirées.

L'augmentation de λ_{S_EDN} conduit à une réduction de disponibilité de l'architecture EDCD, car la transmission de message ne peut démarrer. La fiabilité est également réduite, car selon nos hypothèses (voir section 1.6.2), une architecture de diagnostic n'est pas fiable, lorsqu'une perturbation a lieu sur le(s) réseau(x) de communication.

Les temps cumulés d'analyse des fausses alarmes (CTFA) et des vraies alarmes (CTTA) de l'architecture EDCD sont inférieurs à l'architecture RCD (Figure 31f). Cette observation est également visible sur PTFA (Figure 31g), qui illustre que l'architecture EDCD conduit à une meilleure répartition du temps d'analyse de toutes les alarmes (CTAA).

2.3.Sensibilité des architectures RCD et EDCD au temps de validation d'une alarme au système de diagnostic global (S_GD)

Pour réaliser cette étude de sensibilité, le temps de validation d'une alarme au système de diagnostic global (T_A) est fixé à des valeurs comprises entre 1h et 10h (Tableau 15). De la même manière que précédemment, les autres paramètres des modèles RdPC sont fixés aux valeurs synthétisées dans le Tableau 10.

Paramètre	Type de distribution	Valeurs			
T_A	déterministe	1h	2h	6h	10h

Tableau 15 : Valeurs utilisées pour l'étude de sensibilité à T_A

- Résultats

Les résultats associés à ces entrées, présentés Figure 32, illustrent l'influence du temps de validation d'une alarme au niveau du système de diagnostic global (T_A) sur la FMD de l'architecture EDCD.

En architecture EDCD, la disponibilité asymptotique est peu influencée (Figure 32a) : multiplier T_A par 10 implique en sortie une diminution de 0,32%. Cette observation est également illustrée par la MDT, qui augmente de 46,99h à 47,63h (Figure 32b). La diminution est plus importante en architecture RCD : la disponibilité asymptotique passe de 0,969 à 0,950 et le MDT évolue de 48,96h à 64,68h lorsque T_A passe de 1h à 10h. Multiplier T_A par 10 implique en sortie une diminution de 1,91% de la disponibilité asymptotique. La disponibilité des architectures RCD et EDCD diminue donc avec l'augmentation de T_A.

L'augmentation du temps de validation d'une alarme au système de diagnostic global n'influence pas les indicateurs MTTF et N_{RE} (Figure 32c et Figure 32d). Les valeurs moyennes et écart types de ces indicateurs ont été calculés (Tableau 16). Le nombre d'erreurs résiduelles en architecture EDCD reste supérieur au nombre d'erreurs résiduelles en architecture RCD du fait de la présence de S_EDN.

	Architecture RCD		Architecture EDCD	
Indicateur	Moyenne	Ecart type	Moyenne	Ecart type
MTTF	13,497h	0,258	12,652h	0,131
N_{RE}	0,539	0,04	1,008	0,033

Tableau 16 : Moyennes et écarts types des valeurs des indicateurs MTTF et N_{RE}, pour l'étude de sensibilité des architectures à T_A

Le nombre total d'alarmes (NAA), de fausses alarmes (NFA) et de vraies alarmes (NTA) augmente avec la diminution de T_A (Figure 32e). Ce résultat est interprété au paragraphe suivant. L'indicateur NFA diminue respectivement de 13,09 à 12,61 en architecture EDCD et de 11,80 à 11,47 en architecture RCD. De même, l'indicateur NTA diminue respectivement de 49,78 à 47,63 en architecture EDCD et de 44,46 à 43,17 en en architecture RCD.

L'augmentation du paramètre T_A est également visible sur les indicateurs de temps cumulé d'analyse de fausses alarmes (CTFA), de vraie alarme (CTTA), et de toutes les alarmes (CTA) (Figure 32f).

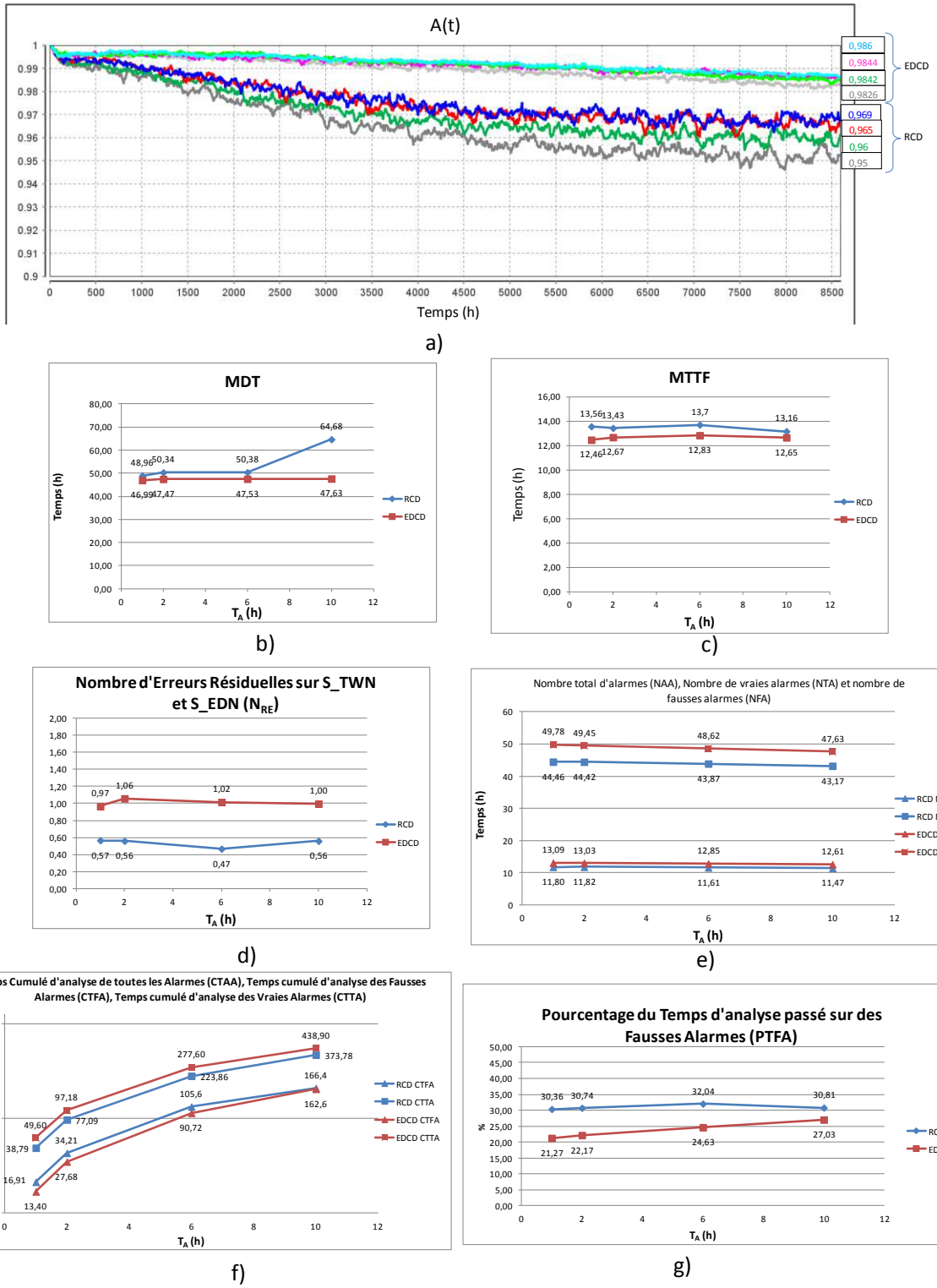


Figure 32 : Résultats de simulation pour l'étude de sensibilité au temps de validation d'une alarme au système de diagnostic global (n=3).

L'indicateur CTFA augmente de 49,60h à 438h en architecture EDCD et de 38,79h à 373h en architecture RCD. De même, l'indicateur CTTA augmente en architecture RCD de 16,91h à 166,4h et en architecture EDCD de 13,40h à 162,6h. Cependant, PTFA reste inférieur en architecture EDCD par rapport à l'architecture RCD.

- Interprétation

Pour les valeurs choisies, l'architecture EDCD conduit à une réduction du temps cumulé d'analyse des fausses alarmes CTFA et une augmentation du temps cumulé d'analyse des vraies alarmes CTTA, par rapport à l'architecture RCD, lorsque T_A varie de 1h à 10h.

A délai de validation égal (T_A), l'architecture EDCD étant plus réactive, elle a la possibilité (sur la même durée de simulation) de traiter un plus grand nombre de défaillances, et génère de ce fait un plus grand nombre de diagnostics avec validation (NTA) ou non (NFA) des alarmes.

Cette observation implique en sortie une amélioration de la disponibilité de l'architecture EDCD par rapport à l'architecture RCD.

2.4.Synthèse

Une comparaison semi-quantitative des indicateurs en sortie des modèles, basée sur les valeurs prises par les indicateurs pour les deux cas réels (n=1 et n=3 systèmes accès voyageurs) et pour les études de sensibilité (partie 2 de ce chapitre) est présentée au Tableau 17. Il est rappelé que les valeurs prises par les indicateurs sont fonction des paramètres d'entrée du Tableau 10.

Attribut	Indicateur	Architecture RCD	Architecture EDCD
Disponibilité	A(t)	+	++
Fiabilité	MTTF	++	+
Maintenabilité	MDT	+	++
Performance du diagnostic global	CTFA	+	++
	CTTA	+	++
	CTAA	+	++
	PTFA	+	++
Performance des réseaux de communication	N_{RE}	++	+
Réactivité	NFA	+	++
	NTA	+	++
	NAA	+	++
Globalement		**2/11**	**9/11**

Légende :	+	pire
	++	meilleur

Tableau 17 : Comparaison semi-quantitative des valeurs des indicateurs des architectures RCD et EDCD (valeurs du cas réel et des trois études de sensibilité)

Le Tableau 17 permet d'observer que l'architecture EDCD est meilleure que l'architecture RCD sur neuf indicateurs parmi onze. En effet, le concept de diagnostic haut niveau utilisé par l'architecture EDCD permet de réduire le temps d'analyse d'une alarme au diagnostic global (T_A) et de déclencher une réparation plus rapidement qu'en architecture RCD. La disponibilité de EDCD est donc améliorée, ce qui est illustré par de meilleures valeurs de A(t) et de MDT. D'autre part, le temps cumulé passé à analyser les vraies et fausses alarmes (CTTA et CTFA) est également réduit.

