THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par *l'Institut National Polytechnique de Toulouse*

Discipline ou spécialité : *Systèmes Industriels*

Présentée et soutenue par *ANNE-LISE BENABEN (née VILOTTE)*

Le 26 juin 2009

Méthodologie d'identification et d'évaluation de la sûreté de fonctionnement en phase de réponse à appel d'offre

---

JURY

M. Améziane AOUSSAT	Professeur des Universités	Rapporteur
M. Eric BONJOUR	Maître de conférences HDR	Rapporteur
Mme Claude BARON	Professeur des Universités	Présidente du jury
M. Gilles DELBREIL	Industriel	Membre
M. Abdessamad KOBI	Professeur des Universités	Membre
M. Daniel NOYES	Professeur des Universités	Directeur de thèse
M. François PERES	Maître de Conférences HDR	Co-Directeur de thèse

---

École doctorale : *Systèmes*
Unité de recherche : *Laboratoire Génie de Production de l'École Nationale d'Ingénieurs de Tarbes*
Directeur(s) de Thèse : *M. DANIEL NOYES ET M. FRANÇOIS PERES*

REMERCIEMENTS

Le travail rapporté dans ce mémoire a été réalisé dans le cadre d'une Convention Industrielle de Formation par la Recherche entre Continental Automotive France SAS et le Laboratoire Génie de Production de l'ENI de Tarbes.

Je tiens à remercier Monsieur Gilles DELBREIL pour m'avoir accueilli au sein de son service, pour m'avoir permis de mener mes travaux dans de bonnes conditions ainsi que pour le suivi de mon travail durant ces trois années. Je tiens également à remercier Messieurs Michel POURNAIN et Gilles MORISET pour leur encadrement tout au long de mon parcours.

Je souhaite témoigner toute ma gratitude à Daniel NOYES, d'une part, pour avoir accepté de prendre la responsabilité de directeur de recherche, et, d'autre part, pour ses qualités humaines. Il a su me guider tout au long de ma thèse endossant successivement les rôles de conseiller de recherche, d'examinateur critique pour m'aider à prendre du recul sur mes travaux et cela de manière toujours constructive et, enfin, il a su régulièrement m'aider à expliciter des idées enfouies ou difficiles à formuler pour arriver à l'aboutissement de mes travaux de recherche.

De la même manière, un grand merci à François PERES pour avoir endossé le rôle d'encadrant et pour ses qualités humaines. Il a su se préoccuper de mes travaux et de mon moral tout au long de mon parcours. Il a su me donner des conseils avisés qui m'ont permis d'avancer dans mes travaux tout en gardant la motivation nécessaire pour leur aboutissement.

Je tiens également à remercier Madame Claude BARON de m'avoir fait l'honneur de présider mon jury de soutenance.

Je suis très reconnaissante envers Monsieur Améziane AOUSSAT et Monsieur Eric BONJOUR d'avoir accepté d'étudier mes travaux et d'en être les rapporteurs.

Enfin, je remercie Monsieur Abdessamad KOBI et Monsieur Gilles DELBREIL d'avoir participé à mon jury de soutenance.

Au sein de Continental Automotive France SAS et plus particulièrement, de la Business Unit Chassis Components, je tiens à adresser des remerciements à l'ensemble du service Electronique. Dans le détail : merci à Claude et Philippe pour m'avoir soutenue dans mes moments de doute très tôt le matin. Merci à Daniel d'avoir partagé son expérience et de m'avoir accordé du temps même à des moments où il n'en avait pas trop. Un merci particulier pour le box 128 qui m'a supporté durant ma thèse : Matthias, Stéphane, Hans et Dimitri. Un merci à tous ceux que je n'ai pas cité ici.

Je tiens également à remercier toutes les personnes de la division Safety & Chassis de Toulouse qui m'ont

apporté leur aide ponctuelle tout au long de mon parcours que ce soit d'un point de vue technique, administratif ou de détente : Sandrine, Ericx2, Christophe, Alain, etc.

Je remercie aussi mes collègues du LGP que j'ai pu rencontrés lors de mes passages ponctuels au laboratoire ainsi que Cécile et Henriette pour leur aide dans les démarches administratives et le petit café du matin toujours servi avec le sourire et des petits gâteaux.

Ensuite, je souhaite remercier du plus profond de mon cœur mes parents. Ils m'ont apporté tout au long de ma scolarité leur aide et leur soutien. Un article du code civil précise que le rôle des parents est d'associer leurs enfants aux décisions qui les concernent, mes parents m'ont toujours laissé le choix dans mes décisions et ils ont su me guider dans la voie que j'ai choisie.
Merci aussi à mes proches : papi, mami, Mathieu, Géraldine, Lysiane, Frédérick, Seb, Danielle, Robert et Christiane, mes neveux et nièces : Enzo, Nino et Luz, et tout ce que je n'ai pas cité pour leur soutien.
Une spéciale dédicace à Patrick dont la phrase fétiche m'a aidé à tenir le coup notamment dans les moments difficiles : "Tant qu'on n'est pas arrivé, on n'est pas arrivé !".

Pour les moments de détente, un merci particulier à Vincent et Olivier pour nos soirées de printemps et d'été.

Enfin, merci à mon soutien quotidien Julien qui a du supporter plus que les autres mes doutes, mes difficultés, ma mauvaise humeur mais aussi les bons moments. Tu as cru en moi à chaque instant et tu as su m'en convaincre. Je te dédie ce mémoire avec tout mon amour.

A ma grand-mère grâce à laquelle je serais toujours une petite princesse....

A mon bon-papa pour son sens de l'humour....

TABLE DES MATIERES

TABLE DES FIGURES

TABLE DES TABLEAUX

INTRODUCTION GENERALE

La sûreté de fonctionnement (SdF) des produits, des processus et des services est une préoccupation permanente de tous les acteurs industriels. C'est le cas notamment dans le secteur automobile à l'exemple des équipementiers confrontés à des clients de plus en plus exigeants en matière de sûreté de fonctionnement. Jusqu'alors uniquement intéressé par les résultats, le client requiert aujourd'hui, dès les négociations couplées à l'appel d'offre (AO), une information précise sur la démarche même que le fournisseur prévoit de mettre en place pour satisfaire aux exigences SdF.

Conscients de ces nouveaux besoins, nous nous sommes intéressés à la problématique d'identification de la "dimension SdF" du produit au stade de l'AO et à l'évaluation de l'impact économique de son intégration au développement futur du produit. Les conséquences de la prise en compte de la SdF sont doubles puisqu'elles concernent à la fois le produit qui voit sa robustesse optimisée mais aussi la démarche d'analyse permettant de dimensionner les solutions appropriées.

Les produits considérés dans le cadre de notre travail sont des équipements mécatroniques embarqués. Initialement dédiés aux fonctions de confort du véhicule (climatisation,...), ces produits sont très souvent associés aujourd'hui à des fonctions de sécurité (freinage, direction,...) et revêtent, de ce fait, une importance majeure en termes de SdF. De plus, ils sont soumis au respect des normes de sécurité fonctionnelle (IEC 61508 en vigueur et ISO 26262 à paraître) qui fixent des niveaux d'intégrité de sécurité (SIL ou ASIL) à valider par rapport à des objectifs de sécurité fixés.

Une gestion efficace de la sûreté de fonctionnement nécessite l'intégration des éléments relatifs à la SdF tout au long du cycle de vie du produit. Cela passe par la définition et l'expression au plus tôt dans la vie du produit des objectifs à atteindre et par la mise en place d'une équipe pluridisciplinaire composée de représentants des différents métiers de l'entreprise pour la définition, la vérification et la validation de ces objectifs. Plus l'intégration de la dimension SdF interviendra tôt dans le cycle de vie du produit, moins il y aura de risque de surcoût vis à vis de modifications liées aux non-conformités. Si la SdF est encore considérée comme une contrainte, la prise en compte des besoins en terme de sûreté dès la réception des premiers cahiers des charges doit lui conférer le statut d'objectif de premier niveau.

Les méthodologies existantes pour le traitement de la SdF sont généralement déployées au début du cycle de développement du produit mais en aval du processus de réponse à appel d'offre (PRAO) et elles engagent des outils classiques d'évaluation prévisionnelle et d'analyse tels les outils SdF, les réseaux de Petri, les graphes de Markov ou autres langages de programmation avancés. Ces outils nécessitent une connaissance déjà bien précise de l'architecture du produit ce qui n'est pas le cas de la phase d'acquisition dans laquelle cette étude est positionnée. Ces constats nous ont incités à formuler un objectif de spécification d'une démarche instrumentée centrée sur la phase d'appel d'offre et

assistée par les acteurs projets pour la prise en compte de la dimension SdF dès le stade du processus de réponse à appel d'offre (PRAO).

La prise en compte dès le PRAO de la dimension SdF est contraignante. Le temps imparti pour mener à bien les études est court (de l'ordre de quelques semaines), le produit n'existe pas encore, les exigences client (exprimées dans le dossier d'AO) sont hétérogènes. Malgré ces difficultés, il faut convaincre le client du bien fondé des actions qui seront entreprises au niveau de la sûreté des produits.

Prenant en compte toutes les contraintes précédentes, nos travaux s'attachent à la proposition d'une organisation du PRAO en différentes étapes instrumentées allant de l'identification des éléments relatifs à la SdF dans les documents clients fournis pour l'AO à la définition et à l'évaluation de l'impact SdF. Deux aspects sont considérés dans le cadre de cette étude :

- le premier a trait aux conséquences sur le produit de la prise en compte des exigences SdF par le biais d'analyses accélérées réalisées durant le PRAO pour chiffrer l'impact sur le coût final du produit,
- le second concerne le dimensionnement de la charge de travail relative au traitement des exigences SdF durant le développement futur : ressources nécessaires à la réalisation des différentes études, durée et coût de ces études.

Pour arriver à caractériser l'impact SdF, nous avons considéré plusieurs plans d'abstraction relativement :

- au "Contexte" pour la prise en compte des contraintes inhérentes à l'environnement d'instanciation de l'organisation du PRAO préconisée : déroulement du PRAO, activités du concepteur dans le PRAO, identification du niveau d'intégration de la SdF dans le cycle de vie, définition d'une démarche de gestion SdF à partir de méthodes usuelles au sein des entreprises, ...,
- à l'"Organisation du PRAO" consistant à la définition des différentes étapes faisant progresser des exigences client vers le coût de la SdF. Cette organisation permet, à la fois, de structurer la démarche de gestion de la SdF dans le PRAO mais aussi de capitaliser la démarche et les choix du concepteur,
- à l'"Instrumentation de l'organisation" qui fixe les principes d'instanciation des différentes étapes de l'instrumentation,
- aux "Supports d'instrumentation" permettant l'identification des connaissances disponibles dans une entreprise, susceptibles d'être utilisées pour l'instrumentation, et des connaissances ou supports de connaissances à créer pour doter la solution de toutes les caractéristiques définies.

La définition de l'organisation a permis de mettre en évidence l'importance, pour le PRAO, de garantir un niveau d'abstraction élevé pour la représentation du produit, celui-ci n'existant pas et, d'autre part, d'intégrer facilement les caractéristiques SdF puisque c'est cette "dimension" du produit qui nous intéresse prioritairement. Dans cet objectif, une partie du travail a consisté à établir un formalisme de représentation du produit permettant :

- la compréhension de la représentation par l'ensemble des acteurs projets,
- l'intégration des degrés de liberté du concepteur dans la création du concept de solution (puisque les principaux concepts de la solution sont fixés dans le PRAO pour permettre l'évaluation du coût du produit),
- l'intégration des caractéristiques et de la connaissance SdF du produit.

Le mémoire de thèse est organisé en quatre chapitres,
Dans le premier chapitre, nous exposons le contexte général des travaux, la problématique de recherche, sa formalisation et le positionnement parmi les travaux scientifiques afférents.

Nous développons dans le second chapitre l'organisation que nous proposons pour le PRAO afin de structurer la démarche d'analyse des contraintes SdF. Cette organisation comporte différentes étapes qui, à partir des documents client fournis dans le dossier de réponse à l'AO, vont progressivement conduire à l'évaluation économique de la prise en compte des exigences SdF du client dans le projet.
Cette organisation nécessite des supports d'instrumentation rendant la démarche reproductible et facilement applicable.

Une part importante du développement des supports concerne ceux dédiés à une étape clef d'analyse d'impact SdF, l'étape Projection. Le troisième chapitre est consacré aux modèles intégrant la SdF développés à cet effet. Ces modèles ont été établis en regard des produits existants de l'entreprise partenaire ainsi qu'à partir de travaux existants concernant les systèmes embarqués du monde automobile.
L'étude et l'analyse des différentes représentations d'un produit nous ont fait nous orienter vers un modèle matriciel qui présente l'avantage d'une forme visuelle facilement intelligible par les acteurs des différents métiers de l'entreprise et qui satisfait aux principales exigences que nous mettrons en avant dans la recherche de solution.

Le dernier chapitre est consacré au couplage entre les modèles développés et l'organisation proposée dans l'objectif de définir l'impact de la prise en compte des exigences SdF dans un projet et d'évaluer le coût de cet impact à différents niveaux : sur le produit et la démarche à mettre en place. Nous exposons la méthode permettant l'évaluation et le dimensionnement de l'impact SdF sous la forme d'activité à déployer dans deux étapes clés de l'organisation proposée et illustrons le déploiement de celle-ci.

I. Chapitre 1 : Contexte et Problématique

1. Introduction

Les travaux présentés dans ce mémoire se placent dans le contexte de l'industrie automobile. La problématique émane de l'augmentation de la criticité des caractéristiques de sûreté de fonctionnement des systèmes embarqués automobile. Ces systèmes, initialement dédiés aux fonctions de confort induisaient par leur non fonctionnement une simple gêne pour l'utilisateur ; utilisés aujourd'hui pour la sécurité du véhicule (freinage, traction, régulation de vitesse...), leur défaillance peut avoir des conséquences très graves pour les usagers.

Dans l'automobile, la prise de conscience a débuté chez les constructeurs il y a une dizaine d'années et s'est ensuite propagée par étape chez les fournisseurs. La thèse s'inscrit dans le cadre d'une problématique d'affichage du savoir-faire sûreté de fonctionnement pour le client et de prise en compte des caractéristiques SdF du produit dans son cycle de vie.

Le travail a débuté par une analyse du contexte et des paramètres du problème afin d'arriver à la formalisation de la problématique. Cette analyse a permis de déboucher sur la nécessité de définir une méthodologie de prise en compte de la sûreté de fonctionnement, dès le premier contact avec le client, dans les phases de réponse à appel d'offre. De façon plus générale, l'objectif est de proposer une approche permettant l'organisation des phases de réponse à appel d'offre ayant pour finalité d'évaluer l'impact de la dimension sûreté de fonctionnement au sein d'un projet de développement de produit.

La résolution de la problématique générale passe par l'identification des besoins réels en termes d'organisation et par une phase d'analyse des contraintes relatives à l'intégration des solutions dans une organisation industrielle pour déboucher sur la proposition d'une solution instrumentée de gestion de la SdF.

Nous présentons, dans ce chapitre, en lien avec l'étude que nous menons, les paramètres du contexte de l'industrie automobile et son organisation. Nous nous intéressons ensuite à l'analyse du problème et à sa formulation scientifique.

2. Problématique industrielle

2.1. L'industrie automobile

L'industrie automobile est un secteur organisé selon un modèle pyramidal de sous-traitance [Frigant&al, 01]. Le premier niveau est celui des constructeurs (généralement dénommés "O.E.M". pour Original Equipment Manufacturer) qui sont les donneurs d'ordre. Les équipementiers de rang 1 (dénommés "Tiers-1") apparaissent au niveau suivant. Ils fournissent des systèmes complets aux constructeurs. On trouve ensuite au troisième niveau les équipementiers (ou fournisseurs) de rang 2 (dénommés "tiers-2",). Ce niveau est constitué d'entreprises très variées, fournisseurs ou sous-

traitants du niveau supérieur. Ce mode de fonctionnement peut ensuite être décliné en autant de niveaux que de rangs concernés par l'organisation industrielle mise en place. On parlera alors de « tiers-n » pour les entreprises apparaissant au rang n.

Cette industrie a évolué au cours du temps pour passer d'un mode de fonctionnement inter-niveaux à une organisation dans laquelle existent des relations intra-niveaux, plus particulièrement dans les niveaux 2 et 3 comme schématisé sur la Figure I-1 [Le-Bars, 08].

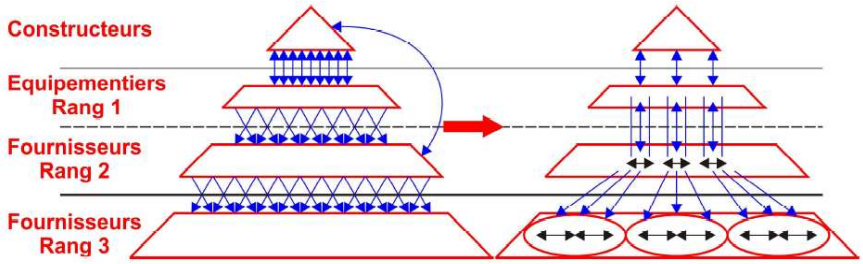


Figure I-1 : Organisation de l'industrie automobile

L'industrie automobile est constituée d'une multitude d'entreprises dont nous allons maintenant exposer l'organisation.
Dans la suite du mémoire, nous appellerons "client" l'entreprise qui provoque la relation dans le cadre du développement d'un produit (par l'envoi d'un appel d'offre par exemple) et "prestataire" l'entreprise (ou les entreprises) qui fournit (fournissent) tout ou partie du système. L'entreprise délivrant uniquement des composants sera qualifiée de "fournisseur". Enfin, nous utiliserons le vocable « entreprise partenaire » pour faire référence à la structure commanditaire de ce travail, en l'occurrence la société Siemens VDO[1].