Le Tableau 17 illustre également une perte de l'architecture EDCD par rapport à l'architecture RCD en termes de fiabilité (MTTF) et d'erreurs résiduelles sur les réseaux de communication (N_{RE}). Cependant, la perte de fiabilité par rapport à RCD est limitée (perte inférieure à 10% dans tous les cas). En ce qui concerne les erreurs résiduelles, N_{RE} en architecture EDCD reste inférieur à 1 dans tous les cas. De plus, les conséquences d'une erreur résiduelle sont limitées : le message est inhibé mais le système diagnostic local peut être réarmé et un nouveau diagnostic local peut être généré et retransmis. Par conséquent, l'architecture EDCD peut donc être considérée comme globalement équivalente à l'architecture RCD en termes de fiabilité et d'erreurs résiduelles sur les réseaux de communication.

L'architecture EDCD est soit meilleure que l'architecture RCD soit équivalente à l'architecture RCD, pour les valeurs choisies et pour les hypothèses retenues. L'architecture EDCD développée dans le contexte industriel est donc conforme au principe GAMAB préconisé dans le transport ferroviaire français.

Conclusion

Dans ce chapitre, les modèles RdPC des architectures de diagnostic ont été appliquées sur un cas réel.

Dans un premier temps, l'estimation des paramètres du système élémentaire réel, un accès voyageurs ferroviaire, a été réalisée. Puis, les paramètres des réseaux de communication et des systèmes de diagnostic des architectures RCD et EDCD ont été estimés.

Pour l'application réelle, l'objectif est de comparer l'architecture RCD à l'architecture EDCD. Pour les paramètres d'entrée, les résultats illustrent que l'architecture EDCD est GAMAB (globalement au moins aussi bonne) que l'architecture RCD. L'architecture EDCD permet de gagner en disponibilité et sur le temps d'analyse des fausses alarmes, mais réduit la fiabilité (exprimée par le MTTF) de 10%. L'architecture EDCD est aussi plus réactive que l'architecture RCD car elle permet de traiter plus de défaillances de systèmes élémentaires que l'architecture RCD sur la même période.

Dans un second temps, la sensibilité des architectures RCD et EDCD au taux de défaillance des réseaux de communication et au temps de validation d'une alarme au système de diagnostic global a été étudiée. Pour les valeurs utilisées, les résultats illustrent que l'augmentation du taux de défaillance d'un réseau de communication conduit à une réduction de disponibilité et de fiabilité de l'architecture. D'autre part, l'augmentation du temps de validation d'une alarme au système de diagnostic global conduit également à une réduction de la disponibilité des architectures RCD et EDCD et une augmentation du temps cumulé passé à analyser des fausses alarmes. Lors de ces deux études, l'architecture EDCD reste néanmoins plus disponible que l'architecture RCD.

Chapitre 5 : Conclusion générale et perspectives

1. Conclusion

La mission d'un système de transport ferroviaire consiste à transporter des passagers ou des marchandises d'un point de départ à un point d'arrivée, selon un temps de parcours établi et selon des conditions de sécurité optimales. Pour optimiser le coût du système de transport ferroviaire, une des solutions consiste à optimiser les coûts de maintenance. Cette solution peut être mise en œuvre en améliorant les architectures de diagnostic. Pour justifier l'intérêt d'une nouvelle architecture de diagnostic, il faut que le niveau de disponibilité atteint par la nouvelle architecture de diagnostic soit au moins aussi bon que l'architecture de diagnostic actuelle. Cependant, l'amélioration du diagnostic passe par l'emploi de systèmes intelligents et complexes, ce qui rend l'évaluation de la FMD plus difficile.

Les travaux présentés dans ce mémoire de thèse ont eu pour objectif de proposer des modèles et un protocole de validation, afin d'évaluer la FMD d'architectures de diagnostic. La tâche est rendue difficile, du fait de la complexité inhérente aux systèmes intelligents, du fait de l'emploi de réseaux de communication et du fait de la grande taille d'un système de transport ferroviaire. Ces observations ont orienté le choix vers une modélisation par réseaux de Petri colorés et une résolution par simulation de Monte Carlo.

Dans le premier chapitre, les notions de fiabilité, maintenabilité et disponibilité et les notions de base en surveillance, diagnostic et gestion de faute non-intrusive ont été rappelées afin de donner un cadre théorique aux travaux réalisés. Puis, quelques travaux de la littérature, proches de la problématique d'évaluation FMD d'architectures de diagnostic ont été recensés. Les formalismes utilisés sont essentiellement dynamiques, tels que les Réseaux de Pétri et les chaînes de Markov.

Nous avons détaillé au deuxième chapitre le contexte général et les objectifs de ces travaux de thèse, qui se déroulent dans le cadre du projet FUI SURFER. Les architectures de diagnostic du transport ferroviaire ont été présentées, afin de mieux cerner les limites de la situation actuelle et la solution envisagée dans le projet FUI SURFER. Cette présentation a permis de poser les objectifs de cette thèse, qui consiste à modéliser et évaluer d'un point de vue FMD des architectures de diagnostic. Enfin, les verrous scientifiques de cette thèse liés aux réseaux de communication, au diagnostic et à la sûreté de fonctionnement ont été identifiés et détaillés.

Le troisième chapitre a permis de justifier et de présenter le formalisme retenu, à savoir les Réseaux de Pétri colorés associés à la résolution par simulation de Monte Carlo. Dans un premier temps, nous avons proposé un modèle générique pour les réseaux de communication, qui occupent une place centrale dans les architectures de diagnostic du transport ferroviaire. Puis nous avons proposé des modèles en Réseaux de Pétri colorés des architectures de diagnostic RCD et EDCD. Les modèles proposés ont ensuite été validés par un protocole de validation composé de cas pessimistes et optimistes, qui a permis de valider les résultats en sortie du modèle pour les valeurs d'entrée retenues.

Le quatrième chapitre a permis d'appliquer les modèles proposés sur un cas réel proposé par Bombardier, coordinateur du projet FUI SURFER, où les systèmes élémentaires sont des accès voyageurs. Dans un premier temps, la distribution du taux de défaillance et la distribution des temps de réparation d'un accès voyageurs ont été estimées à partir du retour d'expérience fourni par Bombardier. Puis, les paramètres des réseaux de communication et des systèmes de diagnostic ont été estimés. Les résultats pour l'application réelle ont été obtenus. Devant le manque de données concernant le réseau de communication bord sol et le réseau de communication embarqué pour le diagnostic, nous avons décidé de réaliser des études de sensibilité afin d'étudier l'influence de leur dysfonctionnement sur la FMD des architectures de diagnostic.

La conclusion générale de ce travail, synthétisant les objectifs et les résultats est exposée ci-dessous :

- Ces travaux de thèse permettent de proposer une méthodologie d'évaluation de FMD pour comparer des architectures de diagnostic basée sur les RdPC et la simulation de Monte Carlo.
- En ce qui concerne l'application réelle proposée par Bombardier : les résultats illustrent, pour les valeurs d'entrée, que passer de l'architecture RCD à de l'architecture EDCD permet un gain en disponibilité et conduit à une meilleure répartition du temps d'analyse des alarmes. Cependant, l'ajout d'un réseau supplémentaire dégrade légèrement la fiabilité et augmente le nombre d'erreurs résiduelles. Cet inconvénient peut être perçu comme négligeable car l'objectif est d'avoir une architecture EDCD au moins aussi disponible que RCD et car le nombre d'erreur résiduelle est faible. Nous pouvons donc affirmer que, selon les hypothèses et les valeurs d'entrées retenues, l'architecture de diagnostic type EDCD développée dans le projet FUI SURFER est conforme au principe GAMAB.
- Les études de sensibilité réalisées illustrent, pour les hypothèses et les valeurs d'entrée retenues, que les réseaux de communication ont un effet très faible sur la disponibilité. Cependant, l'effet est plus important sur la fiabilité des architectures de diagnostic.

2. Perspectives

Des perspectives aux travaux réalisés ont été identifiées tant sur le plan scientifique que sur le plan industriel.

2.1.Perspectives scientifiques

Deux perspectives scientifiques aux travaux réalisés ont été identifiées. Elles concernent l'enrichissement des modèles proposés pour les architectures de diagnostic et la proposition d'une méthodologie d'évaluation FMD a priori.

2.1.1. Enrichissement des modèles proposés

Les modèles RdPC des architectures de diagnostic RCD et EDCD ont été proposés et sont basés sur des hypothèses. Ainsi, la politique de maintenance modélisée est la maintenance corrective. Au diagnostic global, les alarmes ou diagnostics sont traités et toutes les fausses alarmes sont détectées. Les systèmes élémentaires sont caractérisés par deux états. Les systèmes élémentaires sont indépendants. Ci-dessous, des perspectives sont proposées.

- Enrichissement des modèles des systèmes élémentaires

Nous avons posé l'hypothèse qu'un système élémentaire ne peut être que dans deux états (état de marche ou état de panne). De plus, la transition depuis l'état de marche vers l'état de panne est la conséquence d'une défaillance soudaine. Cette hypothèse permet des simplifications dans les modèles RdPC des architectures de diagnostic. Cependant, d'autres types de défaillances peuvent se produire, comme les défaillances progressives (Zwingelstein,1995). Il est alors possible de distinguer des états de fonctionnement dégradé, c'est-à-dire des états de fonctionnement où le service fournit par le système élémentaire est limité.

De plus, le système élémentaire accès voyageurs est un cas particulier, dans le sens où il peut être considéré comme un système fonctionnant à la sollicitation (Gandibleux et al.,2012b). Par exemple, lorsque le train roule, les portes sont fermées et verrouillées. Quand le train arrive à une station donnée, l'accès voyageurs est sollicité en ouverture, si un voyageur appuie sur le bouton d'ouverture de porte. Cette observation ouvre la voie à l'intégration de modèles de systèmes élémentaires fonctionnant à la sollicitation (Meshkat et al.,2002).

- Modélisation des défaillances de cause commune

Les systèmes élémentaires, soumis au diagnostic, ont été considérés comme indépendants et subissant des défaillances indépendantes. Or, l'hypothèse d'indépendance n'est pas toujours vérifiée dans la pratique (Kumamoto & Henley,1996). Dans le cas de plusieurs systèmes élémentaires de type accès voyageurs, il est possible d'identifier plusieurs éléments communs. Par exemple, la commande d'ouverture ou de fermeture des portes vient d'un seul signal, propagé par une ligne de train. Une défaillance sur la commande des portes peut provoquer une défaillance de cause commune sur l'ensemble des accès voyageurs du train. Cette perspective mérite également d'être explorée.

- Ajout de processus continus : fiabilité dynamique

Les systèmes élémentaires peuvent contenir des variables continues (par exemple une température, une pression). L'évolution du système dans différents états ou l'évolution de la loi de défaillance du système élémentaire peut être fonction de franchissement de seuils sur ces variables continues (cas

d'un équipement électronique refroidi par un ventilateur (Kermisch & Labeau,2000). Par exemple, la défaillance du ventilateur entraine une hausse de la température et un stress supplémentaire pour l'équipement électronique, ce qui modifie la loi de défaillance de l'équipement électronique. La modélisation de tels systèmes est habituellement réalisée par la "fiabilité dynamique", qui est " *la partie de la sûreté de fonctionnement qui étudie de manière intégrée le comportement des systèmes industriels complexes affectés par une évolution dynamique continue sous-jacente* " (Kermisch & Labeau,2000).

- Affinement de l'estimation de la distribution du taux de défaillance d'un accès voyageurs

Pour l'application spécifique d'un système élémentaire de type accès voyageurs, l'estimation de la distribution du taux de défaillance a été réalisée sur des données censurées par une durée maximale de 8544h de fonctionnement. Dans un premier temps, nous avons réalisé une estimation de la distribution du taux de défaillance sans tenir compte de la censure des données. Une perspective consiste donc à tenir compte de cette censure afin d'estimer la distribution du taux de défaillance. D'autre part, la durée d'observation n'atteint que 8544h (soit un peu moins d'un an) sur un système dont la durée de fonctionnement est prévu pour une période de 40 ans. Une autre perspective consiste donc à mettre à jour avec davantage de données l'estimation de la distribution réalisée. Suite à ces deux perspectives, l'hypothèse initiale d'une distribution de Weibull peut être confortée ou non.

- Nouvelle stratégie au diagnostic global

Il est envisagé d'intégrer une nouvelle stratégie d'analyse au niveau du diagnostic global. Il s'agit de l'inhibition, qui est proposée dans (Le Mortellec et al.,2012). Dans ce cas, chaque système élémentaire est supposé avoir son propre contexte environnemental (par exemple : la température ambiante du système élémentaire). Des tables d'inhibitions sont utilisées pour décider, en fonction du diagnostic généré et en fonction du contexte environnemental, si le diagnostic est inhibé ou non. Par exemple, pour le cas d'un accès voyageurs ferroviaire, le dévers influence le bon fonctionnement (voir chapitre 4). Avec la stratégie d'inhibition, lorsque le diagnostic "porte fermée avec un retard (ΔT)" est généré et que le contexte environnemental "train arrêté dans une station en dévers " existe, alors le diagnostic peut être inhibé. La modélisation de ces nouvelles stratégies doit permettre de montrer d'autres avantages de l'architecture EDCD par rapport à l'architecture RCD.

- Nouvelles stratégies de maintenance

Enfin, il est également envisagé d'intégrer d'autres politiques de maintenance dans les modèles. En effet, nos avons modélisé le diagnostic curatif et modélisé la maintenance curative, mais le projet FUI SURFER vise aussi le développement du diagnostic prédictif et de la maintenance conditionnelle. L'intégration de ces nouvelles stratégies doit permettre de vérifier si l'architecture EDCD développée dans SURFER conduit à l'optimisation de la maintenance.

2.1.2. Proposition d'une méthodologie d'évaluation FMD a priori

L'approche proposée en réponse à la problématique de thèse peut être qualifiée d'approche "a posteriori", dans le sens où l'évaluation de FMD est réalisée après l'analyse technique et

fonctionnelle de l'architecture développée dans le projet FUI SURFER. Cette démarche est l'approche habituellement réalisée lors d'une évaluation FMD (Villemeur,1991).

Cette démarche a un caractère itératif (Villemeur,1991). L'analyse technique et fonctionnelle du système est d'abord réalisée. Puis, une analyse qualitative et une analyse quantitative sont réalisées. Enfin, l'étude est synthétisée et les conclusions sont tirées : si les objectifs initiaux sont atteints, alors l'étude prend fin. Sinon, le projet est révisé et des modifications sont apportées au système (bouclage).

Le nombre de bouclage, en cas de non atteinte des objectifs, peut potentiellement être important, du fait de la complexité des architectures de diagnostic. D'autre part, le coût des modifications est croissant avec le temps écoulé depuis le démarrage du projet (Calvez,1990). Ce constat nous a poussés à rechercher une démarche permettant de limiter le nombre de bouclages.

Dans cette optique, intégrer les objectifs de sûreté de fonctionnement dès la phase d'analyse fonctionnelle et technique semble prometteuse. Dans cette approche, qualifiée d'approche a priori, les objectifs de FMD sont intégrés dès le départ. Les objectifs finaux doivent être plus facilement atteints et le nombre de bouclages doit diminuer.

Nous avons apporté une première réponse dans ce sens dans (Gandibleux et al.,2012a), en utilisant les concepts de la norme (IEC 61508,2012) pour concevoir un système de surveillance/diagnostic. La démarche proposée se base sur l'approche de risque et la réduction du risque, préconisée par la norme (IEC 61508,2012) et préconisée dans le transport ferroviaire français (EN 50126,2000). La norme (IEC 61508,2012) introduit la notion de sécurité fonctionnelle et propose une démarche de conception pour les systèmes Electriques/Electroniques/Electroniques Programmables (E/E/PE) relatifs à la sécurité.

La démarche proposée dans (Gandibleux et al.,2012a) peut se résumer comme suit. Bombardier définit le risque maximal tolérable lié au système de transport, noté MTR. Si le risque initial lié au système de transport, est supérieur au MTR, alors il est nécessaire de procéder à une réduction du risque. Pour réduire le risque, un système de surveillance/diagnostic est greffé sur le système de transport. Pour réaliser une réduction de risque donnée, le système de surveillance/diagnostic doit atteindre un objectif donné (par exemple, une valeur minimale de MTTF). Pour atteindre ce niveau de fiabilité, différentes alternatives d'architectures sont possibles (par exemple : architecture redondante ou non).

Cette démarche s'inscrit bien dans la démarche proposée dans la norme (IEC 61508,2012), car la norme précise que la sécurité fonctionnelle est "*centrée sur la fiabilité des systèmes relatifs à la sécurité dans l'exécution des fonctions de sécurité*". Donc, concevoir un système relatif à la sécurité conformément à la norme (IEC 61508,2012) revient à concevoir un système fiable.

2.2.Perspectives industrielles

Deux perspectives industrielles à nos travaux de recherche ont été identifiées. Elles consistent à réutiliser les modèles génériques proposés d'une part et à exploiter les modèles pour réaliser des études technico économiques d'autre part.

- Réutilisation des modèles génériques

La méthodologie proposée a aujourd'hui permis d'argumenter, d'un point de vue sûreté de fonctionnement, l'intérêt de passer d'une architecture RCD à une architecture EDCD. Les conclusions ont conduit à l'implantation de l'architecture EDCD sur le train NAT ("Nouvelle Automotrice Transilien"), qui est aujourd'hui en exploitation en Ile-de-France. Fort ce succès, l'utilisation de la méthodologie est aujourd'hui envisagée pour justifier l'intérêt d'installer une architecture de type EDCD sur les prochaines générations de trains conçus par Bombardier à Crespin (métros, trains régionaux).

- Etudes technico-économiques

Pour Bombardier, il est envisagé de coupler les modèles proposés à une étude économique, car l'occurrence d'une défaillance est liée à des coûts (Umiliacchi et al.,2011). Une telle étude doit permettre de calculer le coût global lié à l'architecture RCD et à l'architecture EDCD. Ce nouvel indicateur permettrait de comparer sur un plan économique les deux alternatives. Ce type d'indicateur est intéressant pour le constructeur, car il s'agit d'un critère de comparaison pour l'exploitant ferroviaire, lors du choix d'un nouveau matériel roulant.

Bibliographie

ATOC. (2007). *Ten-year European Rail Growth Trends. Britain's railways - the fastest growing in Europe* (Rapport). London, UK. Association of Train Operating Companies.

Agudelo, C., Anglada, F. M., Cucarella, E. Q., et Moreno, E. G. (2013). Integration of techniques for early fault detection and diagnosis for improving process safety: Application to a Fluid Catalytic Cracking refinery process. *Journal of Loss Prevention in the Process Industries*. 26 (4), 660-665. ISSN 0950-4230. Elsevier

Alanen, J., Haataja, K., Laurila, O., Peltola, J., et Aho, I. (2006). *Diagnostics of mobile work machines.* Research Notes 2343. Finland. VTT Technical Research Centre of Finland.

Amari, S. V., Myers, A. F., Rauzy, A., et Trivedi, K. S. (2008). Imperfect Coverage Models: Status and Trends. Dans K. B. Misra (Éd.), *Handbook of Performability Engineering*. Springer London, UK., 321-348. 10.1007/978-1-84800-131-2_22

Antoni, M. (2009). *Validation d'automatismes ferroviaires de sécurité à base de réseaux de Petri* (Thèse de doctorat). Braunschweig Technische Universität. Braunschweig, Allemagne.

Arlat, J. (2000). *Composants logiciels et sûreté de fonctionnement: intégration de COTS*. Paris. Hermès science publications. COTS: Components off the shelf. ISBN 978-2-7462-3840-4.

Aubrun, C., Sauter, D., et Yamé, J. J. (2008). Fault diagnosis of networked control systems. *International Journal of Applied Mathematics and Computer Science*. 18 (4), 525-537. ISSN 2083-8492. University of Zielona Góra, Institute of Control and Computation Engineering. Poland.