2.2. Les entreprises du secteur

A l'intérieur de cette structure industrielle, on trouve des entreprises organisées selon différents modèles. Il existe trois types de structures organisationnelles pour une entreprise [Guide PMBOK, 00].
Le premier type de structure, dit "structure fonctionnelle" (Figure I-2a), est basé sur la décomposition de l'entreprise en départements relatifs à des fonctions ou à des spécialisations (production, ressources humaines, ingénierie, commercialisation,...,). La fonction ingénierie peut elle-même être divisée en unités fonctionnelles (mécaniques, informatiques,...). Dans ce type d'organisation, les projets sont gérés par les unités fonctionnelles. Lorsqu'il y a des besoins vis à vis d'une autre entité fonctionnelle, les demandes sont transmises par le biais de la hiérarchie.
Le second type d'organisation possible, correspond à la "structure par projet" (Figure I-2b). Dans cette configuration, tous les acteurs travaillent pour un même projet piloté par un responsable. Il peut cependant exister, dans ce type d'organisation, des fonctions supports dépendant d'un chef de projet ou intervenant transversalement sur différents projets.
Enfin, le dernier type d'organisation, dit "structure matricielle" (Figure I-2c), est une combinaison des principes des deux

[1] Siemens VDO ayant été rachetée par Continental Corporation en 2008, il se peut que certains documents fassent donc référence à cette nouvelle structure.

structures précédentes. Il existe trois structures matricielles :

- la structure matricielle faible : elle possède de nombreuses caractéristiques de l'organisation fonctionnelle. La particularité majeure vient du fait que les échanges ne passent pas par la hiérarchie,
- la structure matricielle équilibrée : elle est identique à la précédente à la différence près qu'il existe un chef de projet à temps plein assurant la coordination des tâches,
- la structure matricielle forte : elle est assez proche d'une organisation par projet mais, dans ce type de structure, il existe une entité fonctionnelle "chef de projet" qui a autorité fonctionnelle sur le personnel du projet.

Nous illustrons sur la Figure I-2 les différents types d'organisation. Les rectangles noirs représentent le personnel impliqué dans le projet, les encadrements pointillés caractérisent la coordination et l'intégration du projet dans la structure.

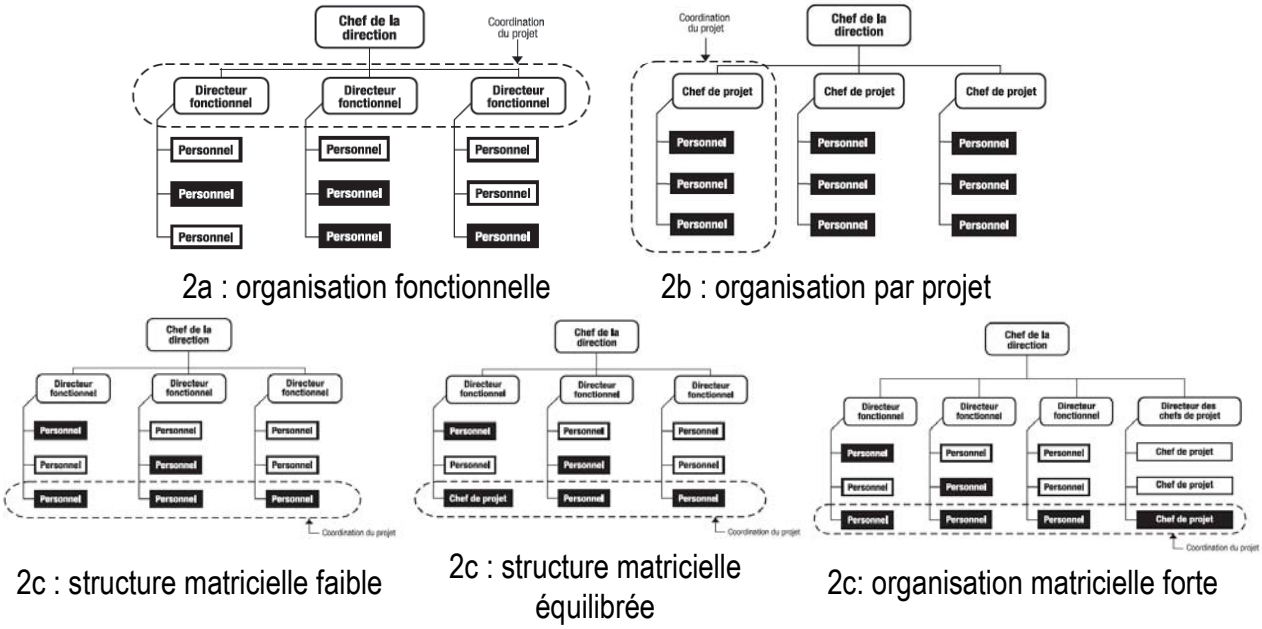


Figure I-2 : Différents types de structures organisationnelles [Guide PMBOK, 00]

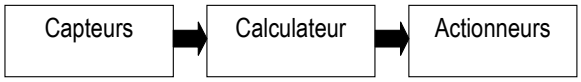
Après avoir succinctement présenté les modes possibles d'organisation d'une structure industrielle du secteur automobile, nous présentons à la suite les caractéristiques des produits cibles de notre étude.

2.3. Les systèmes embarqués automobiles et leurs caractéristiques

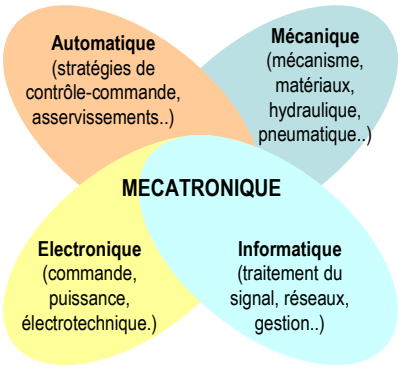
Les systèmes embarqués automobiles sont généralement répartis en quatre domaines relatifs aux différentes fonctions que l'on peut trouver dans un véhicule : le domaine Châssis, le domaine Télématique et Multimédia, le domaine Contrôle moteur et enfin le domaine Habitacle [Simonot-Lion&al, 06]. D'autres intitulés de domaines ou des structurations différentes peuvent être parfois utilisés mais cette définition est la plus générique. C'est donc celle que nous conserverons.

Le domaine "Châssis" comprend les systèmes tels que la suspension, la direction assistée, le freinage, etc. Le domaine "Télématique et Multimédia" intègre les systèmes sur lesquels l'utilisateur peut interagir : télécommunication, GPS, multimédia (image et son), etc. Le domaine "contrôle moteur" englobe tous les systèmes liés à la motorisation du véhicule et enfin, le domaine "habitacle" regroupe les systèmes de confort du véhicule (sièges, éclairage, vitres, portes).

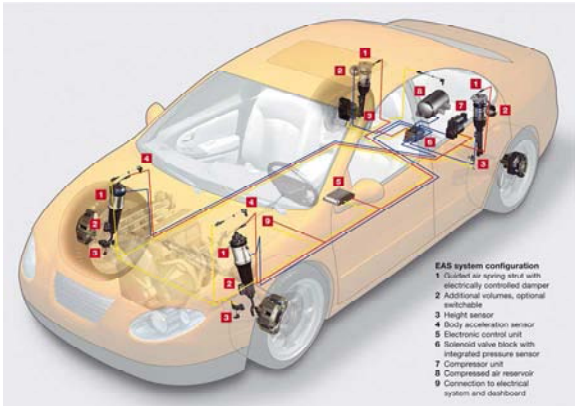
L'ensemble des systèmes de ces quatre domaines sont des systèmes embarqués composés à un haut niveau d'un calculateur, de capteurs qui fournissent les informations au calculateur et d'actionneurs commandés par le calculateur (Figure I-3a). Ils sont constitués d'éléments électroniques, mécaniques et logiciels qui en font des systèmes mécatroniques (Figure I-3b) intégrés au véhicule (Figure I-3c) : exemple d'un système de suspension complet issu de http://mediacenter.conti-online.com).



3a : composition d'un système embarqué



3b : champs disciplinaires de la mécatronique



3c : système de suspension

Figure I-3 : Systèmes automobiles

Les spécificités des systèmes embarqués [Simeu, 05] sont liées :

- à leur complexité et leur hétérogénéité du fait des composants qu'ils contiennent,
- aux contraintes fortes imposées en termes de coût de revient et de consommation,
- à l'environnement critique dans lequel ils évoluent : vibrations, humidité,...,
- à la sécurité et à la fiabilité imposées par les fonctions qu'ils remplissent.

La caractéristique que nous considérerons plus particulièrement dans le cadre de ce travail est la criticité relative à la sûreté de fonctionnement de ces systèmes. Quel que soit le domaine concerné, les systèmes doivent être fiables et intégrer des fonctions de sécurité évitant la mise en danger de l'utilisateur. Si ces paramètres ne sont pas respectés dans le cadre de produits de grande série tels que les systèmes embarqués dans les véhicules, les conséquences peuvent être très graves sur le plan de l'intégrité de l'utilisateur, de son matériel et de son environnement. De plus, les problèmes liés à la sécurité ont un impact négatif sur l'image du constructeur, notamment, dans le cas d'une médiatisation de ce type d'incident. La sécurité et la fiabilité sont donc des enjeux importants à prendre très au sérieux pour éviter des désagréments causés par des procès, des pénalités financières ou autres campagnes médiatiques peu flatteuses (notamment dans le cas de rappel de véhicule) [Blancart, 07].

Ces impératifs vont également dans le sens de la législation puisque les constructeurs ont l'obligation de ne mettre sur le marché que des produits sûrs (article 3 de la directive 2001/95/CE transposée en 2004). Un produit sûr est défini comme "...tout produit qui, dans des conditions d'utilisation normales ou raisonnablement prévisibles,..., ne présente aucun risque ou seulement des risques réduits à un niveau bas, compatibles avec l'utilisation du produit et considérés comme acceptables dans le respect d'un niveau élevé de protection de la santé et de la sécurité des personnes..." [Bracquemond, 07].

Finalement, ces systèmes, par les fonctions qu'ils remplissent, sont soumis au respect de normes spécifiques en termes de sécurité fonctionnelle, notamment la norme IEC 61508 : Sécurité fonctionnelle des systèmes électriques, électroniques et électro-programmables de sécurité[2]. Cette norme fixe des niveaux de sécurité correspondant à l'atteinte d'objectifs de sécurité (prescriptions pour le développement de ces systèmes, plages de valeurs à respecter pour les métriques représentatives,...). Elle est générique et s'applique à un certain nombre de secteurs, induisant par contrecoup, des difficultés d'instanciation dans un domaine spécifique, notamment, dans le secteur automobile où les systèmes intègrent des fonctions pluridisciplinaires. Pour ces raisons, une norme est en cours d'élaboration : l'ISO 26262, déclinaison de la précédente destinée au secteur automobile.

Nous avons, dans cette première partie, introduit le cadre industriel dans lequel s'inscrivent les travaux scientifiques que nous avons engagés. Nous abordons maintenant la description de la problématique sur laquelle a porté notre réflexion.

2.4. Problématique industrielle

Les travaux et activités effectués dans le cadre du développement d'un projet imposent le respect de spécifications fortes en matière de sûreté de fonctionnement : SIL (Safety Integrity Level), niveaux de fiabilité, sécurité,… spécifications qui rejoignent les préoccupations récurrentes d'amélioration de la disponibilité opérationnelle et de maîtrise du coût global de possession.

L'expertise des acteurs d'une équipe projet en sûreté de fonctionnement n'est pas toujours explicite ; il en est de même des méthodes et techniques engagées au cours du développement pour répondre à ces contraintes de sûreté de fonctionnement.

Le cycle du projet (couplé au cycle de commercialisation du produit) comporte trois étapes principales :

- une phase d'acquisition,
- une phase de développement,
- une phase de production.

L'étape d'acquisition est décisive dans le sens où elle conditionne très largement la décision de démarrage du développement du produit (près de 90% des projets sont abandonnés avant). De plus, elle fixe de façon quasi-définitive la marge d'évolution du projet sachant qu'à ce stade, les incertitudes et les risques sont encore mal cernés et le niveau de connaissance encore faible.

Dans l'entreprise partenaire, les produits sont développés selon un modèle itératif conduisant à la réalisation d'un certain nombre de prototypes :

- prototype A : produit représentatif de la fonction à réaliser mais non astreint à des spécifications de "sûreté de fonctionnement",

[2] Il s'agit de systèmes mettant en œuvre les fonctions de sécurité requises pour que l'équipement commandé atteigne ou maintienne un état de sécurité ou qui atteignent eux-mêmes le niveau d'intégrité de sécurité nécessaire à la mise en œuvre des fonctions de sécurité requises [IEC 61508-4].

- prototype B : prototype de type A (fonctionnalités de base), satisfaisant aussi les aspects sécurité et diagnostic mais non engagé en production industrielle,
- prototype C : prototype de type B satisfaisant aux critères de production industrielle.

L'organisation de l'entreprise partenaire est de type "matriciel fort". L'équipe projet type est pluridisciplinaire ; elle réunit un chef de projet et un représentant de chaque métier contribuant à la réalisation du produit : ingénieur électronique, ingénieur logiciel, ingénieur électricien, ingénieur manufacturing/méthode, ingénieur qualité, etc.

L'expertise sûreté de fonctionnement dans le contexte que nous avons étudié n'est pas explicite ; elle est diffuse (répartie entre les membres de l'équipe projet) et inégalement répartie selon les métiers.

Une partie de l'expertise est distribuée dans plusieurs bases de données :

- BD composants (défauts sur les composants, données établies en production, chez le client ou en SAV),
- BD "leçons apprises" en fin de projet (capitalisation sur l'expérience projet),
- BD sur les résultats de test en production,
- BD en exploitation chez le client et en SAV.

Dans ce contexte, l'entreprise veut uniformiser la prise en compte de la sûreté de fonctionnement et afficher son savoir-faire au client dès les premiers contacts commerciaux, dans les phases de réponse à appel d'offre. Dans cette optique, il est important de pouvoir s'appuyer sur une méthodologie générique. L'objectif final est de permettre la prise en compte et le traitement efficace des caractéristiques de sûreté de fonctionnement du produit au plus tôt dans le cycle de vie et dans le respect de l'organisation industrielle en place et déjà éprouvée.

3. Formulation du problème

3.1. Revue des contraintes du problème

L'organisation de l'industrie automobile sous forme pyramidale induit certains effets sur les entreprises concernées. Tout d'abord, les constructeurs sont le moteur du marché puisqu'ils sont à l'origine des appels d'offres originels.

Dans les entreprises, la connaissance sûreté de fonctionnement n'est pas souvent formalisée. De plus, la discipline SdF étant récente, lors de la cotation d'un nouveau produit ou d'une évolution de celui-ci, les acteurs ne disposent pas d'un recul suffisant sur les produits précédents.

Les constructeurs ont été les premiers à prendre conscience de l'importance de la SdF et se sont organisés en conséquence afin d'intégrer cette caractéristique dans la spécification de leurs produits. Le décalage temporel lié à la transmission progressive de ces contraintes vers les équipementiers et fournisseurs des rangs inférieurs et la complexité des réseaux d'entreprises impliquées dans un même projet (Figure I-4) a conduit à une hétérogénéité dans les modes de prise en compte des notions de sûreté de fonctionnement. Il est donc difficile d'homogénéiser la connaissance et les pratiques en termes de sûreté de fonctionnement.

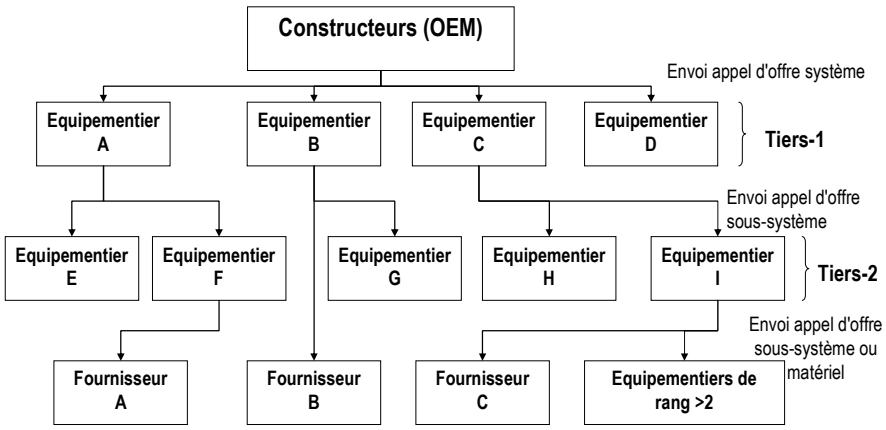


Figure I-4 : Propagation de contraintes sur un réseau d'entreprise

Entre chaque niveau hiérarchique, la transmission des exigences peut donner lieu à des interprétations. Les contraintes SdF sont ainsi susceptibles de ne pas être considérées sur un même référentiel selon l'industriel ou le projet concerné.
Sur le plan de l'organisation industrielle, nous avons constaté que le fonctionnement de l'entreprise pour laquelle nous travaillions privilégiait souvent une organisation matricielle de ses ressources, croisant équipes « métiers » et équipes « projets ». L'équipe projet, support de réalisation du cycle de développement du produit, réunit les compétences de métiers complémentaires. Elle est donc généralement pluridisciplinaire. Cela entraîne une variabilité dans la composition des équipes puisque les ressources sont affectées en fonction de la charge de travail à l'instant d'affectation.

Une autre particularité est liée au type même de produits développés et, plus particulièrement, à la pluridisciplinarité induite par ces produits qui constitue une caractéristique forte de la problématique. La spécificité de chaque métier implique en effet des approches distinctes dans le traitement de la SdF et impose l'engagement de méthodes et outils différents en fonction des disciplines concernées mais utilisés malgré tout dans un objectif commun de sûreté de fonctionnement.

La dernière contrainte considérée dans le cadre de ce travail concerne le renforcement des exigences clients sur la sûreté de fonctionnement. Jusqu'alors intéressés par les résultats finaux relatifs à la performance sûreté de fonctionnement des produits, le client requiert aujourd'hui des garanties sur la démarche même suivie par le fournisseur pour atteindre les objectifs SdF fixés au niveau du cahier des charges. Ce dernier point nécessite de traiter les exigences au plus tôt pendant le cycle de vie afin d'assurer au client, par une démonstration probante, un véritable savoir-faire de l'entreprise en terme de réalisation de la performance SdF attendue.

Nous prolongeons cette revue des contraintes par un constat sur l'engagement des méthodes SdF dans le cycle de vie du produit. Les méthodes et outils d'évaluation des risques sont en effet, déployés durant la phase de développement, phase postérieure à la phase d'acquisition (acquisition du cahier des charges (CdC) et des exigences client) et peuvent conduire à identifier tardivement dans le projet des éléments importants à prendre en compte pour assurer le niveau de sûreté de fonctionnement désiré.

L'ensemble des points identifiés permet de mettre en relief l'intérêt de la prise en compte de la SdF dès le processus de

réponse à appel d'offre. Les contraintes étant intégrées au démarrage du projet, il sera, par la même, bien plus facile d'afficher un savoir faire SdF, préparer les traitements utiles au développement futur et, donc, maîtriser l'ensemble du cycle d'application de la SdF.

3.2. Caractérisation du problème

Nous formalisons dans cette partie les conclusions de l'état des lieux qui a été réalisé dans l'entreprise partenaire, dans l'objectif de positionner le problème et d'établir les pistes d'actions pour le résoudre. L'analyse effectuée sous forme d'interview des acteurs projets de l'entreprise a concerné différents points.

Le travail a consisté en la définition d'un support pour ces interviews sous la forme d'un questionnaire dont les réponses sont orientées (choix multiples) ou libres. Le questionnaire a été construit par rapport à un état préliminaire des lieux dont l'objectif était d'identifier les éléments relatifs à la SdF dans l'entreprise partenaire. Il est présenté dans l'annexe I-A. Le questionnaire ayant pour finalité d'identifier les connaissances des acteurs projet par rapport à l'existant.

L'interview des différents acteurs a été menée sur un panel de 44 personnes représentant les différentes fonctions de l'entreprise :

- des ingénieurs et techniciens en électronique (nombre : 10),
- des ingénieurs et techniciens en logiciel (nombre : 18),
- des ingénieurs et techniciens en mécanique (nombre : 5),
- des ingénieurs et techniciens en qualité (nombre : 3),
- des chefs de projets (nombre : 5),
- des chefs de service : électronique, logiciel et mécanique (nombre : 3)

Les interviews se sont déroulées sous la forme d'entrevue de trente minutes.

Suite à ces entrevues, un bilan a été proposé. Nous présentons uniquement les conclusions de ce bilan ainsi qu'une généralisation des pistes d'actions en fonction du type de problème mis en évidence.

Dans l'objectif de prendre en compte les caractéristiques SdF, il apparaît tout d'abord essentiel d'identifier les activités, méthodes et outils relatifs à la SdF présents dans le cycle de développement.

La variabilité continue des équipes projets dans une organisation industrielle en "structure projet" induit deux difficultés liées à la complexité d'identification des connaissances/compétences :

- requises pour la réalisation des objectifs, compte tenu de la diversification des points de vue,
- disponibles dans l'équipe projet, compte tenu de la variabilité de composition de cette équipe.

Dans cette optique, nous nous sommes intéressés à la connaissance SdF des acteurs projets et à leurs compétences dans ce domaine. Cette étude a permis de formaliser le problème en sept plans gradués en fonction de la caractéristique qu'ils représentent. Ces plans correspondent :

- au niveau d'intégration de la SdF dans le cycle de développement 1 qui peut être élevé, moyen ou faible,
- à la cartographie des méthodes, démarches et outils permettant le traitement et la gestion de la sûreté de fonctionnement 2 qui peut être complète, incomplète ou inexistante,

- à la connaissance SdF des acteurs projets, tous métiers confondus, 3 qui peut être à un niveau bas, moyen et élevé,
- à la caractérisation de la connaissance en termes d'hétérogénéité, de distribution et de diversification 4 exprimées en niveau bas, moyen ou élevé,
- à l'utilisation des éléments relatifs à la SdF dans les projets 5, utilisation qui peut être courante, occasionnelle ou inexistante,
- à la formation des acteurs aux méthodes et outils SdF 6. Cette formation peut être de niveau bas, moyen ou élevé en fonction du taux de formation SdF des acteurs projets,
- à la diversification des supports d'expertise et de connaissance de l'entreprise 7 étudiés via les bases de données de l'entreprise, de leur utilisation et de leur type qui peut être de niveau bas, moyen ou élevé.

Nous illustrons sur la Figure I-5 un exemple de bilan SdF dans une entreprise, ce bilan est une vue à haut niveau (pour des raisons de confidentialité) du bilan effectué dans l'entreprise partenaire. Nous exposons, sur la base de ce travail d'analyse, les pistes d'actions et d'améliorations en fonction des problèmes identifiés.

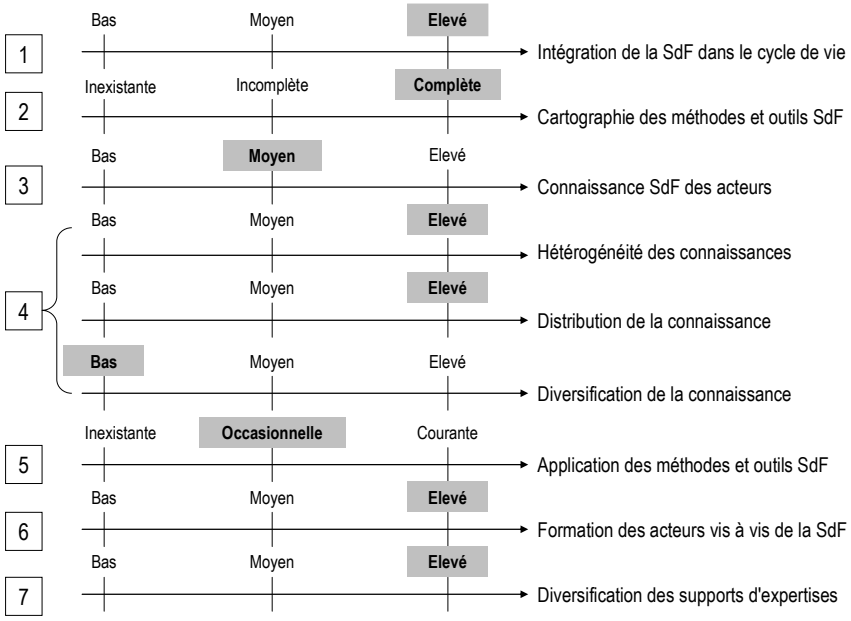


Figure I-5 : Bilan SdF

3.3. Pistes d'actions

Nous reprenons les différents éléments structurants identifiés lors de la réalisation du bilan SdF dans l'entreprise partenaire et proposons pour chacun des voies d'exploration possibles.

L'**intégration** de la SdF dans le cycle de vie est très étroitement liée au système de management de la qualité de l'entreprise. Dans le cadre d'une intégration basse ou moyenne, l'amélioration peut être réalisée soit en complétant le système de management de la qualité soit par le biais d'une vérification de la couverture du cycle de vie SdF par les méthodes et outils disponibles dans l'entreprise.

Concernant la **cartographie** des méthodes et outils SdF, l'entreprise doit disposer d'une panoplie suffisante afin d'identifier les risques, évaluer leur gravité et leur fréquence et vérifier qu'ils ont effectivement été pris en compte dans l'étude concernée. Dans l'étude que nous avons réalisée, les supports nécessaires à la gestion de la SdF étaient disponibles. Dans le cas d'un portefeuille méthodologique vide ou insuffisamment fourni, il aurait fallu définir et implémenter les méthodes et outils utiles aux concepteurs.

Au niveau de la **connaissance** SdF et de ses caractéristiques, de nombreux problèmes peuvent être soulevés.

Le point le plus critique concerne l'**hétérogénéité** de la connaissance et les différences observées vis-à-vis de la capacité à caractériser le niveau de sûreté de fonctionnement lié au développement d'une solution technique en fonction des métiers. L'atteinte d'un niveau élevé de sûreté de fonctionnement n'implique pas une homogénéisation de la connaissance, non obligatoirement répartie de façon homogène sur l'ensemble des acteurs projets. Prenons l'exemple d'une carte électronique et du logiciel qui permet d'assurer son fonctionnement. Si la défaillance électronique (perte d'un composant, par exemple) est relativement intuitive, les aléas de fonctionnement du logiciel s'avèrent eux beaucoup plus difficiles à identifier. Un moyen possible pour lisser cette hétérogénéité est la constitution systématique d'équipes pluridisciplinaires pour la réalisation des analyses SdF. Dans le cadre d'un niveau bas, le niveau de connaissance est alors distribué de façon homogène entre les métiers. Pour un niveau moyen, les différences ne sont pas trop importantes et peuvent être lissées de la même façon que pour le niveau haut.

La **distribution** concerne la répartition entre les acteurs d'un même métier. Une distribution basse indique souvent que la connaissance SdF repose sur une seule personne au sein d'un métier, généralement le "pilote métier[3]". Cette forme de répartition des rôles n'est pas gênante si l'ensemble des acteurs dispose malgré tout d'une connaissance minimale du domaine de la sûreté de fonctionnement. A l'opposé, une distribution élevée traduit un lissage de la connaissance sur les membres de l'équipe projet.

La **diversification** concerne l'étendue des éléments connus relatifs à la SdF. Elle est jugée élevée si la connaissance est large, elle est faible dans le cas contraire. Cette diversification est largement corrélée à l'application des méthodes et outils de la SdF. Par exemple, l'analyse des modes de défaillances de leurs effets et de leur criticité (AMDEC) est une méthode très répandue, généralement imposée par le client, pour l'ensemble des produits. De ce fait, elle est connue de tous les acteurs. Les autres méthodes et outils disponibles sont moins cités par les acteurs projets. Cette situation peut être améliorée par deux voies : la généralisation de l'application des méthodes et la formation des acteurs.

L'**application** des méthodes est fonction des directives de l'entreprise ; elle sera d'autant meilleure que la SdF sera intégrée dans le cycle de vie du produit. L'amélioration de cette caractéristique passe par la définition de règles d'usage pour tous les projets. Cette caractéristique, lorsqu'elle est haute, permet d'augmenter progressivement la connaissance SdF des acteurs. La mise à disposition de connaissance peut être amplifiée par la définition de règles de conduite visant à réutiliser des études antérieures pour faciliter les applications futures.

[3] Le pilote métier dans un projet assure une fonction métier ainsi qu'une fonction de manager envers les autres membres du métier concerné.

Le niveau de **formation** des acteurs dépend directement des choix stratégiques de l'entreprise et de sa volonté de placer la sûreté de fonctionnement au cœur des préoccupations. Nous avons noté durant notre analyse qu'une partie conséquente des acteurs projet (tous métiers confondus) avaient suivi ou prévu une formation liée à la SdF. A court terme, cela permet d'uniformiser la connaissance entre les acteurs.

Enfin, le point concernant la **diversification des supports d'expertise** est important car la SdF est une discipline pluridisciplinaire qui nécessite le partage et la mutualisation des connaissances. Celles-ci peuvent être véhiculées par des supports appropriés caractérisant la culture de l'entreprise. Un niveau élevé correspond à une panoplie de supports très importants mais non forcément partagés. Notre analyse a montré que, dans le cas étudié, les supports d'expertise étaient principalement des supports métiers.

Nous montrons sur la Figure I-6 l'imbrication et les dépendances entre les caractéristiques que nous venons d'introduire relatives au niveau global de connaissance et de pratique de l'entreprise sur le plan de la sûreté de fonctionnement. Ce schéma ne reprend pas les caractéristiques détaillées de la connaissance 4 (hétérogénéité, distribution, diversification) car elles ne sont pas liées directement aux autres plans, c'est le niveau de connaissance SdF des acteurs 3 qui est relié aux autres plans. Chaque flèche indique que l'augmentation du niveau d'une caractéristique à la base de la flèche permet d'augmenter le niveau de celle qui est à l'autre extrémité.

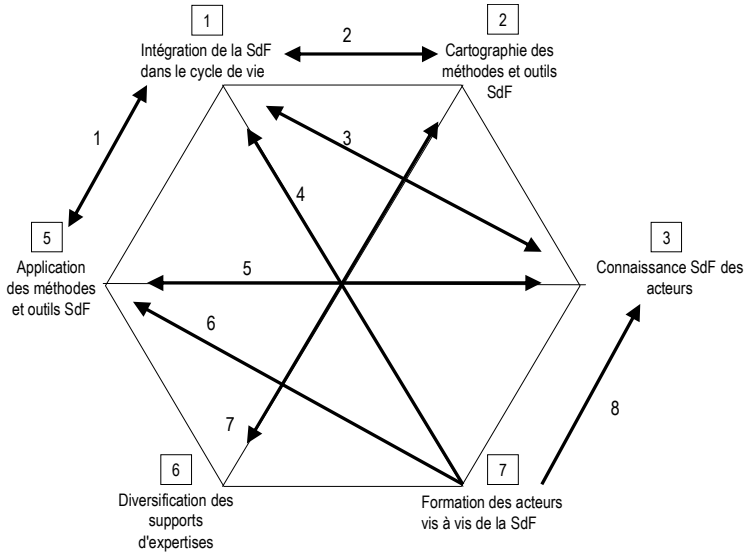


Figure I-6 : Liens entre les caractéristiques du problème

Nous explicitons les différents liens de la figure :

- lien n°1 : l'augmentation de l'utilisation des méthodes améliorera l'intégration de la SdF tout au long du cycle de vie et inversement,
- lien n°2 : plus l'intégration de la SdF sera élevée dans le cycle de vie, plus la cartographie sera complète dans le but de traiter les différentes phases du cycle de vie,
- lien n°3 : plus l'intégration de la SdF sera élevée, plus la connaissance des acteurs augmentera au fil des expériences,
- lien n°4 : une formation importante des acteurs projet permettra de renforcer l'intégration de la SdF dans le cycle de vie,

- lien n°5 : l'application courante des méthodes et outils SdF augmentera la connaissance des acteurs au fil du temps et inversement,
- lien n°6 : plus la formation des acteurs sera importante, plus l'application des méthodes et outils sera aisée,
- lien n°7 : plus la cartographie des méthodes et outils sera importante, plus il y a de chances d'avoir un nombre de supports d'expertise élevé,
- lien n°8 : une formation importante des acteurs projet à la SdF permettra l'augmentation des connaissances SdF au sein de l'entreprise.

Cet état des lieux a permis d'établir un premier schéma d'actions à suivre ou à consolider pour assurer une meilleure gestion de la sûreté de fonctionnement.

3.4. Revue des problèmes liés au PRAO

L'objet de ce paragraphe est d'analyser les spécificités du traitement de la SdF au stade de la phase d'acquisition. L'objectif est d'aboutir à l'identification et à l'évaluation de la dimension "sûreté de fonctionnement" du futur produit afin d'en tenir compte dans la réponse à l'Appel d'Offre (AO). Au-delà de cet objectif, la finalité du travail est d'offrir une aide aux acteurs projet dans leur prise en compte, à ce stade amont du projet, des exigences sûreté de fonctionnement. Cette aide doit respecter les routines de conception et s'intégrer parfaitement aux méthodologies existantes. Afin de ne pas modifier fortement les modes de fonctionnement en place dans l'entreprise et ayant fait preuve d'efficacité dans certains contextes, une contrainte importante a consisté à conserver les principaux outils et méthodes utilisés et à renforcer la traçabilité des actions menées pour améliorer indirectement les processus de capitalisation et de formalisation d'expertise.

Déclenché par la réception d'un appel d'offre, le PRAO correspond à la première phase du cycle de vie du produit (phase d'acquisition) et comporte les étapes suivantes :

- réception de l'AO et des documents associés (cahier des charges clients (CdC)),
- faisabilité (étude des possibilités de réponse incluant une analyse technique et financière primaire),
- décision de poursuite couplée aux choix stratégiques d'entreprise,
- élaboration de la réponse, cotation et évaluation,
- négociation.

La principale caractéristique du PRAO est sa très courte durée, deux à huit semaines, pour élaborer la réponse au client, ce qui impose une forte réactivité de l'entreprise. S'agissant du premier contact avec le client, il est nécessaire d'afficher le plus clairement possible le savoir-faire de l'entreprise pour mettre celui-ci en confiance. Dans le cas que nous traitons, la sûreté de fonctionnement apparaît comme un élément capital de la démonstration à réaliser.