Aubrun, C., Simon, D., et Song, Y.-Q. (2010). *Co-design Approaches for Dependable Networked Control Systems*. London, UK. ISTE Wiley. ISBN 978-1-84821-176-6.

Avizienis, A., Laprie, J. C., et Randell, B. (2000). Fundamental concepts of dependability. *Proceedings of ISW 2000. 34th Information Survivability Workshop*. Los Alamitos, USA., 7–12.

Aza-Vallina, D., Denis, B., et Faure, J.-M. (2011). Communications reliability analysis in networked embedded systems. Dans G. & G. S. Bérenguer (Éd.), *Actes de ESREL2011. Advances in Safety, Reliability and Risk Management*. Troyes, France. Taylor & Francis Group., 2639-2646.

Barger, P. (2003). *Evaluation et validation de la fiabilité et de la disponibilité des systèmes d'automatisation à intelligence distribuée, en phase dynamique* (Thèse de doctorat). Université Henri Poincaré Nancy 1. Faculté des sciences et techniques. Nancy, France.

Benard, V., Cauffriez, L., et Renaux, D. (2008). The Safe-SADT method for aiding designers to choose and improve dependable architectures for complex automated systems. *Reliability Engineering & System Safety*. 93 (2), 179 - 196. ISSN 0951-8320. Elsevier

Benedettini, O., Baines, T. S., Lightfoot, H. W., et Greenough, R. M. (2009). State-of-the-art in integrated vehicle health management. *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering*. 223 (2), 157-170. SAGE journals

Bengtsson, M. (2003). *Condition Based Maintenance on Rail Vehicles - Possibilities for a more effective maintenance strategy* (Technical Report). Malardalen University, Malardalen, Sweden.

Berbineau, M. (2002). *Les systèmes de télécommunication existants ou émergents et leur utilisation dans le domaine des transports guidés*. Synthèse INRETS. Arcueil, France. INRETS. ISBN 9782857825623.

Biteus, J., Frisk, E., et Nyberg, M. (2011). Distributed Diagnosis Using a Condensed Representation of Diagnoses With Application to an Automotive Vehicle. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*. 41 (6), 1262-1267. ISSN 1083-4427. IEEE

Boiteau, M., Dutuit, Y., Rauzy, A., et Signoret, J.-P. (2006). The AltaRica data-flow language in use: modeling of production availability of a multi-state system. *Reliability Engineering & System Safety*. 91 (7), 747-755. ISSN 0951-8320. Elsevier

Bombardier. (2010). *Le site de Crespin - les compétences réussies d'un intégrateur ferroviaire* (Dossier de presse). Crespin, France. Bombardier Transport.

Borrel, M. (1996). *Interactions entre composants matériel et logiciel de systèmes tolérants aux fautes: caractérisation, formalisation, modélisation - application à la sureté de fonctionnement du CAUTRA* (Thèse de doctorat). Institut National Polytechnique de Toulouse, Toulouse, France.

Boudali, H., et Dugan, J. B. (2005). A discrete-time Bayesian network reliability modeling and analysis framework. *Rel. Eng. & Sys. Safety*. 87 (3), 337-349. ISSN 0951-8320. Elsevier

Bouillaut, L., François, O., Aknin, P., Donat, R., Bondeux, S., et Dubois, S. (2011). VirMaLab — atelier virtuel de maintenance: un outil d'aide à la décision pour l'optimisation des politiques de maintenance. *Recherche Transports Sécurité*. 27 (4), 241-257. ISSN: 1951-6614. Springer

Brissaud, F., Barros, A., et Bérenguer, C. (2010). Improving availability and safety of control systems by cooperation between intelligent transmitters. *Actes de PSAM 10: Probabilistic safety assessment and management*. Seattle, États-Unis.

Broy, P., Chraibi, H., et Donat, R. (2011). Using dynamic Bayesian networks to solve a dynamic reliability problem. *Actes de ESREL2011. Advances in Safety, Reliability and Risk Management*. Troyes, France. Taylor & Francis Group., 335-341.

Byington, C. S., Kalgren, P. W., Johns, R., et Beers, R. J. (2003). Embedded diagnostic/prognostic reasoning and information continuity for improved avionics maintenance. *Proceedings of the AUTOTESTCON 2003 IEEE Systems Readiness Technology Conference.* California, USA., 320-329.

CCE. (2004). *Directive du parlement européen et du conseil modifiant la directive 91/440/CEE du Conseil relative au développement de chemins de fer communautaires*. Bruxelles, Belgique. Commission des Communautés Européennes.

CEI 61508. (2010). *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité. Parties 1 à 7.* Geneva, Switzerland. Commission Electrotechnique Internationale.

CIA. (2013). *CAN (Controller area network) Specification 2.0, Part A* (Spécification technique). Erlangen, Germany. CAN in Automation (CiA). Consulté le 01 Mai 2013

Cabarbaye, A., et Laulheret, R. (2005). Evaluation de la sûreté de fonctionnement des systèmes dynamiques par modélisation récursive. *Actes du 6ème Congrès International pluridisciplinaire, qualité et sûreté de fonctionnement, Qualita 2005*. Bordeaux, France.

Calderón-Espinoza, G. (2003). *Model based fault diagnosis techniques: an overview and a proposal* (Research report). Universitat de Girona-Departament EIA, Girona, España.

Calvez, J. P. (1990). *Spécification et conception des systèmes: une méthodologie*. Manuels informatiques Masson. Alençon, France. Masson. ISBN 2-225-82107-0.

Cauffriez, L. (2005). *Méthodes et modèles pour l'évaluation de la sûreté de fonctionnement de systèmes automatisés complexes: Application à l'exploitation de lignes de production - Application à la conception de systèmes intelligents distribués* (Habilitation à Diriger des Recherches). Université de Valenciennes et du Hainaut-Cambresis, Valenciennes, France.

Cauffriez, L., Ciccotelli, J., Conrard, B., et Bayart, M. (2004). Design of intelligent distributed control systems: a dependability point of view. *Reliability Engineering and System Safety*. 84 (1), 19-32. ISSN 0951-8320. Elsevier.

Cauffriez, L., Loslever, P., Caouder, N., Turgis, F., et Copin, R. (2013). Robustness study and reliability growth based on exploratory design of experiments and statistical analysis: a case study using a train door test bench. *The International Journal of Advanced Manufacturing Technology*. 66 (1-4), 27-44. ISSN 0268-3768. Springer-Verlag.

Cauffriez, L., Renaux, D., Bonte, T., et Cocquebert, E. (2012). Systemic modeling of integrated systems for decision making early on in the design process. *Cybern. Syst.* 44 (1), 1–22. ISSN 0196-9722.

Ciame. (2009). *Réseaux de terrain - critères de sûreté de fonctionnement*. Traités IC2 (Information - Commande - Communication), série systèmes automatisés. Paris, France. Hermes-Lavoisier. ISBN 2-7462-1946-8.

Ciutat, F. (2010). *SIL: automatisme & sécurité: SIS, SRECS, SRP-CS, APIdS, FS-PLC, réseaux*. Fontvieille, France. Apta éd. ISBN 9782746613997.

Claesson, V. (2002). *Efficient and Reliable Communication in Distributed Embedded Systems* (Thèse de doctorat). Chalmers University of Technology, Göteborg, Sweden.

Clark, J., Clarke, C., De Panfilis, S., Granatella, G., Predonzani, P., Sillitti, A., Succi, G., et al. (2004). Selecting components in large COTS repositories. *Journal of Systems and Software*. 73 (2), 323-331. ISSN 0164-1212. Elsevier

Cordier, C., Fayot, M., Leroy, A., et Petit, A. (1997). Integration of process simulations in availability studies. *Reliability Engineering & System Safety*. 55 (2), 105-116. ISSN 0951-8320. Elsevier

Cordier, M.-O., Dague, P., Lévy, F., Montmain, J., Staroswiecki, M., et Travé-Massuyès, L. (2004). Conflicts versus Analytical Redundancy Relations: a Comparative Analysis of the Model Based Diagnosis Approach from the Artificial Intelligence and Automatic Control Perspective. *IEEE transactions on systems, man and cybernetics*. 34, 2163-2177.

Corman, F., D'Ariano, A., et Hansen, I. A. (2012). *Evaluating disturbance robustness of railway schedules* (No. RT-DIA-197-2012.). Roma, Italy. Universita degli Studi di Roma Tre.

DIN EN 13306. (2010). *Maintenance – Maintenance terminology* (Norme). Berlin, Allemagne. Deutsches Institut für Normung. European Committee for Standardization

David, R., et Alla, H. (2005). *Discrete, continuous, and hybrid Petri Nets*. Springer. ISBN 9783540224808.

De Kleer, J., et Williams, B. C. (1987). Diagnosing multiple faults. *Artificial Intelligence*. 32 (1), 97 - 130. ISSN 0004-3702. Elsevier.

Dersin, P. (2009). Reliability Challenges in Rail Transport Industry. *Proceedings of Mathematical Methods in Reliability 2009*. Moscow, Russia.

Dersin, P., et Péronne, A. (2007). Influence de la testabilité et de la politique de maintenance sur la disponibilité d'un système ferroviaire. *Actes de PENTOM2007*. Valenciennes, France.

Diaz, M. (2001). *Les réseaux de Petri: Modèles fondamentaux*. IC2. Paris, France. Hermès science publications. ISBN 2-7462-0250-6.

Dievart, M. (2010). *Architectures de diagnostic et de pronostic distribuées de systèmes techniques complexes de grande dimension* (Thèse de doctorat). Toulouse. Institut National Polytechnique de Toulouse, Toulouse, France.

Donat, R. (2009). *Modélisation de la fiabilité et de la maintenance par modèles graphiques probabilistes Application à la prévention des ruptures de rails* (Thèse de doctorat). Institut National des Sciences Appliquées de Rouen, Rouen, France.

Dubuisson, B. (2001). *Diagnostic, intelligence artificielle et reconnaissance des formes*. IC2 information - commande - communication. Paris, France. Hermès Science publications. ISBN 2-7462-0249-2.

E.800. (2008). *Qualité de service: concepts, modèles, objectifs, planification de la sûreté de fonctionnement – Termes et définitions relatifs à la qualité des services de télécommunication. Définition de termes relatifs à la qualité de service.* (Recommandation UIT-T). Genève, Suisse. Union Internationale des Télécommunications.