La tâche de prise en compte de la dimension SdF est rendue difficile par le fait que le PRAO est engagé dans un cadre incertain puisque le produit n'existe pas encore et que les informations dont on dispose sont souvent parcellaires. Il faut donc anticiper le développement potentiel du produit en élaborant le futur scénario de ce développement pour établir, en cohérence avec les règles financières et commerciales de l'entreprise, la proposition au client. A ces fins, il est nécessaire de connaître l'ensemble des informations sur les exigences du client mais aussi sur les méthodes et procédures de développement du produit, sur les méthodes SdF et sur tous les éléments qui permettront de définir la "valeur d'impact" de la SdF requise.

Lors de la réception de l'appel d'offre, une équipe d'acquisition est mise en place. Elle est composée d'acteurs représentant les compétences nécessaires de l'entreprise : marketing, financier, management, qualité, production et technique (responsables, experts,..). Cette équipe diffère peu de l'équipe projet sur le plan des compétences ; c'est une équipe réduite, de composition variable en fonction du type de client (connu ou nouveau), du type de produit et de l'enjeu de l'appel d'offre. Les solutions proposées par ces acteurs devront être compréhensibles des acteurs projet afin de maintenir une continuité dans les actions qui seront menées pour le développement du produit.

Soulignons également qu'il est particulièrement important de mener à bien la phase d'acquisition dans la mesure où la majorité des coûts du produit final sont fixés à ce niveau d'avancement du projet.

Une autre particularité du PRAO, en lien avec les exigences SdF, réside dans les nouvelles attentes du client qui ne veut plus seulement savoir si le prestataire atteindra les objectifs SdF mais qui veut aussi s'assurer des dispositions prises pour atteindre ces objectifs. Ceci impose de pouvoir visualiser toutes les activités SdF qui seront engagées sur le cycle de vie du produit.

Enfin, la dernière spécificité liée au PRAO concerne la nature des documents à traiter par l'équipe d'acquisition (documents du dossier fourni par le client pour l'appel d'offre). Ce dossier est variable d'un client à l'autre ; il contient différents types de documents :

- le cahier des charges du produit,
- des annexes relatives à un aspect particulier du produit, des informations sur les procédures clients, des informations ou documents règlementaires,...,
- des documents administratifs à compléter par le fournisseur : documents standards du client pour la réponse du fournisseur (matrice d'agrément, matrice de conformité, tableau d'exigences sur lequel le fournisseur doit situer sa proposition).

L'aspect sûreté de fonctionnement figure dans ces documents en termes d'exigences :

- relatives aux caractéristiques de sûreté de fonctionnement : taux de défaillance, fiabilité,..., ou incluses dans des exigences de qualité,
- relatives aux objectifs de sécurité (SIL : Safety Integrity Level) des fonctions,
- relatives aux études à réaliser et aux résultats à fournir au client.

Ces informations permettront de fixer les caractéristiques du produit et de structurer la démarche projet.

En outre, le CdC peut comporter des informations sur la façon dont le client appréhende la sûreté de fonctionnement.

Les données issues des CdC sont cependant souvent hétérogènes et beaucoup de données relatives à la sûreté de fonctionnement restent implicites.

Après avoir introduit la problématique industrielle, nous présentons dans le paragraphe suivant les solutions existantes susceptibles de satisfaire certains aspects du problème posé.

4. Placement de la problématique / Etude de l'existant

L'objectif des travaux est de proposer une méthodologie permettant d'évaluer la "valeur d'impact" SdF dès les phases de réponse à l'appel d'offre. Il est donc nécessaire d'analyser les travaux relatifs au PRAO mais aussi ceux en lien avec le déploiement des méthodes SdF et à la modélisation d'un processus de conception. Nous présentons ci-après un panorama de l'existant dans ces domaines.

4.1. Etat de l'art PRAO

Les travaux portant sur le processus de réponse à appel d'offre (PRAO) se concentrent généralement sur des problématiques stratégiques. En effet, dans ces phases, les entreprises vont chercher à prendre les meilleures décisions pour faire au client une offre optimisée par rapport à l'ensemble des contraintes. Il s'agit d'identifier les risques susceptibles de porter atteinte à la réussite du projet. Nous proposons un inventaire des différents travaux potentiellement utiles à ce niveau et déclinés dans les phases de réponse à appel d'offre.

Une partie des travaux s'intéresse particulièrement aux décisions à prendre ainsi qu'aux facteurs influant la réussite d'un appel d'offre. C'est le cas, par exemple des travaux de [Cagno&al, 01] dans lesquels les auteurs proposent une approche basée sur la simulation pour l'évaluation de la probabilité de gain d'un appel d'offre du point de vue de l'entreprise qui y répond. Dans [Zafra-Cabeza&al, 02], les auteurs proposent un système d'aide à la décision destiné aux phases de réponse à appel d'offre. Les décisions considérées sont celles qui concernent le choix de poursuite ou d'arrêt de l'appel d'offre et celles de fabriquer ou d'acheter le produit à développer. Aucun de ces travaux ne traite des activités réalisées par l'équipe acquisition durant ce processus. Le point de vue adopté est celui de la stratégie d'entreprise.

Un domaine largement couvert par les travaux dédiés au PRAO est celui de la gestion des risques "projet". Parmi ces travaux, plusieurs éléments sont traités :

- le management des risques projet,
- la capitalisation des connaissances sur les risques projet,
- l'estimation des coûts des risques projet.

Pour la partie management des risques projet, on trouve dans [Gouriveau, 03] une étude sur les méthodes, outils et techniques de management de ces risques utilisables dans le cadre du PRAO. Cette étude est intégrée au projet européen PRIMA : "Projet Risk Management" (présenté en détail à la fin de cette partie). L'étude menée permet de mettre en évidence l'importance du retour d'expérience dans cadre du PRAO. Les rares informations dont on dispose à ce stade vis à vis des risques encourus doivent, en effet, être complétées par des expériences sur des projets précédents notamment par le biais de feuilles de risques retraçant l'histoire et le contexte d'apparition de ces risques. L'approche proposée nous intéresse puisqu'elle met en évidence la relation étroite entre PRAO et Retour d'expérience (Figure I-7).

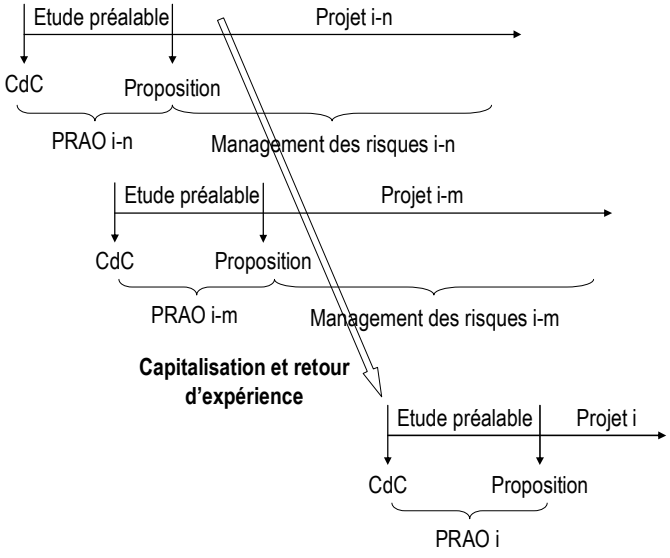


Figure I-7 : PRAO et retour d'expérience [Gouriveau, 03]

Dans [Chalal&al, 05], les auteurs proposent la définition d'un système d'information destiné au management des connaissances sur les risques projet fournissant une aide à la décision stratégique durant le PRAO. Le système d'information ainsi défini doit permettre la constitution d'un référentiel sur les risques internes et externes. Il propose une structure des connaissances pour l'organisation de la capitalisation, basée sur quatre composantes : le risque, ses causes, ses impacts ainsi que les actions prises dans un contexte donné pour gérer ce risque. Cette approche semble pertinente par la nature des concepts introduits. Elle ne répond cependant pas à notre problématique dans la mesure où l'objectif est de prendre, à un instant donné, une décision par rapport à une connaissance alors que, dans notre cas, il s'agit d'utiliser la connaissance pour établir des scénarios de développement et des alternatives de conception.

On trouve des éléments intéressants sur l'estimation du coût des risques projet dans [Cagno&al, 00]. Les auteurs partent du constat que, dans le cadre d'un appel d'offre, l'estimation des coûts du projet est une étape critique vis à vis de la compétitivité et de la rentabilité d'une entreprise. Dans le contexte de projets de construction, ils proposent un modèle analytique destiné à estimer le coût des analyses HAZOP (Hazard and Operability Study) permettant, pour de tels projets, de prendre en compte l'ensemble des risques liés à une installation industrielle. Dans le modèle de coût, l'étude est décomposée en différentes phases caractérisées par un certain nombre de facteurs destinés à évaluer le coût. Dans le cadre de ce type de projet, la décomposition de l'installation en éléments distincts et indépendants s'avère relativement facile. Ce constat est moins évident lorsqu'on s'intéresse aux systèmes embarqués.

Pour terminer, nous nous sommes particulièrement intéressés au projet PRIMA[4] qui évoque la plupart des thématiques abordées au niveau de l'étude des risques projet dans le cadre du PRAO. Ce projet, basé sur un consortium d'industriels européens, avait pour objectif la définition d'une méthodologie et les outils qui lui sont associés afin d'intégrer le management des risques projet dans le PRAO, de proposer un système d'aide à la décision fondé sur l'évaluation simultanée des risques et des coûts du produit et de fournir une mémoire d'entreprise sur ces problématiques. Les concepts s'appuient sur une définition des coûts liés aux conséquences potentielles de l'occurrence de différents risques. Aucune analyse économique du traitement de ces risques n'est proposée. Ce manque correspond précisément à un des objectifs que nous nous sommes fixés dans le cadre de ce travail. La notion de capitalisation d'expérience sur les risques en phase d'acquisition est jugée fondamentale dans le projet PRIMA. Les mécanismes associés à cette forme de réutilisation de la connaissance passée sont présentés sur la Figure I-8. Nous les reprendrons à notre compte dans la suite de cette étude.

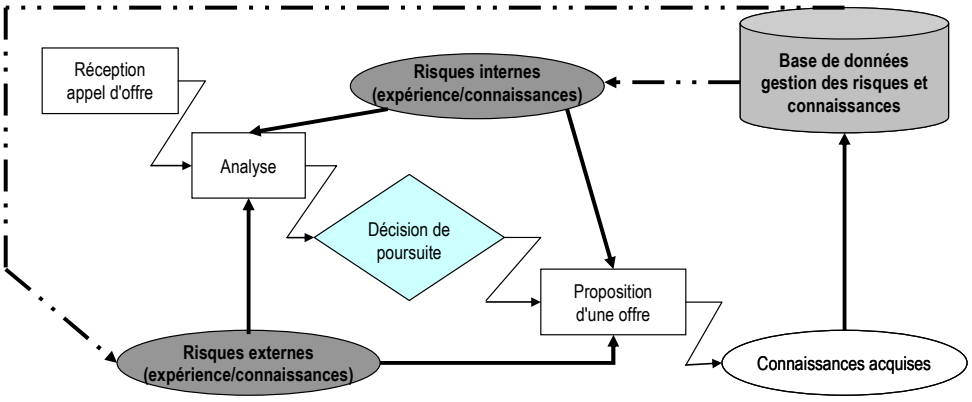


Figure I-8 : Spectre du projet PRIMA

[4] Le lecteur intéressé trouvera plus d'informations sur le projet à l'adresse http://www.esi2.us.es/prima/Abstract1.html : notamment les publications, les partenaires, les démonstrations.

4.2. Méthodologies de Sûreté de Fonctionnement

4.2.1. Les approches classiques

La sûreté de fonctionnement est définie comme la science des défaillances ; elle englobe l'ensemble des aptitudes d'un système à réaliser une fonction donnée, dans des conditions données et pendant un temps donné. Elle s'intéresse à leur connaissance, leur évaluation, leur prévision, leur mesure et leur maîtrise, [Villemur, 97]. Il existe une autre définition qui, selon nous, offre une perspective plus large de réflexion : c'est la propriété d'un système qui permet à ses utilisateurs de placer une confiance justifiée dans le service délivré [Laprie, 96].

La mise en œuvre d'une analyse de sûreté de fonctionnement est susceptible de déboucher sur la quantification de différentes mesures ou attributs. Nous les présentons avec leurs interactions sur la Figure I-9.

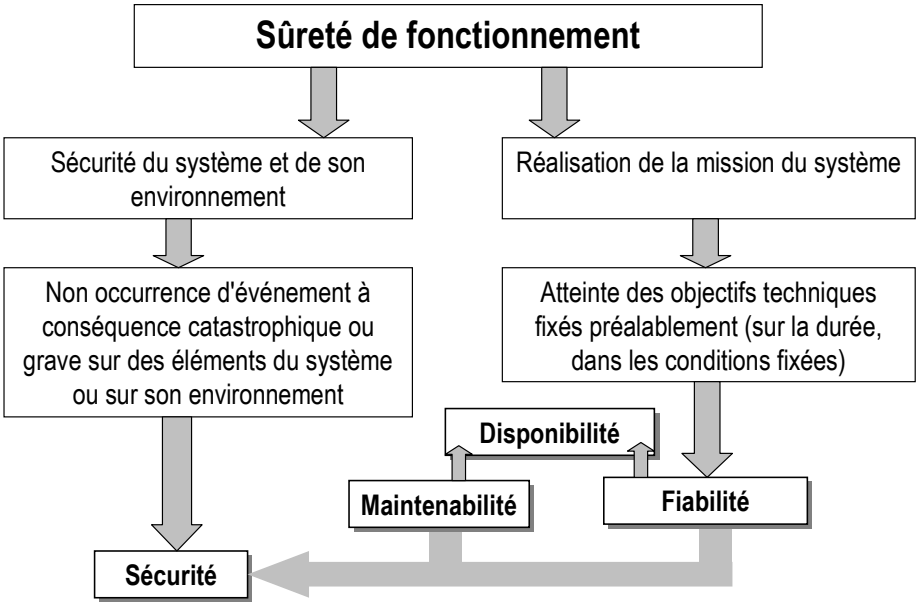


Figure I-9 : Concepts de la sûreté de fonctionnement

La fiabilité est définie comme l'aptitude d'un produit à accomplir une fonction requise, dans des conditions données, pendant un temps donné [AFNOR X 60-500].

La maintenabilité est l'aptitude d'un produit à être maintenu ou rétabli, pendant un intervalle de temps donné, dans un état dans lequel il peut accomplir une fonction requise, lorsque l'exploitation et la maintenance sont accomplies dans des conditions données, avec des procédures et des moyens prescrits [AFNOR X 60-010].

La disponibilité est l'aptitude d'un bien, sous les aspects combinés de sa fiabilité et de l'organisation de maintenance, à être en état d'accomplir une fonction requise dans des conditions de temps déterminées [AFNOR X 60-010].

Enfin, la sécurité est la propriété d'un produit de présenter, pour son environnement et pour lui même, un risque déterminé en fonction des dangers potentiels inhérents à sa réalisation et à sa mise en œuvre qui ne doit pas être supérieur à un risque convenu [IEC 61508-4].

On parle souvent dans le cadre de la sûreté de fonctionnement (SdF) de "FMDS" ou de "RAMS" (en anglais : Reliability, Availability, Maintainability, Safety).

Le management de la SdF dans une entreprise passe par une organisation du système de management de la qualité intégrant les moyens nécessaires à la prise en compte des attributs SdF. Nous donnons sur la Figure I-10 une

représentation possible de l'activité de management de la sûreté de fonctionnement. Cette schématisation montre que la mise en place d'un système de gestion de la sûreté de fonctionnement nécessite de mener à bien plusieurs tâches supportées par des moyens de différentes natures pour faire face à des contraintes diverses en vue de respecter les objectifs fixés. On notera que le niveau d'abstraction de la représentation lui confère un caractère générique non spécifique au domaine SdF.

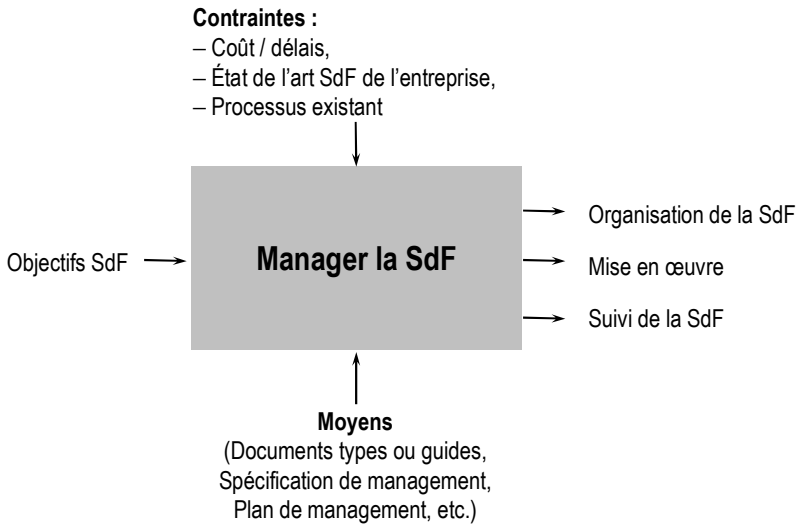


Figure I-10 : Management de la SdF (adaptée de [Cours UTC, 08])

Les moyens mis en œuvre pour la réalisation de l'activité englobent l'ensemble des méthodes, techniques et outils permettant la conception et le développement d'un système sûr de fonctionnement. Plusieurs modes de classement permettent de regrouper les méthodes de sûreté de fonctionnement selon le point de vue considéré. Le premier classement, le plus courant, sépare les méthodes en deux types par rapport au raisonnement suivi :

- les méthodes inductives : dans cette catégorie, l'objectif est de partir des défaillances (causes) pour en déduire leurs effets (conséquences). La méthode la plus répandue pour ce genre d'étude est l'analyse des modes de défaillances de leurs effets et de leur criticité (AMDEC),
- les méthodes déductives : elles ont pour objectif d'identifier les causes potentielles d'un évènement donné. Elles partent des effets (conséquences) pour arriver aux causes. Les arbres de défaillances font partie des méthodes les plus couramment utilisées à ce niveau.