EN 50121. (2006). Applications ferroviaires - Compatibilité électromagnétique. (Norme). Bruxelles, Belgique. Comité Européen de Normalisation Electrotechnique.

EN 50126-1. (2000). *Applications ferroviaires. Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS). Partie 1: Exigences de base et procédés génériques.* (Norme). Bruxelles, Belgique. Comité Européen de Normalisation Electrotechnique.

EN 50155. (2007). *Applications ferroviaires - Equipements électroniques utilisés sur le matériel roulant.* (Norme). Bruxelles, Belgique. Comité Européen de Normalisation Electrotechnique.

Eurostat. (2010). *Railway passenger transport decreased slightly at the beginning of 2009* (Rapport No. ISSN 1977-0316). Luxembourg. Eurostat.

Feldman, A. (2010). *Approximation Algorithms for Model-Based Diagnosis* (Thèse de doctorat). Technische Universiteit Delft, Delft, Netherlands.

Fota, N., Kaâniche, M., et Kanoun, K. (1999). Dependability evaluation of an air traffic control computing system. *Proceedings of the IEEE Computer Performance and Dependability Symposium*. Durham, USA., 206-215.

FprEN50159. (2010). *Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems. Final Draft* (Projet de norme). Bruxelles, Belgique. Comité Européen de Normalisation Electrotechnique. Final Draft

Fries, J. M., Weingartner, A. A., et Herinckx, D. J. (2009). Surveillance à distance d'équipement de voie ferrée à l'aide de protocoles réseau. Brevet. WO2009042283 A2. General Electric Company

Galdun, J., Thiriet, J.-M., Ligus, J., et Sarnovsky, J. (2008). Reliability increasing through networked cascade control structure - consideration of quasi-redundant subsystems. Dans IFAC (Éd.), *Preprints of the 17th IFAC World Congress*. Seoul, Corée., 6839-6844.

Gandibleux, J., Cauffriez, L., et Branger, G. (2012b). Evaluation de FMD d'un système dynamique hybride par Réseaux de Petri: application à un accès voyageurs. *Actes de Lambda Mu 18*. Tours, France. IMDR., 1376-1385.

Gandibleux, J., Cauffriez, L., et Branger, G. (2012a). Extension des Concepts de la norme CEI-61508 pour la conception d'un système de surveillance/diagnostic embarqué. *Actes de la Conférence Internationale Francophone d'Automatique CIFA2012*. Grenoble, France., 131-136.

Gandibleux, J., Cauffriez, L., et Branger, G. (2011). Improving the reliability/availability of a complex system by an active monitoring based onto « augmentation concept »:Application onto a railway system. *Actes de ESREL2011. Advances in Safety, Reliability and Risk Management*. Troyes, France. Taylor & Francis Group.

Gandibleux, J., Clarhaut, J., Cauffriez, L., et Sallez, Y. (2013). Comparison of embedded diagnosis architectures in the field of railway transport:a dependability point of view. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*. Submitted to the journal. SAGE Journals.

Gaudoin, O., et Ledoux, J. (2007). *Modélisation aléatoire en fiabilité des logiciels*. Méthodes stochastiques appliquées. Paris, France. Hermès Science Publications. ISBN 978-2-7462-1608-2.

Ghostine, R., Thiriet, J.-M., et Aubry, J.-F. (2006). Dependability evaluation of networked control systems under transmission faults. *Proceedings of the 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Safeprocess*. Beijing, China. Elsevier., 1129-1134.

Hallgren, D., et Skog, H. (2005). *Distributed Fault Diagnosis for Networked Embedded Systems* (Thèse de Master). Linköping University, Department of Electrical Engineering, Linköping, Sweden.

Herzog, U. (2002). Lectures on formal methods and performance analysis. Dans E. Brinksma, H. Hermanns, & J.-P. Katoen (Éd.), . New York, NY, USA. Springer-Verlag New York, Inc., 1–37.

Hoyland, A., et Rausand, M. (2004). *System reliability theory: models, statistical methods, and applications*. Wiley series in probability and statistics: Applied probability and statistics. New York, USA. Wiley-Interscience. ISBN 9780471471332.

IEC 60300-3-1. (2003). *Dependability management - Part 3-1: Application guide - Analysis techniques for dependability - Guide on methodology* (Norme). Genève, Suisse. International Electrotechnical Commission.

IEC 61375. (2012). *Electronic railway equipment - Train communication network - Parts 1 to 3* (Norme). Bruxelles, Belgique. International Electrotechnical Commission. International Electrotechnical Commission

ISDF. (2000). *Démarche et méthodes de Sûreté de Fonctionnement des logiciels* (Rapport du Groupe de Travail et de Réflexion « Démarche et méthodes de Sûreté de Fonctionnement des logiciels »). France. Institut de Sûreté de Fonctionnement.

ISO 11898-1. (2003). *Road vehicles - Controller area network (CAN). Part 1: Data link layer and physical signalling* (Norme). Geneva, Switzerland. International Organization for Standardization.

ISO 13374-1. (2003). *Condition monitoring and diagnostics of machines -- Data processing, communication and presentation -- Part 1: General guidelines* (Norme). Geneva, Switzerland. International Organization for Standardization.

Isermann, R. (2006). *Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance*. Berlin, Allemagne. Springer-Verlag Berlin Heidelberg. ISBN 9783540241126.

Jensen, K. (1994). An Introduction to the Theoretical Aspects of Coloured Petri Nets. *Lecture Notes in Computer Science*. 803, 230-272. Springer-Verlag

Jensen, K., Kristensen, L. M., et Wells, L. (2007). Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems. *International Journal on Software Tools for Technology Transfer*. 9 (3-4), 213-254. ISSN 1433-2787. Springer

Kohl, J., et Bauer, A. (2010). Role-Based Diagnosis for Distributed Vehicle Functions. *Online Proceedings of the 21st International Workshop on the Principles of Diagnosis (DX)*. Portland, USA. PHM Society.

Koopman, P., et Chakravarty, A. (2001). Analysis of the Train Communication Network Protocol Error Detection Capabilities. *Institute for Software Research*. Pittsburgh, USA. Carnegie Mellon University.

Kootkar, S. B. (2008). *Reliable sensor networks - a case study in commuter trains* (Thèse de Master). Delft, Netherlands. Delft University of Technology, Delft, Netherlands.

Koutsoukos, X., Biswas, G., Mylaraswamy, D., Hadden, G., Mack, D., et Hamilton, D. (2010). Benchmarking the Vehicle Integrated Prognostic Reasoner. *Proceedings of the Annual Conference of the Prognostics and Health Management Society*. Portland, USA. PHM Society.

Kumamoto, H. (2007). *Satisfying safety goals by probabilistic risk assessment*. Springer series in reliability engineering. London, UK. Springer-Verlag. ISBN 9781846286810.

Kumamoto, H., et Henley, E. J. (1996). *Probabilistic risk assessment and management for engineers and scientists*. IEEE Press. ISBN 9780780310049.

Laprie, J. C. (1995). *Guide de la sûreté de fonctionnement*. Toulouse, France. Cépaduès-Editions. ISBN 2-85428-382-1.

Lavina, Y., et Perruche, E. (1998). *ISO 9000 - EAFQ maintenance et assurance de la qualité*. Paris, France. Ed. d'Organisation. ISBN 2-7081-2087-5.

Le Mortellec, A., Clarhaut, J., Berger, T., et Trentesaux, D. (2013). Embedded holonic fault diagnosis of complex transportation systems. *Engineering Applications of Artificial Intelligence*. 26 (1), 227-240. ISSN 0952-1976. Elsevier

Le Mortellec, A., Clarhaut, J., Sallez, Y., Berger, T., et Trentesaux, D. (2012). Embedded cooperative holarchy for diagnosing complex moving systems. *Proceedings of the 14th IFAC symposium on Information & Control problems in Manufacturing (INCOM)*. Bucarest, Romania., 673-678.

Lyonnet, P. (2006). *Ingénierie de la fiabilité*. Paris, France. Tec & Doc Lavoisier. ISBN 9782743008239.

MIL-HDBK-217F. (1991). *Military handbook - Reliability prediction of electronic equipment*. USA. Department of Defense.

Menighed, K. (2010). *Commandes coopératives embarquées et tolérantes aux défauts* (Thèse de doctorat). Université Henri Poincaré Nancy 1. Faculté des sciences et techniques. Nancy, France.

Metodi, A., Stern, R., Kalech, M., et Codish, M. (2012). Compiling Model-Based Diagnosis to Boolean Satisfaction. *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence*. Toronto, Canada.

Myers, A. F., et Rauzy, A. (2008). Assessment of redundant systems with imperfect coverage by means of binary decision diagrams. *Rel. Eng. & Sys. Safety*. 93 (7), 1025-1035. ISSN 0951-8320. Elsevier

Márquez, F. P. G., Lewis, R. W., Tobias, A. M., et Roberts, C. (2008). Life cycle costs for railway condition monitoring. *Transportation Research Part E: Logistics and Transportation Review*. 44 (6), 1175 - 1187. ISSN 1366-5545. Elsevier

Meshkat, L., Bechta Dugan, J., et Andrews, J. D. (2002). Dependability Analysis of Systems WithOn-Demand and Active Failure Modes,Using Dynamic Fault Trees. *IEEE Transactions on Reliability*. 51 (2), 240-251. ISSN 0018-9529. IEEE.

NF ISO 13372. (2005). *Surveillance et diagnostic des machines - Surveillance et diagnostic de l'état des machines - Vocabulaire.* (Norme). Paris, France. AFNOR.

Navet, N., Song, Y.-Q., et Simonot, F. (2000). Worst-case deadline failure probability in real-time applications distributed over controller area network. *Journal of Systems Architecture*. 46 (7), 607 - 617. ISSN 1383-7621. Elsevier

Nicolet, J.-L., Carnino, A., et Wanner, J.-C. (1989). *Catastrophes? Non merci! La prévention des risques technologiques et humains*. Paris, France. Masson. ISBN 2-225-81710-3.

Niel, E., et Craye, E. (2002). *Maîtrise des risques et sûreté de fonctionnement des systèmes de production*. IC2: Série Productique. Paris, France. Hermès Science Publications. ISBN 9782746204027.

Nyberg, M. (2002). Criterions for detectability and strong detectability of faults in linear systems. *International Journal of Control*. 75 (7), 490-501. ISSN 0020-7179. Elsevier.

Pagès, A., et Gondran, M. (1980). *Fiabilité des systèmes*. Collection de la Direction des études et recherches d'Électricité de France. Paris. Eyrolles. ISBN 978-2-212-01582-9.

Papadopoulos, Y., Tran, A., Faure, J.-M., et Grante, C. (2006). Component Failure Behaviour: Patterns and Reuse in Automated System Safety Analysis. *Proceedings of SAE 2006 World Congress*. Detroit, États-Unis.

Patton, R. J. (1997). Robustness in model-based fault diagnosis: The 1995 situation. *Annual Reviews in Control*. 21 (0), 103-123. ISSN 1367-5788. Elsevier

Petri, C. A. (1962). *Kommunikation mit Automaten* (Thèse de doctorat). Universität Hamburg, Hambourg, Allemagne.

Prabhu, V. V., et Duffie, N. A. (1996). Modelling and Analysis of Heterarchical Manufacturing Systems Using Discontinuous Differential Equations. *CIRP Annals - Manufacturing Technology*. 45 (1), 445-448. ISSN 0007-8506. Elsevier

Procaccia, H., Ferton, E., Procaccia, M., et Lannoy, A. (2011). *Fiabilité et maintenance des matériels industriels réparables et non réparables*. SRD, sciences du risque et du danger. Paris, France. Éd. Tec & doc. ISBN 978-2-7430-1362-2.

Prosyst. (2008). Diagnostic Automatique. Une nouvelle approche de diagnostic machine basée sur l'exécution d'un modèle structurel. *Actes de la Journée SEE–AAI, GDRMACS-S3. Les nouveaux outils de diagnostic dans les processus industriels - Les clés de la compétitivité*. Paris, France.

Rahoual, M., et Siarry, P. (2006). *Les réseaux informatiques: conception et optimisation*. Paris, France. Technip. ISBN 978-2-7108-0877-0.

Redmill, F. (2004). Analysis of the COTS debate. *Safety Science*. 42 (5), 355 - 367. ISSN 0925-7535. Elsevier

Renner, E., et Umiliacchi, P. (2003). TrainCom: an Integrated Communication System for Intelligent TrainApplications. *Proceedings of the WCRR, World Conference on Railway Research*. Edinburgh, UK.

Ribot, P. (2009). *Vers l'intégration diagnostic-pronostic pour la maintenance des systèmes complexes* (Thèse de doctorat). Toulouse. Université Paul Sabatier, Toulouse, France.

Roos, N., Teije, A. T., et Witteveen, C. (2003). Multi-Agent Diagnosis with Semantically Distributed Knowledge. *Proceedings of the 15th Belgium-Dutch Conference on Artificial Intelligence (BNAIC-2003)*. Nijmegen, Netherlands., 259–266.

SNCF. (2009). Maintenance prédictive : Savoir pour anticiper. *Rail et Recherche n°52*., 9-12.

Schweiger, S. (2009). *Lebenszykluskosten optimieren: Paradigmenwechsel für Anbieter und Nutzer von Investitionsgütern*. Wiesbaden, Allemagne. Gabler Verlag / GWV Fachverlage GmbH. ISBN 978-3834909893.

Shingler, R., et Umiliacchi, P. (2003). Advances in railways maintenance: the EuRoMain project. *Proceedings of the WCRR, World Conference on Railway Research*. Edinburgh, UK.

Smedley, V. A., et Steijger, L. A. (2004). Remote system condition monitoring. Brevet. GB2392983. Bombardier Transportation

Smith, G., et Bowen, M. (1995). Considerations for the utilization of smart sensors. *Sensors and Actuators A: Physical*. 47 (1–3), 521 - 524. ISSN 0924-4247. Elsevier

Staroswiecki, M. (2005). Intelligent sensors: a functional view. *IEEE Transactions on Industrial Informatics*. 1 (4), 238–249. ISSN 1551-3203. IEEE

Su, R., Wonham, W. M., Kurien, J., et Koutsoukos, X. (2002). Distributed Diagnosis for Qualitative Systems. *Proceedings of the 6th International Workshop on Discrete Event Systems (WODES-2002)*. Zaragoza, Spain., 169–174.

Söderholm, P. (2007). A system view of the No Fault Found (NFF) phenomenon. *Reliability Engineering & System Safety*. 92 (1), 1-14. ISSN 0951-8320. Elsevier.

Tanarro, F., et Fuerte, F. (2011). OHMS - real-time analysis of the pantograph catenary interaction to reduce maintenance costs. *Proceedings of the 5th IET Conference on Railway Condition Monitoring and Non-Destructive Testing*. Derby, UK. IET Conference Publications.

Thiriet, J.-M. (2004). *Sûreté de fonctionnement de Systèmes d'Automatisation à Intelligence Distribuée* (Habilitation à Diriger des Recherches). Université Henri Poincaré Nancy 1. Nancy, France.

Thomesse, J.-P. (2002). Fieldbuses and Quality of Service. *Proceedings of the 5th Portuguese Conference on Automatic Control*. Aveiro, Portugal., 10-14.

Turgis, F. (2013). *Amélioration de la fiabilité d'un système complexe. Application ferroviaire: accès voyageurs.* (Thèse de doctorat). Université de Valenciennes et du Hainaut-Cambresis,Valenciennes, France.

Turgis, F., Copin, R., Loslever, P., Cauffriez, L., et Caouder, N. (2010). Proposition d'une méthodologie pour la réalisation d'essais de fiabilité sur un système complexe d'accès voyageur. *Actes de Lambda Mu 17*. La Rochelle, France., 1-10.

UIC. (2006). *EIRENE (European Integrated Railway Radio Enhanced NEtwork) System Requirements Specification* (Spécification technique). Paris, France. Union Internationale des Chemins de Fer.

Umiliacchi, P., Lane, D., et Romano, F. (2011). Predictive maintenance of railway subsystems using an Ontology based modelling approach. *Proceedings of the WCRR2011, World Conference on Railway Research*. Lille, France.

Umiliacchi, P., Shingler, R., Langer, G., et Henning, U. (2006). A new approach to optimisation through intelligent integration of railway systems:the InteGRail project.

Proceedings of the 7th WCRR, World Conference on Railway Research. Montréal, Canada.

Utne, I. B., Brurok, T., et Rødseth, H. (2012). A structured approach to improved condition monitoring. *Journal of Loss Prevention in the Process Industries*. 25 (3), 478-488. ISSN 0950-4230. Elsevier.

Vannier, S., et Dersin, P. (2006). Modélisation de la disponibilité d'un système de communication ferroviaire base sur les standards Wireless IEEE 802.11. *Actes de Lambda Mu 15*. Lille, France.

Venkatasubramanian, V., Rengaswamy, R., Yin, K., et Kavuri, S. N. (2003). A review of process fault detection and diagnosis: Part I: Quantitative model-based methods. *Computers and Chemical Engineering*. 27 (3), 293 - 311. ISSN 0098-1354. Elsevier

Vernez, D., Buchs, D., et Pierrehumbert, G. (2003). Perspectives in the use of coloured Petri nets for risk analysis and accident modelling. *Safety Science*. 41 (5), 445 - 463. ISSN 0925-7535. Elsevier

Villemeur, A. (1991). *Reliability, Availability, Maintainability and Safety Assessment*. New York, USA. John Wiley & Sons ltd. ISBN 9780471930488.

Volovoi, V. (2012). Challenges in Assessing System-Level Effects of IVHM. *Proceedings of the Indo-US workshop on Integrated Vehicle Health Management and Aviation Safety (WIAS)*. Bangalore, India.

Wahl, M. (2004). *Les réseaux de terrain embarqués dans les transports guidés*. Synthèse INRETS. Arcueil, France. INRETS. ISBN 2857825913.

Wahl, M. (2010). *Survey of Railway Embedded Network Solutions: Towards the Use of Industrial Ethernet Technologies*. Synthèse INRETS. Mayenne, France. INRETS. ISBN 9782857826828.

Weber, P., Medina-Oliva, G., Simon, C., et Iung, B. (2012). Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence*. 25 (4), 671 - 682. ISSN 0952-1976. Elsevier

Wesling, H. J., Novakovich, M. R., et Roberts, R. D. (1993). REAL-TIME REMOTE SIGNAL MONITORING SYSTEM. Brevet. WO9318952 A1. Aeg Westinghouse Transportation Systems, Inc.

Whittaker, G. S. (2009). Systèmes et procédés de maintenance à base de conditions. Brevet. WO2009070347 A1. The Boeing Company

Willaeys. (2008). Device and method for a system analysis and diagnosis. Brevet. US0086288. Prosyst

Worcester, P. (2003). A fault prediction system for vehicles. Brevet. GB2378248. Worcester Entpr

Wysocki, J., Debouk, R., et Nouri, K. (2004). Shared redundancy as a means of producing reliable mission critical systems. *Proceedings of the Reliability and Maintainability, 2004 Annual Symposium - RAMS*. Los Angeles, USA., 376-381.

Zille, V. (2009). *Modélisation et évaluation des stratégies de maintenance complexes sur des systèmes multi-composants* (Thèse de doctorat). Université de Technologie de Troyes, Institut Charles Delaunay, Troyes, France.

Zimmermann, A., et Hommel, G. (2005). Towards modeling and evaluation of ETCS real-time communication and operation. *Journal of Systems and Software*. 77 (1), 47 - 54. ISSN 0164-1212. Elsevier

Zwingelstein, G. (1995). *Diagnostic des défaillances: théorie et pratique pour les systèmes industriels*. Traité des nouvelles technologies. Série Diagnostic et maintenance. Paris, France. Hermès. ISBN 9782866014636.

Zwingelstein, G. 1996. *La maintenance basée sur la fiabilité: Guide pratique d'application de la RCM*. Paris, France: Hermes Science Publications. ISBN 9782866015459.