Un autre classement consiste à séparer les méthodes par rapport à leurs objectifs. On distingue ainsi :

- les méthodes qualitatives dont l'objectif est d'étudier les dysfonctionnements d'un système sans quantifier les fréquences d'apparition ou autre grandeur SdF,
- les méthodes quantitatives ayant pour objectif l'établissement et l'évaluation des grandeurs adaptées.

En plus des méthodes, la gestion de la SdF repose sur une démarche intellectuelle permettant de définir une méthode adaptée pour une activité donnée. Dans cette optique, nous proposons de structurer les mécanismes de réflexion conduisant à l'établissement d'un mode de gestion de la SdF permettant d'identifier, à chaque étape, les méthodes potentiellement utilisables et celles à retenir.

Classiquement, une démarche SdF est décomposée en différentes étapes. La première étape consiste à caractériser le fonctionnement normal du système dans son environnement (par la définition des limites du système). L'étape suivante

a pour objectif d'identifier les risques potentiels du système et de les hiérarchiser par rapport à leur criticité en étudiant les aspects dysfonctionnels [Noyes&al, 07]. Cette étape d'évaluation précède une étape de recherche de solutions préventives ou correctives sélectionnées selon des critères technico-économiques.

Les méthodes utilisables à chaque étape sont fonction des résultats à fournir. Pour plus de détails sur l'ensemble des méthodes existantes, on pourra consulter [IMDR_SdF_07]. A toutes fins utiles, on peut cependant citer ici :

- pour l'analyse du fonctionnement : l'ensemble des méthodes et outils d'analyse fonctionnelle (IDEF, APTE,...,),
- pour l'identification des risques et leur hiérarchisation : l'analyse préliminaire des risques, méthode conseillée puisqu'elle permet à elle seule [Mortureux, 01] l'identification des évènements redoutés pour un système donné, l'évaluation de leur gravité et de leur fréquence d'apparition dans l'objectif de les hiérarchiser à un haut niveau d'abstraction,
- enfin, pour le traitement et l'évaluation des différents risques, les méthodes possibles sont nombreuses : l'AMDEC est la plus usuelle mais il existe aussi les arbres de défaillances, les diagrammes de fiabilité, les graphes d'états, les réseaux de Petri, les méthodes bayesiennes,... Le choix des méthodes dans cette étape est fonction des connaissances de l'entreprise, du secteur industriel, etc. On notera cependant que certaines de ces méthodes sont basées sur des formulations inspirées du "langage naturel" alors que d'autres s'appuient sur des modes de représentation graphiques. Cette remarque présente un certain intérêt dans la mesure où une contrainte forte de l'étude consiste à mettre en place des solutions innovantes mais respectueuses des modes de fonctionnement actuels.

De nombreux travaux ont été menés sur l'intégration des caractéristiques SdF dans les processus de conception afin de développer des produits plus sûrs. Les travaux de thèse de Schoenig [Schoenig, 04] réalisés en partenariat avec un constructeur automobile concernent une méthodologie de conception des systèmes mécatroniques sûrs de fonctionnement. L'objectif de ce travail n'était pas de proposer une nouvelle méthodologie mais plutôt d'identifier les éléments permettant d'améliorer, d'un point de vue de l'intégration des caractéristiques SdF, le processus existant. L'approche retenue s'appuie sur le cycle de développement en V, généralement suivi pour la conception des systèmes embarqués et propose l'intégration de méthodes formelles, en rendant transparents pour le concepteur les corpus théoriques associés à ce type d'outils. Dans le cadre de notre travail, nous nous démarquons de ces développements car les éléments porteurs de la démarche de Schoenig tels que les réseaux de Petri ou les graphes de Markov ne correspondent pas à des standards utilisés régulièrement par les acteurs projet de systèmes embarqués. Dans la même catégorie, on trouve les travaux menés au LAAS (Laboratoire d'Analyse et d'Architecture des Systèmes) qui se sont intéressés au développement de méthodologie de conception de produits sûrs. Dans sa thèse [Khalfaoui, 03], Khalfaoui propose une méthode de recherche des scénarios redoutés pour l'évaluation de la SdF des systèmes mécatroniques. La méthode proposée est basée sur l'utilisation des réseaux de Petri pour la modélisation des systèmes. Les thèses réalisées à la suite de ce travail s'appuient sur les mêmes représentations et ont un objectif assez proche comme dans [Medjoudj, 06]. Le travail de Sadou [Sadou, 07] ou celui de Demri&al dans [Demri&al, 07b] se basent également sur le formalisme des réseaux de Petri mais l'objectif est plus large car ils proposent une aide à la conception des systèmes embarqués sûrs de fonctionnement. Pour tous ces travaux, nous faisons le même constat que les réseaux de Petri ne sont pas un formalisme assez proche des habitudes des acteurs projet et acquisition ciblés dans cette étude.

Dans [Dumas&al, 08] et [Bieber&al, 04], les méthodes déployées utilisent des langages de modélisation ou de programmation (Altarica, AADL). Plusieurs résultats sont pertinents mais les développements ne remplissent pas non plus la condition impérative d'usage par le plus grand nombre qui nous est demandée.
Il existe beaucoup de travaux proposant des modélisations diverses mais, là encore, les méthodes utilisées sont par trop différentes des modes de fonctionnement de l'entreprise partenaire pour envisager leur implémentation.
L'analyse des méthodes SdF existantes nous a permis de nous rendre compte que peu de travaux placent la conception au centre des développements et, plus particulièrement, le concepteur alors que dans le cadre d'une analyse SdF durant le PRAO, il faut pouvoir s'adapter à tout type d'acteur projet et donc proposer une représentation du produit intelligible de tous.

Le paragraphe suivant est consacré aux problématiques SdF dans le contexte automobile ainsi qu'aux caractéristiques étudiées lors du développement d'un système embarqué automobile.

4.2.2. Déclinaison de la SdF dans l'industrie automobile

Les principales préoccupations en termes de SdF pour les industriels de l'automobile sont liées à la fiabilité et à la sécurité des systèmes.

Sur le plan de la sécurité, on notera tout d'abord l'existence d'un référentiel règlementaire : la norme IEC 61508 (Sécurité fonctionnelle des systèmes électriques, électroniques et électro-programmables relatifs à la sécurité). Ce référentiel est générique. Il est d'ailleurs décliné dans d'autres secteurs d'activité (ferroviaire, médical,...). Dans le milieu automobile, la difficulté par rapport à cette norme émane du fait qu'elle est destinée à définir des niveaux d'intégrité de sécurité non pour un système complet mais pour des sous-systèmes en charge d'assurer une unique fonction sécuritaire [Dumas, 06]. Ces difficultés ont poussé les acteurs du secteur à proposer une déclinaison de l'IEC 61508 pour le milieu automobile. Cette norme, qualifiée norme ISO 26262 (Véhicules routiers : Sécurité fonctionnelle), est en cours de validation et entrera en vigueur à la fin de l'année 2009 ou au début de l'année 2010[5]. Les motivations ayant poussé les acteurs du secteur au développement d'une nouvelle norme, en dépit du besoin d'une norme sectorielle, se basent sur les évolutions futures des systèmes automobiles pour lesquelles il n'existera pas d'état de l'art (par exemple, les technologies "X-by-Wire" dans lesquelles les liaisons mécaniques sont remplacées par des liaisons électriques) et qui seront de plus en plus critiques en termes de sécurité. Les nouveaux systèmes d'assistance à la conduite (notamment les systèmes pouvant se substituer au conducteur) entraînent, en effet, une évolution de la criticité SdF [Chaussis, 06].
Ces normes fixent des niveaux d'intégrité de sécurité "SIL" pour l'IEC61508 et "ASIL" pour l'ISO 26262 ("SIL" Safety Integrity Level, "ASIL" Automotive SIL) déclinés en différentes métriques devant respecter des plages de valeurs prédéfinies pour être validées. Pour définir ces niveaux, la technique la plus répandue est celle des graphes de risques dont le principe est illustré sur la Figure I-11. Cette méthode consiste à définir le niveau de sécurité en définissant des niveaux pour différents paramètres représentatifs de :

[5] Certains clients font cependant déjà référence à cette norme dans les cahiers des charges.

- la conséquence potentielle du risque étudié (sa criticité),
- la fréquence d'exposition au risque,
- les barrières de sécurité pouvant être mises en place pour diminuer l'impact ou la fréquence du risque,
- la probabilité d'occurrence non souhaitée du risque.

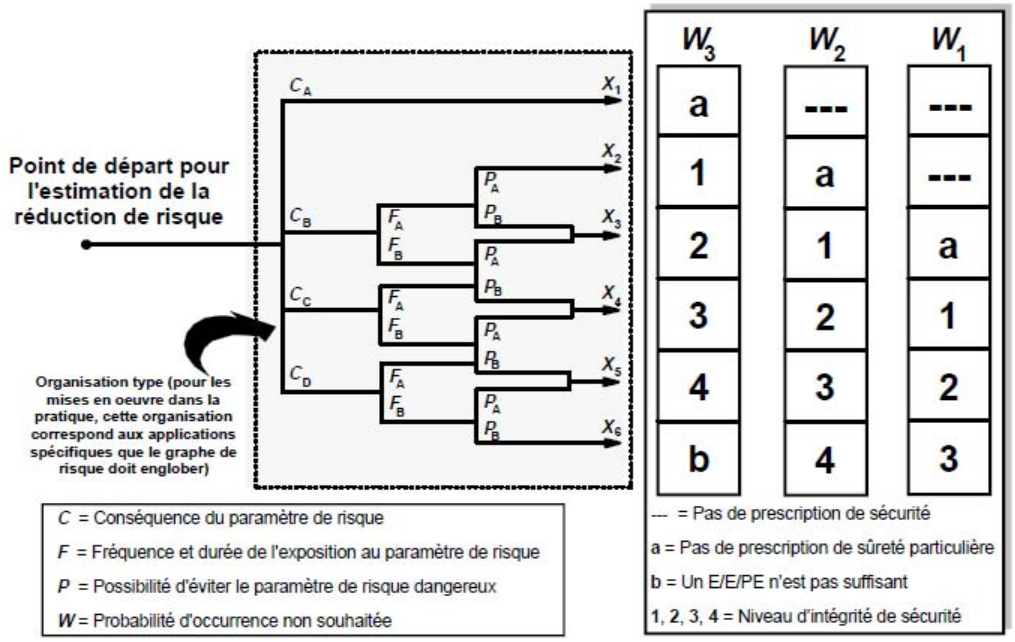


Figure I-11 : Graphe de risque issu de [IEC 61508-5]

Les exigences du client en termes de sécurité seront exprimées, dans le cahier des charges, sous la forme :

- de niveau SIL ou ASIL à respecter,
- d'exigences concernant la démonstration de l'atteinte de ces objectifs,
- de prescriptions règlementaires fonctions de la norme citée en référence IEC 61508 ou ISO 26262.

La question est alors de savoir quelle norme considérer. La norme ISO 26262 n'est en effet pas encore validée donc on peut se poser la question du choix des documents normatifs à appliquer actuellement d'un point de vue règlementaire. Il faut cependant noter que, dans l'automobile, contrairement à des domaines comme le ferroviaire ou le médical, il n'existe pas d'organisme de certification indépendant.

La dernière particularité concernant la sécurité automobile est le fait que, contrairement aux autres domaines auxquels s'applique la norme IEC 61508, un système embarqué est un produit de grande série destiné à différents types d'utilisateurs finaux n'ayant pas forcément la même façon d'appréhender un véhicule. L'impact d'un accident affectera l'image de marque du constructeur mais également son volet financier dans le cas de campagne de rappel d'un véhicule par exemple.

La seconde caractéristique SdF considérée dans l'automobile est la fiabilité. Celle-ci est exprimée dans l'automobile en PPM ("pièces par million"). Elle est calculée par rapport au nombre de systèmes défaillants sur un an d'utilisation rapporté au nombre total de systèmes produits. Dans le secteur des systèmes mécatroniques, la fiabilité est largement corrélée à la composante électronique du produit. Il existe un certain nombre de méthodes théoriques permettant de

faire de la fiabilité prévisionnelle par rapport à des recueils de fiabilité tels que FIDES (Guide méthodologique de fiabilité pour les systèmes électroniques), MIL-HDBK217 (Military Handbook) [Dupouy, 05] ou des méthodes développées par des entreprises du secteur tels que les essais de vieillissement accélérés de Siemens VDO. Ces estimations sont vérifiées dans la phase de production et tiennent compte de l'ensemble des systèmes défaillants effectifs.
Parmi les principaux problèmes liés à la fiabilité, on constate une hétérogénéité des exigences entre constructeurs [VEMS, 05], ce qui rend difficile la définition d'un profil de mission générique capable de supporter toute étude de fiabilité prévisionnelle appliquée au secteur de l'automobile [Roure, 06]. Le profil d'emploi d'un système de freinage, très dépendant du contexte (mode d'utilisation, conditions météorologiques, …) est, d'une certaine manière, plus difficile à caractériser que le profil d'emploi d'un avion par exemple (une phase de décollage, une phase de vol, une phase d'atterrissage).

Les deux attributs que nous considèrerons dans nos travaux sont donc la fiabilité et la sécurité. Nous chercherons à identifier pour ces deux caractéristiques la nature de leur impact sur le produit ainsi que sur les méthodes à engager pour s'assurer de l'atteinte des objectifs correspondants du cahier des charges.

4.3. Méthodes de conception classiques et logique métier / cycle de vie

Une seconde contrainte de la problématique liée au cadre du PRAO concerne le fait que différents types d'acteurs sont susceptibles d'analyser les caractéristiques SdF. La méthodologie que nous développons devra permettre une continuité entre les études faites et prévues dans le PRAO et celles qui seront menées durant le développement pour s'assurer de l'atteinte des objectifs SdF. Dans ces conditions, il apparaît nécessaire de s'intéresser au positionnement du PRAO dans les processus de conception ainsi qu'aux phases de développement qui suivront le PRAO dans le cas de l'acceptation de l'offre par le client.
Nous nous intéressons tout d'abord aux différents types de processus de conception puis nous étudions la place du PRAO dans un cycle de conception classique.

Le modèle de processus de conception défini par Pahl et Beitz fait référence dans ce domaine [Pahl et Beitz, 96]. Hadj-Hamou [Hadj-Hamou, 02], en propose une adaptation en français que nous reprenons sur la Figure I-12. Ce processus est composé de quatre phases successives : élaboration du cahier des charges, conception de principe, conception d'ensemble et, enfin, conception de détail. Chacune de ces phases est, elle même, décomposée en étapes décrivant les activités successives réalisées. Ce processus met en jeu des phases séquentielles mais peut être itératif via des retours d'information permettant d'adapter les spécifications ou les solutions techniques envisagées. L'application de ce processus part du principe que l'entreprise est force de proposition par rapport à un marché dont elle cherche à satisfaire le besoin en utilisant les moyens et compétences à sa disposition. Ce mode de travail ne correspond cependant pas aux formes de fonctionnement des prestataires de l'automobile.

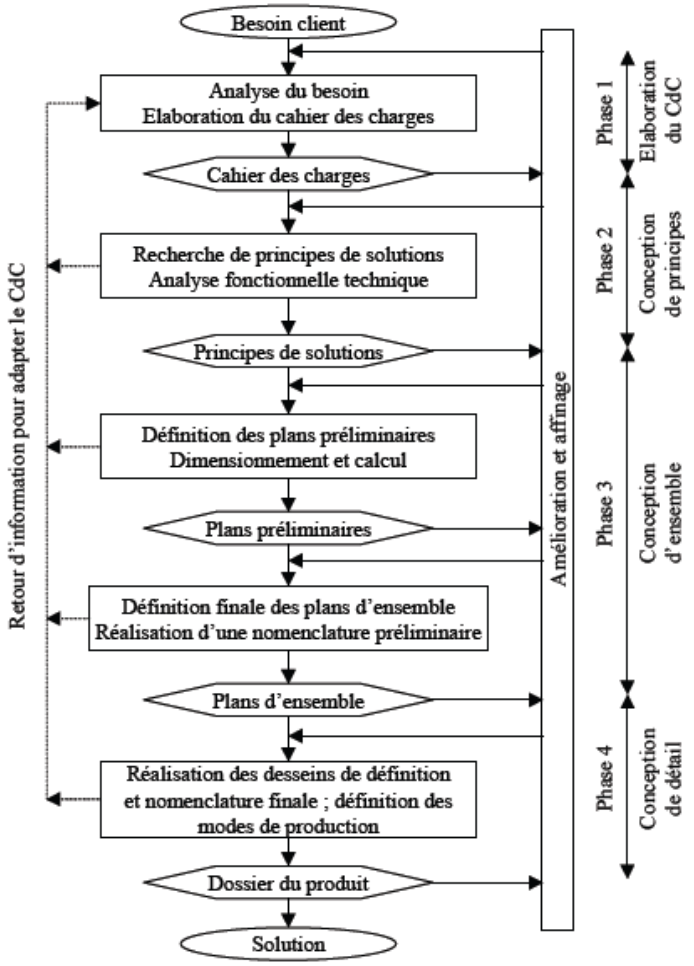


Figure I-12 : Processus de conception [Pahl et Beitz, 96] traduit par [Hadj-Hamou, 02]

Bien que les étapes successives d'un processus de conception restent identiques, il existe différentes façons d'appréhender la conception. La notion classique de cycle en V consiste à mettre en correspondance les étapes de conception (phase descendante) et celles de validation et de vérification (phase ascendante). Elle est présentée sur la Figure I-13.