Annexe 1 : lois de probabilité

Cette annexe détaille les caractéristiques des lois de probabilité dans la partie 1 et les méthodes pour estimer les paramètres des lois dans la partie 2. Enfin, un tracé des ces lois de probabilité est présenté dans la partie 3.

1. Définition des lois

Les lois de probabilité discrète ou continue sont habituellement distinguées en sûreté de fonctionnement (Villemeur,1991). Les caractéristiques générales et les fonctions de répartition des principales lois de probabilité sont rappelées ci-dessous.

1.1.Lois discrètes

Les lois de probabilité discrètes sont utilisées, par exemple, lorsque la fiabilité est quantifiée par un nombre de cycles, un nombre de pièces fabriquées ou lorsqu'il s'agit de quantifier la défaillance à la sollicitation (Lyonnet,2006).

1.1.1. La loi binomiale (ou loi de Bernoulli)

Soient p la probabilité d'occurrence de l'évènement A, et 1-p la probabilité que l'évènement A n'ait pas lieu. La variable aléatoire X représentant le nombre de réalisation de A est distribué selon une loi binomiale si (Pagès & Gondran,1980):

$$F(k) = P(X \leq k) = \sum_{i=0}^{k} C_n^i p^i (1-p)^{n-i} \qquad \forall 0 \leq k \leq n\,; \qquad \forall 0 \leq p \leq 1$$

$$o\grave{u}\ C_n^k = \frac{n!}{k!\,(n-k)!}$$

1.1.2. La loi de Poisson

La loi de Poisson est une loi ayant pour paramètre l'espérance mathématique de X, notée m. X suit une loi de Poisson si (Gaudoin & Ledoux,2007):

$$F(k) = \sum_{i=0}^{k} e^{-m} \frac{m^i}{i!}$$

La loi de Poisson peut être considérée comme un cas limite de la loi binomiale, lorsque le nombre d'expériences est élevé et quand l'espérance mathématique de la variable aléatoire est constante (Villemeur,1991).

1.2.Les lois continues

Les lois de probabilité continues sont associées aux variables aléatoires continues (exemple : durée de fonctionnement d'une entité).

1.2.1. La loi de Weibull

La loi de Weibull permet de modéliser un grand nombre de phénomènes grâce à trois paramètres : le paramètre d'échelle σ, le paramètre de forme β et le paramètre de temps γ (qui est souvent nul, (Pagès & Gondran,1980)). Elle se définit par (Gaudoin & Ledoux,2007):

$$\begin{cases} F(t) = 1 - e^{\left[-\left(\frac{t-\gamma}{\sigma}\right)^{\beta}\right]} \\ \lambda(t) = \frac{\beta}{\sigma}\left(\frac{t-\gamma}{\sigma}\right)^{\beta-1} \end{cases}$$

Le taux de défaillance est fonction du temps et permet de modéliser plusieurs situations (Gaudoin & Ledoux,2007) : un taux de défaillance décroissant ($\beta < 1$), un taux de défaillance croissant ($\beta > 1$), un taux de défaillance constant ($\beta = 1$), qui est le cas de la loi exponentielle.

1.2.2. La loi exponentielle

La loi exponentielle peut-être considérée comme une distribution de Weibull avec des paramètres particuliers (Gaudoin & Ledoux,2007). Elle est fréquemment utilisée en sûreté de fonctionnement car les calculs sont faciles à simplifier (Villemeur,1991).

L'hypothèse du taux de défaillance constant est discutable (Kumamoto,2007). Cependant, cette hypothèse d'indépendance vis-à-vis des états occupés antérieurement par le système est vérifiée dans certains systèmes industriels (Niel & Craye,2002). Les lois régissant le système évoluent alors suivant des temps exponentiellement distribués.

Cette loi est définie par :

$$\begin{cases} F(t) = 1 - e^{-\lambda t} \\ \lambda = constante \end{cases}$$

1.2.3. La loi normale

La loi normale est une distribution symétrique de moyenne m et d'écart type σ (Gaudoin & Ledoux,2007). Cette loi s'applique à de nombreux phénomènes (incertitude liée à des mesures, fabrication…) (Villemeur,1991).

$$\begin{cases} F(t) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{t} e^{\left[-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2\right]} dx \\ \lambda(t) = \frac{\frac{dF(t)}{dt}}{1 - F(t)} \end{cases}$$

1.2.4. La loi Log-Normale

La loi Log-Normale, de paramètres μ et σ, est similaire à la distribution normale à l'exception que ce seront les logarithmes des valeurs qui sont normalement distribuées contrairement aux valeurs elles-mêmes (Kumamoto & Henley,1996). Cette loi est fréquemment utilisée pour décrire des données de maintenabilité (Villemeur,1991) et pour les défaillances dues à la fatigue (Lyonnet,2006).

$$\begin{cases} F(t) = \dfrac{1}{\sigma\sqrt{2\pi}} \displaystyle\int_0^t \frac{1}{x} e^{\left[-\frac{1}{2}\left(\frac{\log(x)-\mu}{\sigma}\right)^2\right]} dx \\ \lambda(t) = \dfrac{\frac{dF(t)}{dt}}{1-F(t)} \end{cases}$$

1.2.5. La loi gamma

La loi gamma est une distribution très générale à deux paramètres λ et β (Villemeur,1991). Des valeurs particulières permettent d'obtenir soit la loi exponentielle, soit la loi d'Erlang (Gaudoin & Ledoux,2007). Cette dernière peut être utilisée lorsqu'un événement se produit après une séquence de sous événements distribués exponentiellement, par exemple dans la méthode des états fictifs (Villemeur,1991). Le taux de défaillance est fonction du temps et permet de modéliser plusieurs situations (Gaudoin & Ledoux,2007) : un taux de défaillance décroissant ($\beta < 1$), un taux de défaillance croissant ($\beta > 1$), un taux de défaillance constant ($\beta = 1$), qui est le cas de la loi exponentielle.

$$\begin{cases} F(t) = \displaystyle\int_0^t \frac{\lambda^\beta x^{\beta-1}}{\Gamma(\beta)} e^{-\lambda x} dx \qquad o\grave{u}\ \Gamma(\beta) = \int_0^\infty x^{\beta-1} e^{-x} dx \qquad \beta > 0;\ \lambda > 0;\ t > 0 \\ \lambda(t) = \dfrac{\frac{dF(t)}{dt}}{1-F(t)} \end{cases}$$

2. Méthodes d'estimation des lois de probabilité

Plusieurs méthodes existent pour estimer les paramètres des lois de probabilité (Pagès & Gondran,1980) (Villemeur,1991). Ci-dessous, cette partie se concentre sur l'estimation du paramètre de la loi exponentielle (λ), par la méthode graphique et par la méthode de l'intervalle de confiance.

2.1. Méthode graphique (Kumamoto & Henley,1996)

Dans le cas de la loi exponentielle, la fiabilité est donnée par :

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

Ce qui peut aussi s'écrire :

$$ln\left[\frac{1}{R(t)}\right] = \lambda t$$

Cette seconde équation permet d'illustrer que, si le logarithme népérien de 1/R(t) est tracé en fonction de t, alors la courbe devrait être une droite de coefficient directeur λ. La méthode graphique va consister à tracer les données empiriques dans un repère $\left[t\ ;\ ln\left[\frac{1}{R(t)}\right]\right]$ et estimer le coefficient directeur de la droite passant par ces points.

Pour faciliter la compréhension, l'estimation de λ par la méthode graphique va maintenant être appliquée à l'exemple des données du Tableau 18.

temps avant défaillance	nombre cumulé de défaillances
0	0
20	9
40	23
60	50
90	83
160	113
230	143
400	160
900	220
1200	235
2500	240
∞	250

Tableau 18 : Exemple de recueil de données de sûreté de fonctionnement (Kumamoto & Henley,1996)

Les données d'exemples sont tracées dans le repère $\left[t \ ; \ ln\left[\frac{1}{R(t)}\right]\right]$ de la Figure 33. Il est finalement possible d'estimer la "meilleure" ligne droite passant par ces points :

$$\lambda = \frac{y2 - y1}{x2 - x1} = \frac{1.08 - 0.27}{400 - 100} = 0.0027 \ h^{-1}$$

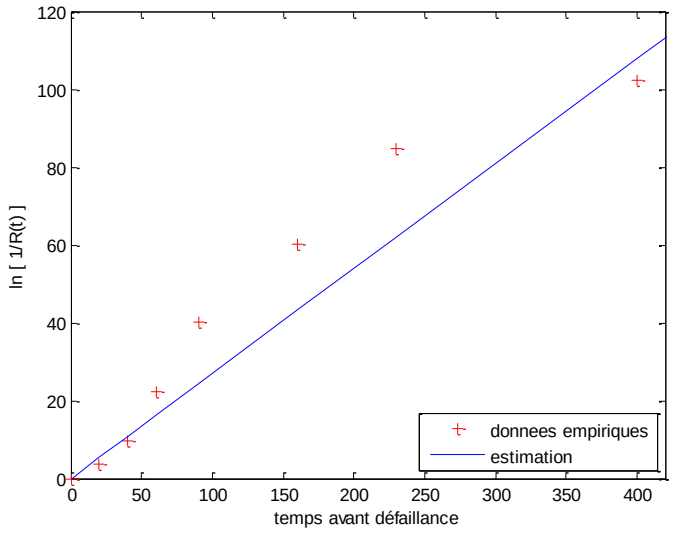


Figure 33 : Test des données pour un λ constant

2.2.Méthode par intervalle de confiance (Lyonnet,2006)

L'estimation par intervalle de confiance permet, en plus, d'indiquer une marge d'erreur sur la précision des paramètres estimés.

Soit un paramètre à estimer θ, dont il faut chercher la valeur estimée, notée $\hat{\theta}$. Soit une probabilité 1-α telle qu'un évènement de probabilité 1-α puisse être considéré comme certain. L'erreur E peut alors être calculée par :

$$P\left(\left|\hat{\theta} - \theta\right| < E\right) = 1 - \alpha$$

L'inégalité signifie que l'intervalle [$\hat{\theta}$-E ; $\hat{\theta}$+E] contiendra la valeur inconnue du paramètre θ avec la probabilité 1-α. Cet intervalle est appelé intervalle de confiance au niveau 1- α.