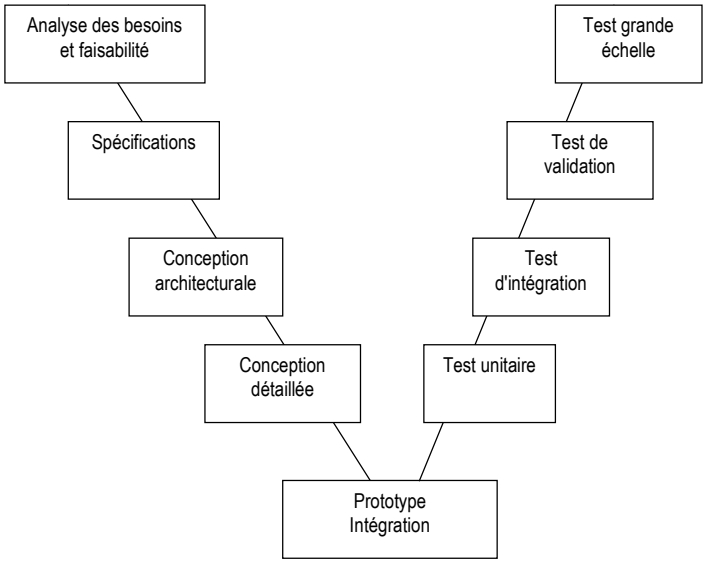


Figure I-13 : Cycle de conception en V

Une autre approche appelée cycle en Y, proposé dans [Gutierrez-Estrada, 07] et repris sur la Figure I-14, consiste à coupler deux processus simultanés pour engager une nouvelle étape de la conception.

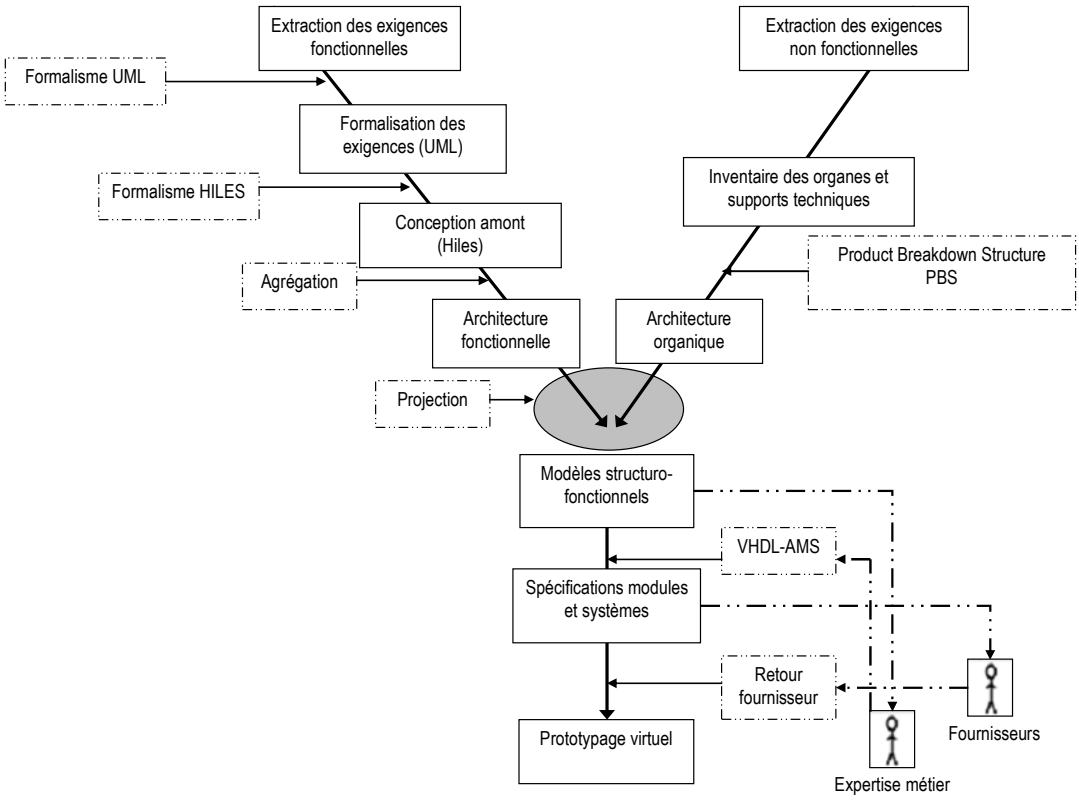


Figure I-14 : Cycle de conception en Y

Nous cherchons ici à identifier les activités du concepteur ou de l'équipe acquisition durant le PRAO. D'une manière générale, quel que soit le modèle considéré, on peut globalement se ramener au modèle de référence de Pahl and Beitz. Comme nous l'avons présenté dans le paragraphe 3.4, l'objectif du PRAO est de proposer une réponse au client à partir des documents transmis. Afin de proposer une méthodologie d'évaluation de la SdF dans ces phases en respectant les modes de fonctionnement de l'entreprise, il apparaît important d'identifier les phases communes au PRAO et au processus de conception. Nous rappelons sur la Figure I-15 les entrées et les sorties d'un processus de réponse à appel d'offre. Pour définir le coût de la solution proposée au client en réponse au cahier des charges, il faudra avoir préalablement défini les principes de solution dans leurs grandes lignes.

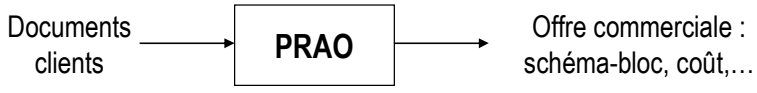


Figure I-15 : PRAO

Nous nous proposons, dans ces conditions, de mettre en correspondance les deux processus à partir d'un panorama des processus de conception (Figure I-16 : extrait de [Scaravetti, 04]) et de l'identification des intrants et extrants du PRAO.

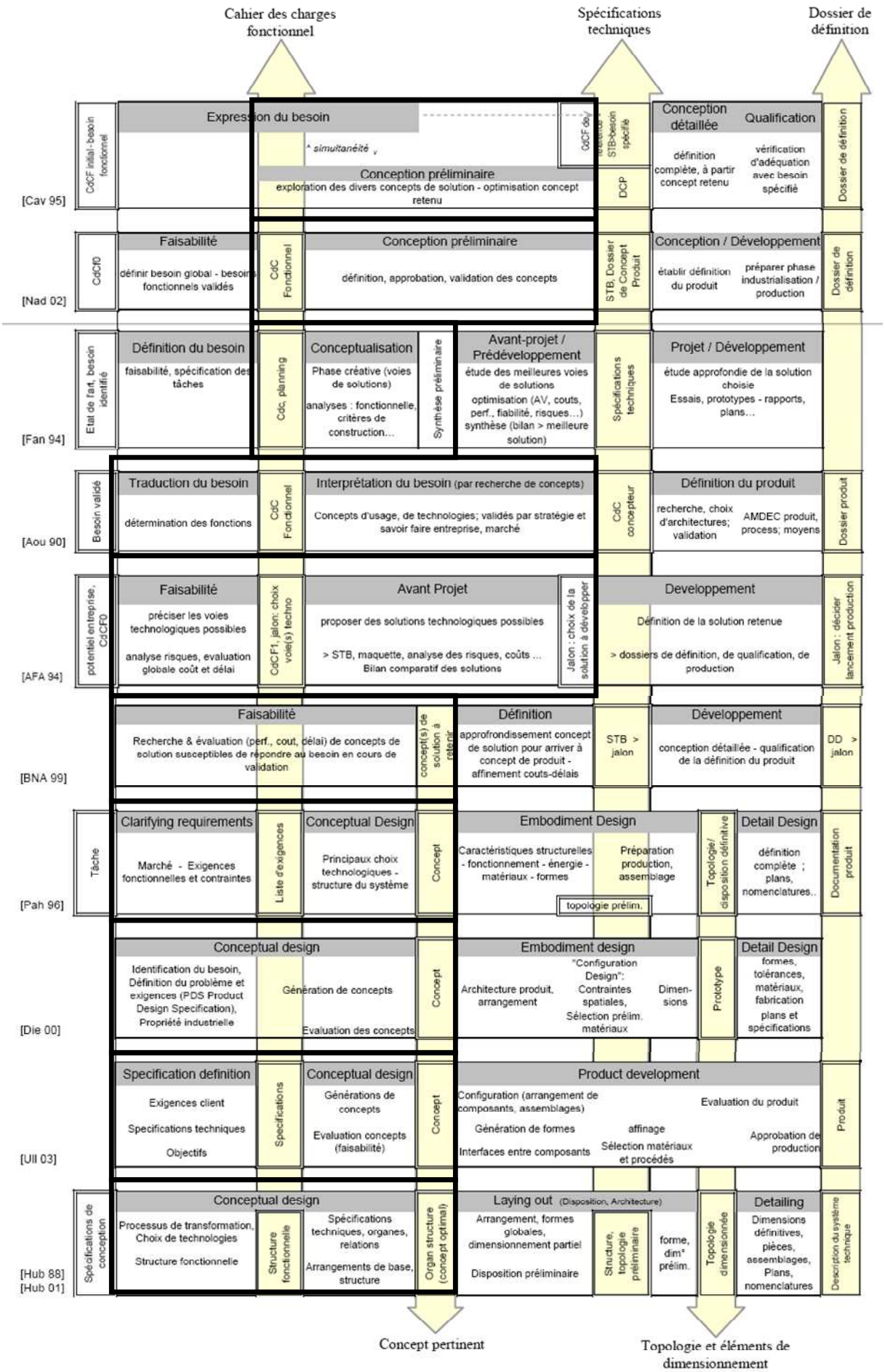


Figure I-16 : Identification des activités réalisées dans le PRAO

L'ensemble des références proposées dans la figure précédente ainsi qu'une description succincte des travaux de Scaravetti sont disponibles en annexe I-B.

Nous avons identifié, par rapport aux processus de conception précédents, quelles pouvaient être les phases ayant les mêmes objectifs que celles du PRAO à partir de l'identification de la disponibilité d'un CdC jusqu'à la proposition d'un concept. Bien sûr, dans le PRAO, même si les intrants et extrants sont similaires, le niveau d'abstraction utilisé sera plus élevé. La Figure I-16 permet de mettre en évidence (via les phases encadrées correspondant aux étapes de la disponibilité d'un CdC à une proposition de concept de solution) que les activités réalisées durant le PRAO correspondent, en fonction du processus de conception considéré, à la phase de :

- conception préliminaire ou création du concept,
- conceptualisation,
- traduction et interprétation du besoin,
- faisabilité.

En comparant ces différentes notions au processus de conception que nous avons présenté sur la Figure I-12, nous constatons que les activités du PRAO peuvent être assimilées à des activités réalisées durant la phase de Conception de principes (ou Création du concept ou Conception préliminaire, selon le vocabulaire employé). Les activités contenues dans cette phase seront détaillées dans le chapitre 2 mais on peut déjà remarquer que la connaissance de la phase correspondant aux activités réalisées dans le PRAO permettra de définir les activités de l'équipe Acquisition durant le PRAO et les modèles du produit sur lesquels il faudra s'appuyer pour caractériser la méthodologie.

Le dernier point à étudier dans le processus de conception est la composition d'une équipe projet, l'équipe Acquisition ayant été définie dans le paragraphe 3.4. En fonction des produits développés, l'équipe projet sera constituée :

- des différents acteurs issus des métiers composant directement le produit ; dans le cadre des systèmes considérés il s'agira des métiers en lien avec la mécanique, le logiciel et l'électronique,
- des différents acteurs issus des services supports : méthodes, industrialisation, qualité, production,
- d'experts : utilisés ponctuellement ou en continu, selon le besoin,
- d'un chef de projet.

5. Positionnement scientifique du problème

A partir des éléments que nous avons introduits dans les paragraphes précédents, notre objectif est de définir une méthodologie permettant de traiter les exigences sûreté de fonctionnement du client dès les phases de réponse à appel d'offre. Cette méthodologie ne devra cependant pas se substituer à la démarche de raisonnement nécessaire à toute analyse SdF mais devra, au contraire, structurer celle-ci afin de forcer les questionnements potentiels nécessaires.

Nous avons précédemment identifié les activités du concepteur durant le PRAO et les exigences orientées SdF à traiter. Il s'agit maintenant de caractériser une méthodologie, respectueuse des modes de fonctionnement de l'entreprise, permettant d'évaluer l'impact de ces exigences SdF dans un projet. Pour cela, plusieurs horizons temporels sont à considérer comme nous le montrons sur la Figure I-17.

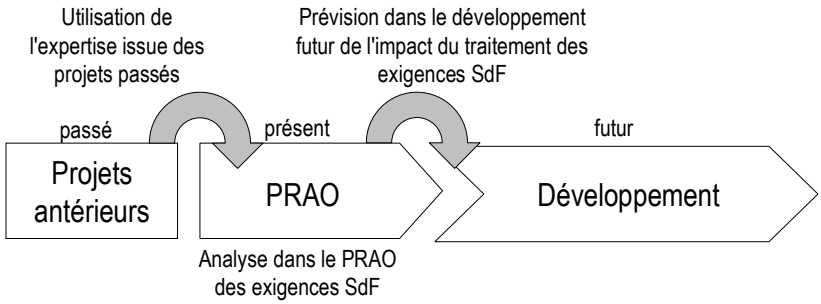


Figure I-17 : Différentes échelles temps à considérer

L'analyse en temps réel dans le PRAO est destinée à la réalisation d'analyses ponctuelles nécessaires à l'éclaircissement ou la compréhension d'un cas particulier vis à vis de la sécurité ou de la fiabilité du produit. Du point de vue du passé, l'utilisation de l'expertise des projets précédents est nécessaire dans un contexte où les informations ne sont pas stabilisées. Enfin, du point de vue du futur, il faudra définir les méthodes à engager dans le développement à venir afin d'avoir une bonne gestion de la SdF.
La juxtaposition de ces trois horizons temporels nécessite, d'une part, de proposer une solution permettant, à la fois, une continuité dans le temps (i.e. entre les cas passés, le PRAO présent et la suite du développement) et, d'autre part, d'être en mesure de capitaliser les connaissances et l'expertise sur ces trois niveaux temporels.

Il faut également proposer une solution d'organisation de la phase d'acquisition de façon à obtenir une répétabilité de la démarche. Les objectifs visés concernent, rappelons le, la définition de l'impact des exigences SdF dans un projet que ce soit au niveau des solutions ou d'éléments de solutions sur le produit ou au niveau des actions qui seront à engager durant le développement avec, dans les deux cas, le dimensionnement économique correspondant. Il faut donc proposer une organisation en différentes étapes instrumentées accompagnant le concepteur dans sa réflexion sur les aspects SdF.

La dernière caractéristique de la solution concerne la nécessité de considérer l'aspect multi-niveaux. Par multi-niveaux, nous entendons :

- le caractère multi-niveaux d'abstraction afin de pouvoir faire le lien entre les connaissances détaillées sur le produit et la SdF disponibles sur les projets précédents et les connaissances non stabilisées qu'il faudra manipuler durant le PRAO,
- le caractère multi-acteurs engendré par la pluridisciplinarité des produits considérés et par le traitement de la SdF par une équipe acquisition (dans le PRAO) et une équipe projet (dans le développement futur),
- le caractère multi-vues et multi-modèles qui découle des trois précédents.

Les concepts à prendre en compte sont présentés sur la Figure I-18.

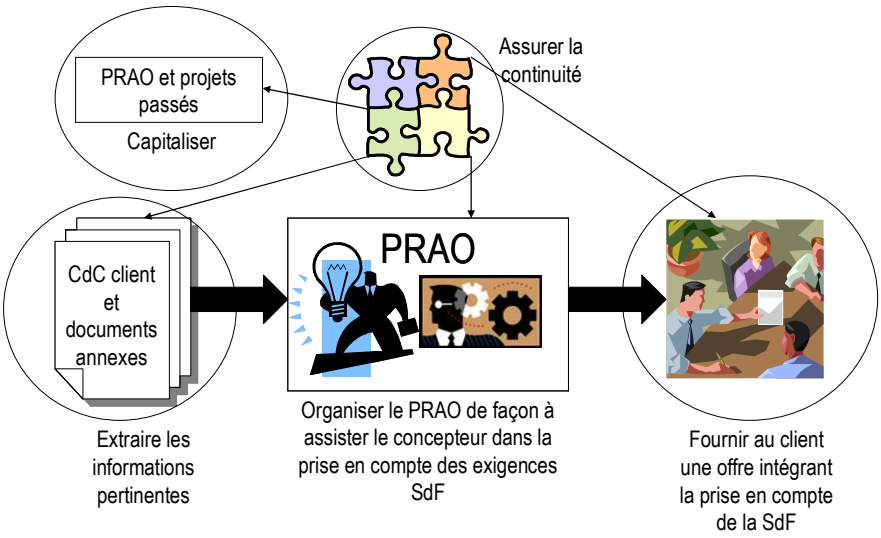


Figure I-18 : Concepts à intégrer dans la solution

L'extraction des informations pertinentes nécessite l'intégration dans l'organisation proposée pour le PRAO d'une démarche de traitement des cahiers des charges clients.

La fourniture au client d'offres intégrant l'impact et le coût de la SdF requiert :

- des analyses SdF de haut niveau dans le PRAO dans l'objectif de prévoir l'impact des exigences SdF sur le produit et sur la démarche à suivre,
- des activités d'estimation de coût de cet impact.

Enfin, la notion de continuité entre les différentes activités nécessite, d'une part, l'intégration de la démarche aux formes de fonctionnement en place dans l'entreprise mais aussi l'identification des activités SdF dans l'ensemble du cycle de vie afin de proposer des activités similaires, au moins sur le plan des concepts, durant le PRAO.

Au niveau de l'organisation du PRAO, il faudra disposer de représentations du produit intégrant les caractéristiques SdF dans l'objectif de réaliser des analyses SdF en temps réel durant le PRAO, puisque le produit n'existe pas encore.

Nous proposons sur la Figure I-19 une représentation à un haut niveau d'abstraction des concepts d'assistance qui devront être proposés dans l'organisation du PRAO.

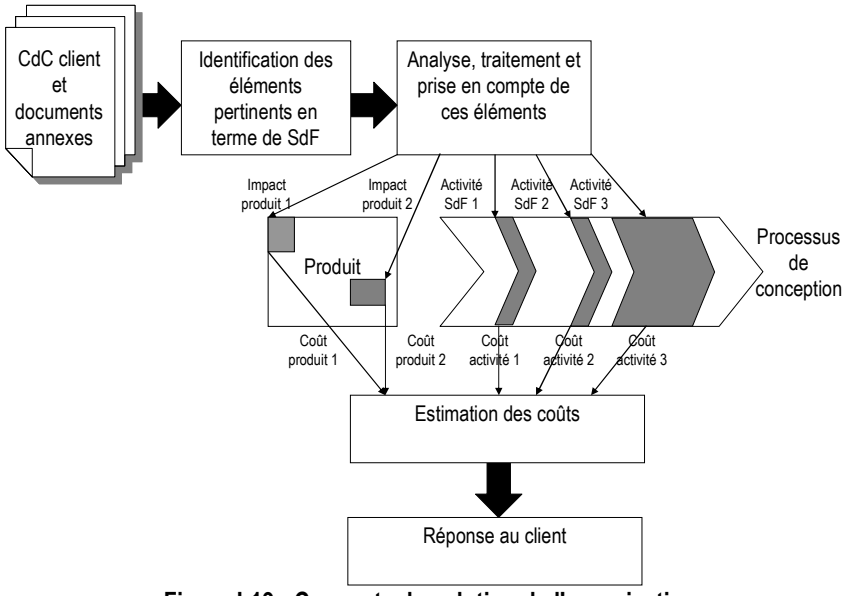


Figure I-19 : Concepts de solution de l'organisation

Le dernier élément à considérer est celui des représentations du produit qu'il faudra adapter, si ces représentations existent ou définir sinon afin de pouvoir réaliser des analyses SdF dans le PRAO. Ces analyses et la représentation sur laquelle elles s'appuieront seront cruciales puisqu'elles permettront de définir l'impact de la prise en compte de la SdF.

6. Conclusion

Ce chapitre visait, d'une part, à formuler plus précisément la problématique de nos travaux et, d'autre part, à préparer l'argumentation de la démonstration à développer et, par lui-même, celle de la suite du mémoire. Nous avons présenté le contexte industriel de l'étude, notamment l'organisation de l'industrie automobile et l'organisation interne des entreprises de ce secteur. Nous avons ensuite présenté succinctement les systèmes embarqués/mécatroniques considérés dans les travaux pour arriver à la problématique industrielle relative à une meilleure prise en compte de la SdF et une uniformisation des connaissances et compétences SdF des acteurs tout au long du cycle de vie du produit.

Dans une seconde partie, nous nous sommes focalisés sur les contraintes en lien avec la problématique abordée. Pour cela, nous avons analysé ces contraintes et présenté le bilan de l'état des lieux préliminaire effectué au début de la thèse. Les différentes caractéristiques identifiées ont ensuite été étudiées et généralisées afin de proposer des pistes d'amélioration en fonction du niveau de ces caractéristiques de façon générale. L'intérêt du bilan, en plus d'aider la caractérisation du problème, réside dans l'approche méthodologique et structurante utilisée pour le réaliser qui pourrait servir de base à une démarche organisée d'enquête (ou questionnaire) ou d'audit d'entreprise dans un autre contexte.

Nous avons proposé un panorama des travaux susceptibles d'être utilisés en appui de la problématique traitée ainsi qu'une analyse de l'existant sur le plan du processus de réponse à appel d'offre, des méthodologies SdF et du processus de conception.

La suite du mémoire est consacrée au développement de la solution. Dans un premier temps, nous présentons l'organisation du PRAO préconisée pour la prise en compte de la dimension SdF dans un projet ainsi que les supports de connaissance nécessaires à la mise en place et à l'instanciation de la solution dans une entreprise. La partie suivante concerne le développement des modèles produits nécessaires à l'analyse de la SdF dans le PRAO. Enfin, la dernière partie traite du couplage entre l'organisation du PRAO proposée et les supports de connaissances dans l'objectif de définir l'impact SdF dans un projet et d'évaluer économiquement cet impact.

Sur la base de l'ensemble de la réflexion préliminaire que nous avons relatée dans ce paragraphe, nous présentons l'organisation de la suite du mémoire en définissant les liaisons existantes entre les différents chapitres.
Le chapitre 2 sera tout d'abord consacré à la définition de la solution d'organisation du PRAO, des différentes étapes qui le constituent et de l'instrumentation qui leur sera associée. Le chapitre 3 concerne la définition et le développement des représentations du produit nécessaires à la mise en place de l'organisation du PRAO. Enfin, le chapitre 4 permettra d'établir la liaison entre les deux chapitres précédents comme cela est montré sur la Figure I-20.

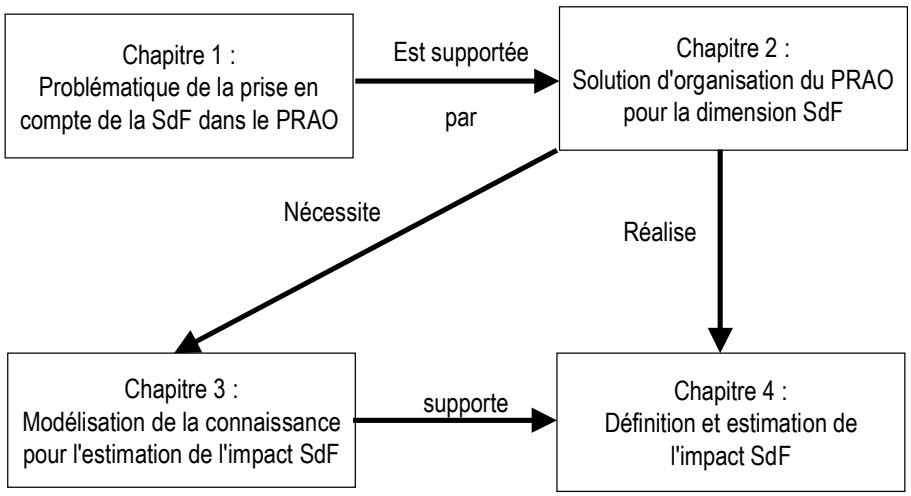


Figure I-20 : Organisation du mémoire

II. Chapitre 2 : Organisation et instrumentation du processus de réponse à appel d'offre

1. Introduction

Le but de ce chapitre est de présenter l'organisation du Processus de Réponse à Appel d'Offre (PRAO) que nous préconisons afin de prendre en compte les exigences SdF. L'objectif est d'arriver à définir l'impact de la "dimension" SdF dans un projet en termes de choix de solution et de la démarche à mettre en place et à appliquer dans le cadre du développement futur pour vérifier et valider cette dimension.

L'intégration de l'ensemble des contraintes dans la définition de cette organisation a nécessité une réflexion organisée en étapes successives ayant pour objectif de raffiner progressivement le problème. Ces étapes correspondent à différents plans d'abstraction de la problématique comme schématisé sur la Figure II-1.

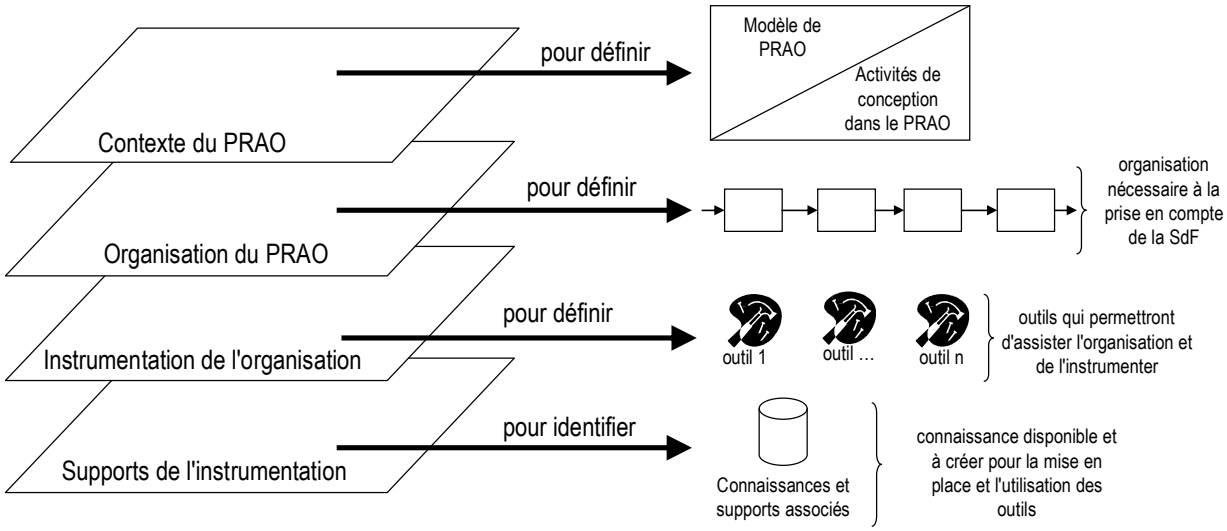


Figure II-1 : Plans d'abstraction pour la définition de l'organisation

Dans le premier plan d'abstraction figurent la modélisation du PRAO et de ses différentes étapes ainsi que l'identification des activités du concepteur durant ce processus. La définition des activités du concepteur est liée à la prise en compte des schémas de fonctionnement de l'entreprise dans le développement de l'organisation.

L'organisation du PRAO a pour objectif de proposer une méthodologie structurée d'analyse de la SdF afin d'aider les acteurs du PRAO dans la prise en compte de cette dimension et à rendre cette analyse reproductible. C'est le deuxième plan d'abstraction qui consiste en la définition d'une organisation en différentes étapes nécessaires pour passer des exigences client disponibles dans le PRAO à la définition et à l'évaluation de l'impact de ces exigences que ce soit au niveau du produit ou des méthodes nécessaires à leur validation et leur vérification.

La mise en place de la démarche et sa reproductibilité passent par la définition d'outils ou de principes d'activités qui

aideront les acteurs du PRAO dans l'analyse des exigences SdF. Cette instrumentation de l'organisation forme le troisième plan d'abstraction.

Enfin, le dernier plan d'abstraction consiste en l'identification de la connaissance existante ou à créer et est nécessaire à l'instrumentation des outils qui devront s'appuyer sur le savoir-faire de l'entreprise et s'intégrer au cadre de développement habituellement appliqué dans celle-ci. Ce plan revêt une importance essentielle dans la mesure où, pour prévoir l'impact de la SdF sur l'ensemble du développement futur du produit, il faut disposer de modèles sur lesquels s'appuyer pour cette prévision. Il faudra donc identifier la connaissance et les supports associés disponibles dans l'entreprise ainsi que la connaissance à créer pour supporter les outils.

Nous présentons, dans le premier paragraphe, le contexte du PRAO et la place du concepteur dans celui-ci dans l'objectif de développer une solution s'intégrant parfaitement au contexte de mise en œuvre. Nous nous intéressons ensuite à l'organisation définie pour la prise en compte de la SdF dans le PRAO et à la description des différentes étapes constitutives de celle-ci. Nous proposons enfin un bilan des supports de connaissances disponibles dans l'entreprise qui permettront de supporter l'instrumentation des étapes, instrumentation présentée dans la dernière partie de ce chapitre.

2. Contextualisation du processus de réponse à appel d'offre

2.1. Définition et modélisation du PRAO

Nous proposons un modèle de processus de réponse à appel d'offre que nous utiliserons par la suite en nous appuyant sur divers modèles issus de travaux concernant l'étude du cycle de développement de produit.

Dans [Chalal&al, 06], par exemple, les auteurs proposent un modèle de PRAO dans le cadre d'une problématique de capitalisation de la connaissance au cours de ces phases. Nous rappelons sur la Figure II-2 ce modèle traduit en français.

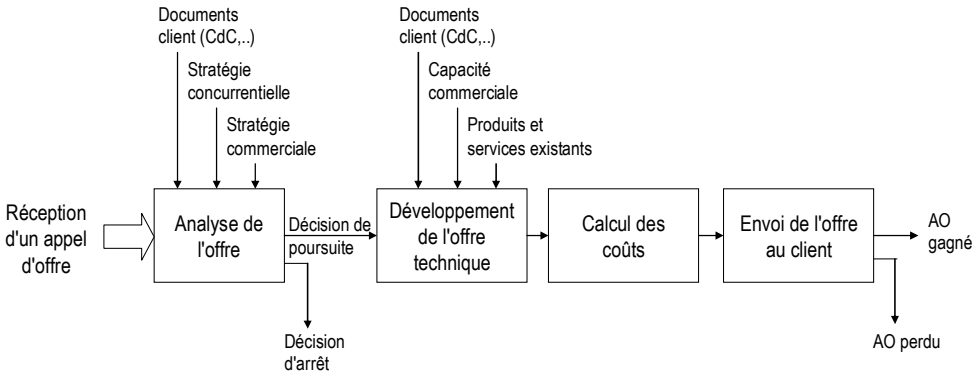


Figure II-2: Modèle d'appel d'offre adapté de [Chalal&al, 06]

On trouve, dans ce modèle, une première étape d'analyse de l'appel d'offre qui permet une prise de décision quand à la poursuite de l'AO par rapport à des orientations stratégiques de l'entreprise concernée, des critères commerciaux et concurrentiels mais aussi de la capacité de l'entreprise à répondre à la demande (faisabilité). La phase de définition de l'offre technique débute lorsque la décision de poursuite est prise. Cette définition s'appuie sur les documents de définition du produit fournis par le client ainsi que sur le savoir-faire et l'expertise de l'entreprise. Elle a pour objectif de définir des principes de solution répondant aux exigences du client. L'étape suivante de calcul des coûts est réalisée à

partir du concept de solution retenu, d'une évaluation des coûts de développement et de fabrication ainsi qu'en intégrant des paramètres clients (nombre de pièces par an,...,). Enfin, l'offre est envoyée au client qui émettra une réponse positive ou négative sur l'offre.

La littérature concernant les phases de réponse à appel d'offre est principalement orientée vers les stratégies commerciales. Peu de travaux sont consacrés à la description des différentes étapes de l'appel d'offre.

Dans le projet PRIMA[6] (Project Risk Management ou Management des risques projet), l'objectif était de fournir les méthodes et les outils pour l'analyse, la capitalisation et l'estimation des risques afin d'améliorer la compétitivité durant la phase d'acquisition d'un projet [PRIMA, 99]. Parmi les résultats de ce projet, nous reprenons la description des étapes du PRAO proposées dans [Zafra-Cabeza&al, 02] dans le cadre de la définition d'un système d'aide à la décision en phase d'acquisition.

Le PRAO est composé d'une première phase d'analyse des documents remis par le client afin de statuer sur la décision de poursuite ou non de l'appel d'offre. Dans le cas d'une décision de poursuite, l'étape suivante consiste en la création d'une solution technique (par le biais d'une approche "Top-down"). Lorsque la solution technique est définie, l'équipe d'acquisition doit identifier les différents fournisseurs potentiels pour chaque élément à développer. Elle doit aussi permettre d'analyser l'impact que pourraient avoir ces différents fournisseurs sur la proposition finale par rapport à des paramètres tel que le coût, la qualité, le planning, la viabilité. Enfin, l'outil développé dans PRIMA permet de définir plusieurs propositions pour un même appel d'offre : la meilleure solution est sélectionnée à l'aide d'une analyse multicritère.

Nous nous appuyons sur ces résultats pour proposer le modèle descriptif du PRAO que nous considérerons par la suite (Figure II-3). On retrouve globalement les mêmes étapes que celles du modèle de la Figure II-2, modèle qui synthétise bien les activités successives réalisées durant le PRAO.