Soit le nombre moyen de défaillances attendues noté k et le temps cumulé d'observation noté T, il est possible de démontrer que (Lyonnet,2006):

$$\frac{\chi^2_{\frac{\alpha}{2};2k}}{2} \leq k \leq \frac{\chi^2_{1-\frac{\alpha}{2};2k+2}}{2}$$

où $\chi^2_{X;Y}$ est la loi du Khi deux à Y degrés de liberté et de paramètre X. En posant λ=k/T, il est possible de calculer l'intervalle de confiance sur le taux de défaillances :

$$\frac{\chi^2_{\frac{\alpha}{2};2k}}{2T} \leq \lambda \leq \frac{\chi^2_{1-\frac{\alpha}{2};2k+2}}{2T}$$

3. Tracé des lois de probabilité

Les lois de probabilité présentées précédemment sont tracées ci-dessous (Figure 34).

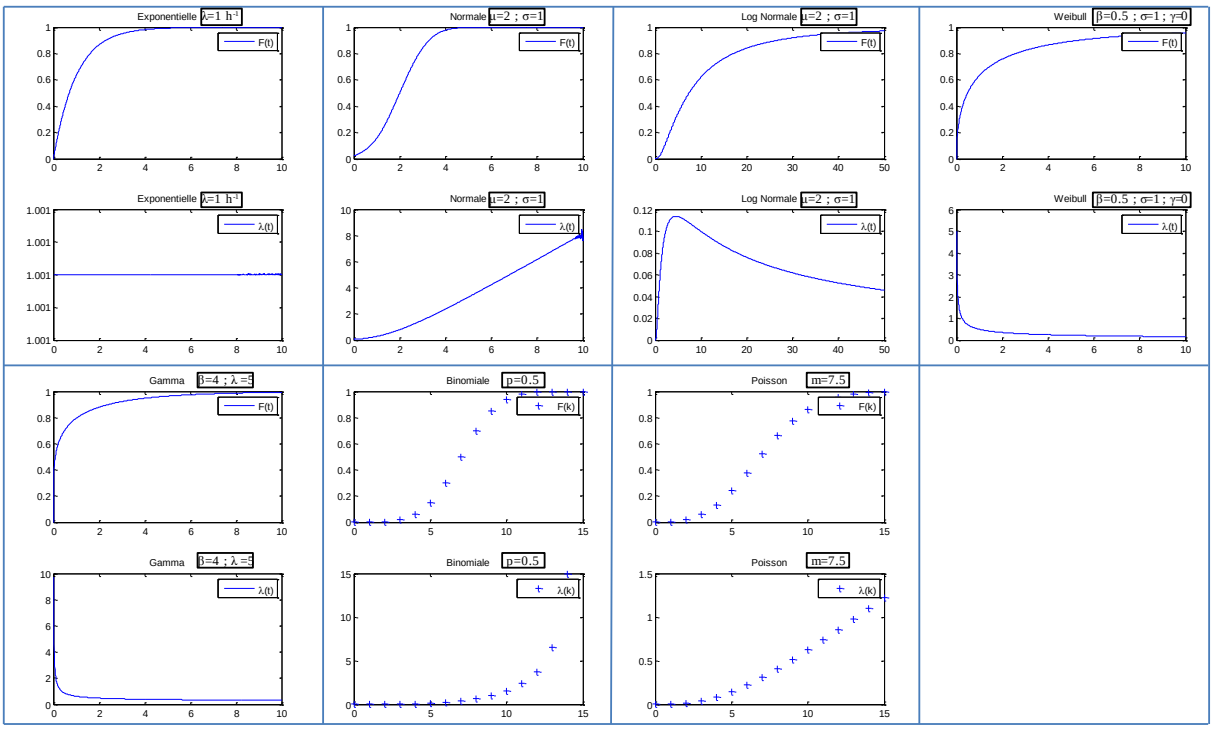


Figure 34 : Tracés des lois de probabilités

Annexe 2 : présentation des autres partenaires du projet FUI SURFER

Le projet FUI SURFER est un projet multipartenaire réunissant BOMBARDIER Transport, le laboratoire TEMPO, Prosyst, l'IFSTTAR et HIOLLE INDUSTRIES, soutenus par les pôles de compétitivité I-Trans et Advancity. Le laboratoire TEMPO, BOMBARDIER Transport et Prosyst, sont brièvement introduits à la partie 3. L'IFSTTAR et HIOLLE INDUSTRIES et les pôles de compétitivité I-Trans et Advancity sont présentés ci-dessous.

1. IFSTTAR

L'IFSTTAR est l'Institut Français des Sciences et Technologies des Transports, de l'Aménagement et des Réseaux. C'est un établissement public à caractère scientifique et acteur de la recherche sur les transports et leur sécurité. Il est constitué de 18 laboratoires de recherche couvrant tous les modes de transport (principalement terrestres) et toutes les disciplines (des sciences de l'ingénieur aux sciences sociales), dont le laboratoire LTN (Laboratoire des Technologies Nouvelles). Le LTN traite plusieurs aspects des transports ferroviaires : énergie, dynamique des véhicules, et diagnostic/maintenance. L'équipe diagnostic/maintenance est impliquée dans le projet FUI SURFER et a pour objectifs de fournir des modèles de diagnostic prédictif et une méthodologie pour optimiser les paramètres des politiques de maintenance.

2. HIOLLE INDUSTRIES

Hiolle Industries est un groupe proposant des services pour l'industrie, comme la maintenance des matériels roulant. Le Groupe est très impliqué dans les technologies à installer sur les trains, ce qui lui permet proposer des équipements adaptés pour l'intégration (l'installation dans les trains). De plus, les méthodes de dépannage vont évoluer.

La participation de Hiolle Industries au projet FUI SURFER lui permet donc de rester en phase avec les avancés dans le domaine du diagnostic et de la maintenance. Hiolle Industries apporte également son savoir faire pour l'installation de la solution finale dans le train.

3. Positionnement vis-à-vis des pôles de compétitivité

Le projet FUI SURFER s'inscrit dans deux pôles de compétitivité :

- Le pôle i-Trans, qui a vocation à répondre aux enjeux dans les transports innovants en apportant son soutient pour le montage et la gestion de projets d'innovation partenariale et à la recherche de fonds publics. Plus précisément, le projet FUI SURFER s'inscrit dans les axes stratégiques du pôle pour 2010-2012 : l'Axe Qualité-Sécurité, sur le thème « Sécurité, fiabilité et sûreté des modes de transport » et l'Axe Compétitivité, sur le thème « Améliorer l'efficacité et la flexibilité industrielles **»**.
- Le pôle Advancity, qui a vocation à permettre aux entreprises et aux structures de recherche de coopérer et de monter des projets collaboratifs sur le territoire francilien. Les retombées

du projet FUI SURFER concernent aujourd'hui directement l'Ile de France, puisque le développement et l'application pilote du projet FUI SURFER est réalisée sur le train NAT (Nouvelle Automotrice Transilien), produit par BOMBARDIER Transport et exploité sur le réseau Transilien. Il est donc logique que le pôle Advancity ait labellisé ce projet.

Index des figures

Index des tableaux

Contribution à l'évaluation de sûreté de fonctionnement des architectures de surveillance/diagnostic embarquées. Application au transport ferroviaire

Résumé : Dans le transport ferroviaire, le coût et la disponibilité du matériel roulant sont des questions majeures. Pour optimiser le coût de maintenance du système de transport ferroviaire, une solution consiste à mieux détecter et diagnostiquer les défaillances. Actuellement, les architectures de surveillance/diagnostic centralisées atteignent leurs limites et imposent d'innover. Cette innovation technologique peut se matérialiser par la mise en œuvre d'architectures embarquées de surveillance/diagnostic distribuées et communicantes afin de détecter et localiser plus rapidement les défaillances et de les valider dans le contexte opérationnel du train.

Les présents travaux de doctorat, menés dans le cadre du FUI SURFER (SURveillance active Ferroviaire) coordonné par Bombardier, visent à proposer une démarche méthodologique d'évaluation de la sûreté de fonctionnement d'architectures de surveillance/diagnostic. Pour ce faire, une caractérisation et une modélisation génériques des architectures de surveillance/diagnostic basée sur le formalisme des Réseaux de Petri stochastiques ont été proposées. Ces modèles génériques intègrent les réseaux de communication (et les modes de défaillances associés) qui constituent un point dur des architectures de surveillance/diagnostic retenues. Les modèles proposés ont été implantés et validés théoriquement par simulation et une étude de sensibilité de ces architectures de surveillance/diagnostic à certains paramètres influents a été menée. Enfin, ces modèles génériques sont appliqués sur un cas réel du domaine ferroviaire, les systèmes accès voyageurs des trains, qui sont critiques en matière de disponibilité et diagnosticabilité.

Mots clés : Sûreté de fonctionnement, fiabilité, maintenabilité, disponibilité, étude de sensibilité d'architectures, surveillance, diagnostics distribués, réseaux de communication, modélisation réseaux de Petri stochastiques

Contribution to embedded monitoring/diagnosis architectures dependability assesment. Application to the railway transport.

Abstract : In the railway transport, rolling stock cost and availability are major concern. To optimise the maintenance cost of the railway transport system, one solution consists in better detecting and diagnosing failures. Today, centralized monitoring/diagnosis architectures reach their limits. Innovation is therefore necessary. This technological innovation may be implemented with embedded distributed and communicating monitoring/diagnosis architectures in order to faster detect and localize failures and to make a validation with respect to the train operational context.

The present research work, carried out as part of the SURFER FUI project (french acronym standing for railway active monitoring) lead by Bombardier, aim to propose a methodology to assess dependability of monitoring/diagnosis architectures. To this end, a caracterisation et une modélisation génériques des monitoring/diagnosis architectures based on the stochastic Petri Nets have been proposed. These generic models take into account communication networks (and the associated failure modes), which constitutes a central point of the studied monitoring/diagnosis architectures. The proposed models have been edited and theoretically validated by simulation. A sensitiveness of the monitoring/diagnosis architectures to parameters has been studied. Finally, these generic models have applied to a real case of the railway transport, train passenger access systems, which are critical in term of availability and diagnosability.

Keywords : Dependability, reliability, maintainability, availability, architectures sensitivity study, monitoring, distributed diagnosis, communication networks, stochastic Petri Nets modelling