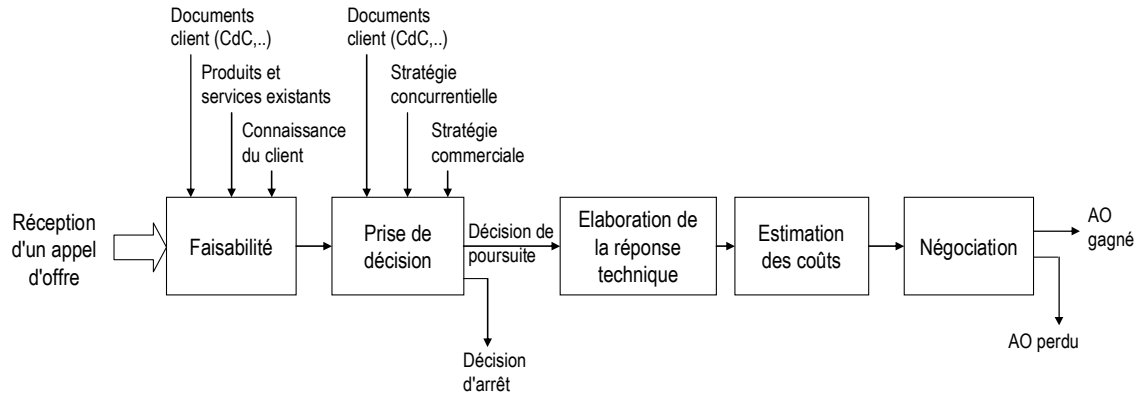


Figure II-3 : Modèle de processus de réponse à appel d'offre

Ce modèle comprend une phase d'analyse de l'offre (de la réception de l'AO à la décision de poursuite) dans laquelle nous avons séparé l'étude de faisabilité (au sens technique) de la prise de décision liée, elle, à des paramètres stratégiques et commerciaux (la faisabilité technique pouvant être un de ces paramètres). On trouve ensuite l'étape d'élaboration de la réponse qui consiste à définir les principes de solutions puis celle d'évaluation économique pour le

[6] PRIMA est un projet de recherche européen IST-1999-10193 soutenue par la société des technologies de l'information qui s'est déroulé sur une période de 2 ans à partir de janvier 2000.
http://www.esi2.us.es/prima/

chiffrage des concepts de solutions retenus et des coûts annexes. L'étape de négociation consiste en l'envoi de l'offre au client et la discussion potentielle avec ce dernier sur des points techniques ou économiques litigieux nécessitant des modifications. Cette étape débouche finalement sur la réponse positive ou négative de la part du client.

Le processus de réponse à appel d'offre présente plusieurs spécificités dont certaines ont déjà été évoquées dans le chapitre 1 :

- la performance de l'entreprise impose une forte réactivité et le PRAO doit être généralement réalisé dans un temps très court (de l'ordre de quelques semaines) [Angueniol&al, 05],
- les décisions doivent être rapidement prises, s'appuyant sur les meilleurs compromis coût, qualité, délais,
- les informations et données sur lesquelles le PRAO est initialisé sont partielles (connaissance des grandes lignes du besoin), imprécises (besoins parfois sous-évalués ou surévalués) et incertaines ; de plus, elles sont souvent distribuées (réparties entre différents acteurs),
- l'élaboration de la réponse à l'appel d'offre impose d'anticiper sur les développements futurs et de caractériser le scénario de réalisation qui pourra être mené.

Ces spécificités permettent déjà d'esquisser certains traits de la solution à mettre en place :

- la nécessité d'une organisation efficace de l'information (données techniques, connaissance normative, connaissance des compétences,...) qui permettra de trouver toutes les informations nécessaires rapidement [Chalal&al, 05],
- l'importance de s'appuyer sur l'expertise acquise, utilisant le retour d'expérience des cas passés.

L'objectif, dans le PRAO, est de proposer une réponse au client sous la forme d'un principe de solution. Pour cela, l'équipe acquisition (généralement réduite et représentant l'ensemble des disciplines de l'entreprise dispose des documents fournis par le client : cahier des charges présentant le besoin, documents annexes tels que références normatives, cadre qualité du client,...

L'objectif est de fournir une réponse "optimale" en un temps réduit en gardant en mémoire que les engagements pris durant ces phases vont conditionner une grande partie des coûts du produit (80% des coûts du produit sont fixés dans la phase de création du concept [Sallaou&al, 05]).

Dans le cadre de nos travaux, nous nous concentrons sur les aspects sûreté de fonctionnement de la réponse ; cependant, cette dimension sûreté de fonctionnement ne peut être décorrélée de la conception de la solution.

2.2. Activités de conception dans le PRAO

Dans le PRAO, l'objectif est de fournir une réponse au client à partir des documents qu'il fournit. Afin de définir les actions successives que nécessite la création d'un concept de solution, nous avons établi une comparaison avec les étapes constitutives d'un processus de conception classique. Nous avons considéré les processus de conception présentés dans le paragraphe 4.3 du chapitre 1 dans l'objectif de dégager les différentes étapes qui nous intéressent plus particulièrement. Les analyses effectuées ont permis de conclure que la phase correspondant au PRAO dans le processus de conception est celle de conception préliminaire sur laquelle nous nous focalisons ici.

En reprenant le processus de conception de Pahl et Beitz (cf. [Pahl et Beitz, 96]) à un niveau plus détaillé, nous

allons pouvoir identifier les tâches réalisées durant le PRAO. Sur la Figure II-4, nous donnons un aperçu des activités réalisées durant les premières phases du cycle de vie : la phase d'analyse du besoin et celle du développement du concept. Ces deux phases contiennent les activités de :

- clarification du besoin (client),
- élaboration des spécifications,
- identification des principaux problèmes/contraintes,
- création de la structure fonctionnelle,
- recherche de principes de solution,
- combinaison et stabilisation des variantes de concept,
- évaluation des concepts de solution d'un point de vue technique et financier,

qui vont permettre d'obtenir les informations demandées par le client dans le processus de réponse à appel d'offre.

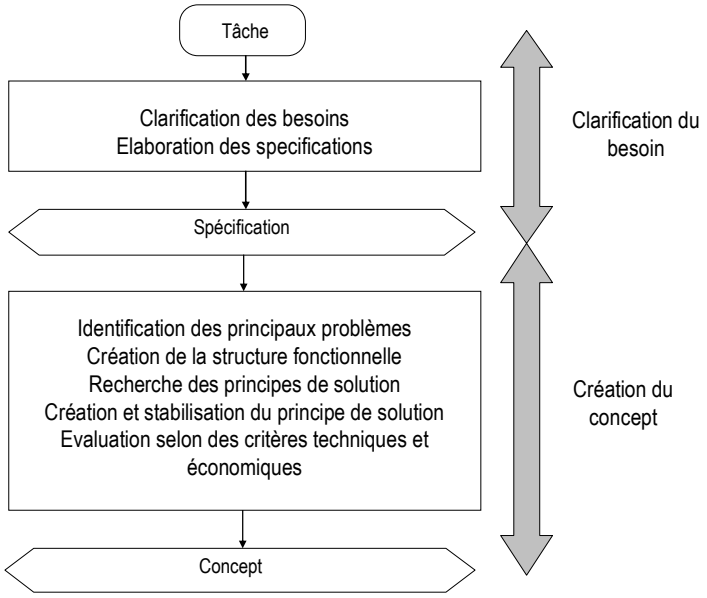


Figure II-4 : Extrait du processus de conception d'après Pahl et Beitz

Dans [Macmillan&al, 01], les auteurs détaillent le contenu de ces phases en y incluant le concept de "partie prenante" (le client dans notre cas) qui n'est pas développé dans les recherches consacrées au processus de conception.

Les activités ainsi définies permettent de passer d'un besoin client à un concept de solution chiffrée. Nous proposons ensuite un modèle haut niveau de ces activités permettant de retracer la démarche du concepteur, plus particulièrement dans la phase d'élaboration de la réponse du PRAO (Figure II-5).

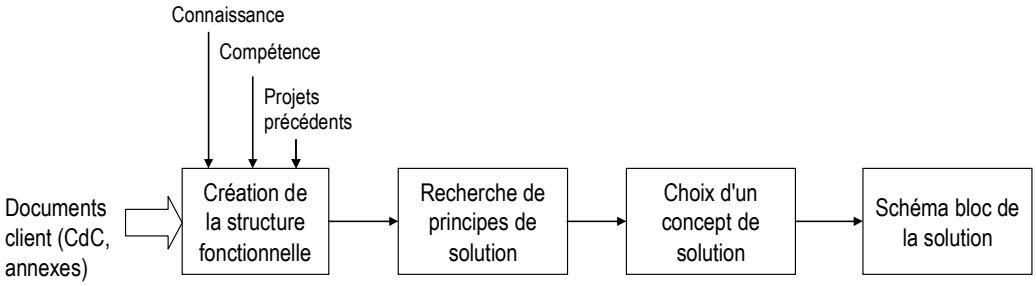


Figure II-5 : Activités de conception durant le PRAO

Nous disposons ainsi de la démarche détaillée que doit suivre le concepteur dans le PRAO pour l'ensemble du produit. Nous focalisons ensuite sur les problématiques de prise en compte de la SdF dans le contexte du PRAO.

2.3. Problématique du traitement de la SdF dans le contexte du PRAO et intérêt de la proposition

La problématique essentielle liée à la prise en compte de la sûreté de fonctionnement dans le PRAO réside dans les caractéristiques même de cette phase. Les informations sur lesquelles vont s'appuyer les différentes activités ne sont pas consolidées ; en effet :

- le besoin est exprimé avec un niveau de détail minimum,
- les exigences SdF peuvent être plus ou moins explicites en fonction du client,
- le produit sur lequel doit être analysé l'impact des exigences SdF n'existe pas encore.

De plus, le PRAO est réalisé sur une durée très courte qui impose de faciliter l'accès aux données relatives à la prévision de l'impact des exigences SdF.

Enfin, comme nous l'avons vu dans le paragraphe 4.3 du chapitre 1, il n'existe pas de méthodes traitant la SdF dès le PRAO et proposant un formalisme permettant le traitement de cette dimension par un ensemble d'acteurs projet différents. Il est donc indispensable de faire une adaptation du PRAO pour la gestion de la SdF au plus tôt.

Afin de définir l'organisation, deux questions particulières ont été considérées :

- Qu'entend-on par impact sûreté de fonctionnement ?
- Quelles informations du cahier des charges client permettront d'évaluer cet impact ?

L'impact SdF a déjà été évoqué comme intervenant à deux niveaux :

- celui du produit, intégrant les développements à effectuer sur le produit pour le rendre fiable et sécurisé et incluant les conséquences des choix physiques et d'architecture pour respecter les exigences clients relatives aux caractéristiques de fiabilité et de sécurité,
- celui de la démarche à mettre en place pour analyser, vérifier et valider les performances SdF.

Au niveau des informations disponibles dans les documents client, il faudra identifier :

- les exigences de performance SdF,
- les exigences normatives relatives à la SdF,
- les exigences sur la gestion de la SdF : procédures, méthodes,...,
- les exigences métier qui peuvent contenir des éléments relatifs à la SdF.

Pour une intégration optimale de l'organisation du PRAO préconisée dans les routines de conception, il faut dresser un état des éléments/modèles/connaissances disponibles au sein de l'entreprise afin :

- d'intégrer ces modèles aux différentes étapes de la solution,
- de respecter les habitudes du concepteur afin de lui permettre de s'approprier aisément la solution proposée,
- d'identifier les éléments à créer dans l'objectif de mettre en place l'instrumentation.

De plus, pour que l'intégration de l'organisation proposée soit facilement acceptée par les acteurs, il faudra veiller à définir clairement les objectifs de cette nouvelle méthode de travail [Perrin&al, 03].

Toutes ces raisons nous ont conduits à présenter les différents éléments que nous exploiterons par la suite suivant la logique donnée sur la Figure II-1:

- présentation globale de l'organisation correspondant au plan d'abstraction "organisation du PRAO",
- détail de chaque étape, principes utilisés et modèles nécessaires correspondant au plan d'abstraction "instrumentation de l'organisation",
- présentation des différents types de supports généralement disponibles dans une "mémoire" d'entreprise correspondant au plan "Supports de l'instrumentation",
- couplage entre les deux plans précédents pour l'instrumentation des différentes étapes de l'organisation.

3. Organisation du PRAO pour la prise en compte de la SdF

Nous proposons dans ce paragraphe l'organisation que nous avons établie pour le PRAO et que nous préconisons pour la prise en compte de la dimension SdF à ce niveau. Nous détaillons ensuite les étapes successives de l'organisation proposée et les principes sur lesquelles elles reposent.

3.1. Présentation générale de l'organisation du PRAO

La performance du PRAO sera caractérisée par les résultats directement produits : réponse à l'AO, réaction et réponse du client,..., mais aussi par la manière avec laquelle ces résultats ont été obtenus ; elle concernera principalement l'efficacité et l'efficience du PRAO.

Une performance maximale sera atteinte lors de l'acceptation de l'offre par le client avec un effort limité pour la création de la réponse. Dans le cas d'un refus de sa part, il faudra analyser les remarques du client concernant l'offre proposée ainsi que les causes de celui-ci afin d'améliorer la performance pour les AO suivants.

L'efficacité correspond au fait que l'engagement du PRAO permet d'atteindre le résultat prévu. Les mesures quantifieront le rapport entre les résultats fournis et les objectifs assignés. Il s'agira, par exemple, de la concordance entre le scénario prévu dans le développement et celui réellement engagé, de celle entre la prévision des coûts de la sûreté de fonctionnement et les coûts réels au final.

L'efficience caractérise la notion de moindre effort ou de temps minimal requis pour atteindre ce résultat. Les mesures quantifieront le rapport entre les résultats fournis et les moyens engagés.

Il est sûr que la performance du PRAO pourra être améliorée par une exploitation adaptée du retour d'expérience (tant par les expériences positives que négatives). La réalisation de performance nécessite évidemment :

- de comprendre le cahier des charges : **expertise technique** engagée pour décrypter le CdC, les attentes du client et les besoins spécifiques,
- de prendre en compte la « logique client », ses méthodes de travail et son approche : **expertise méthodologique**,
- de faire une offre « optimisée » : **expertise commerciale**.

La prise en compte de la dimension SdF dans la réponse à un appel d'offre peut être considérée via l'enchainement d'un certain nombre d'étapes regroupées dans un sous-processus Organisation du PRAO. Il s'agit des étapes :

Filtrage → Traduction → Projection → Evaluation → Restitution

qui correspondent respectivement (cf. Figure II-6) :

- au filtrage des données du CdC, afin d'extraire celles à partir desquelles sera conduite l'analyse de SdF à l'intérieur du PRAO,
- à la traduction des exigences en termes de contraintes associées, exprimées dans le vocabulaire courant de l'entreprise,
- à la projection sur les phases aval du processus de développement des actions à réaliser, pour intégrer les spécifications FMDS précédemment établies,
- à l'évaluation de la performance et du coût correspondant aux choix réalisés sur le produit mais aussi sur la démarche d'organisation spécifiquement mise en place,
- à la restitution sous forme de synthèse de la cotation réalisée, démontrant l'atteinte des objectifs techniques sur le plan SdF et présentant la dimension économique des solutions pressenties.

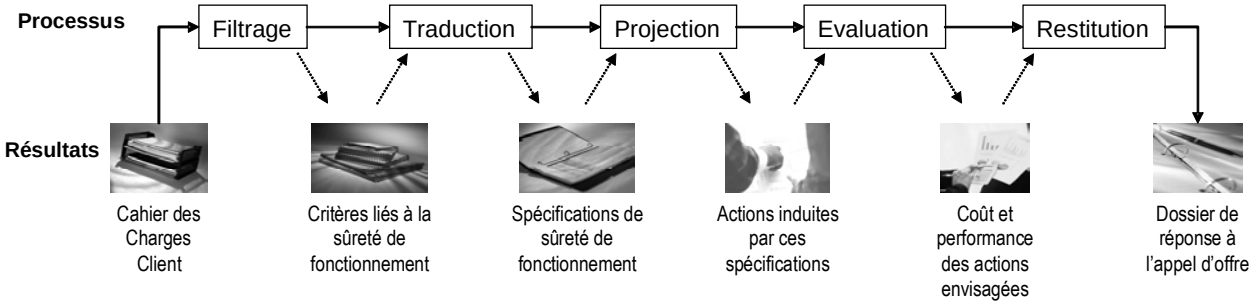


Figure II-6 : Solution d'organisation du PRAO

Les cinq étapes de cette organisation sont décrites en détail à la suite puis globalement positionnées par rapport au contexte du PRAO.

3.2. Présentation des étapes de l'organisation du PRAO

3.2.1. Etape Filtrage

- *Définition*

Le filtrage d'information appartient au domaine de la recherche d'informations. Cette recherche d'informations est généralement définie comme l'ensemble des techniques, méthodes et outils permettant de sélectionner, à partir d'une collection de documents, ceux qui sont pertinents par rapport à la requête d'un utilisateur [Baziz, 05]. La recherche d'informations est, de plus, souvent synonyme de grande quantité d'informations alors que, dans le cadre de nos travaux, nous faisons de la recherche d'informations dans un document unique. Comme le remarque Couto dans [Couto&al, 02], "*un intérêt relatif a été porté [...] sur les techniques d'accès au contenu de documents simples [...]. On retrouve néanmoins les travaux de [*Jacquemin&al, 02*] pour la visualisation de larges documents ainsi que bon nombre de travaux en résumé automatique*".

Le filtrage, au sens général [FUTURA_SCIENCE_WEB], est défini comme "*une fonction (un ensemble de fonctions ou combinaisons de fonctions) qui applique un certain nombre de transformations à son espace d'entrée produisant, en*

sortie, un ensemble contenant seulement les éléments d'entrée qui respectent certains critères. Les éléments sélectionnés peuvent être transformés ou non".

- *Cadre d'utilisation*

Dans l'organisation du PRAO, le filtrage consistera à identifier les éléments relatifs à la sûreté de fonctionnement dans les documents de définition du produit fournis par le client (Figure II-7). La notion d'identification (et non d'extraction, généralement utilisée dans le domaine de la recherche d'information) est employée afin de bien exprimer la finalité de cette étape. L'objectif n'est pas en effet de se substituer au concepteur dans l'étape d'analyse du cahier des charges client. La SdF est basée sur une démarche intellectuelle de questionnements successifs par rapport à des caractéristiques particulières d'un produit, il ne faut donc pas remplacer la réflexion de l'analyste par une automatisation complète de l'examen du CdC mais assister celui-ci dans l'identification des éléments du CdC relatifs à la SdF.

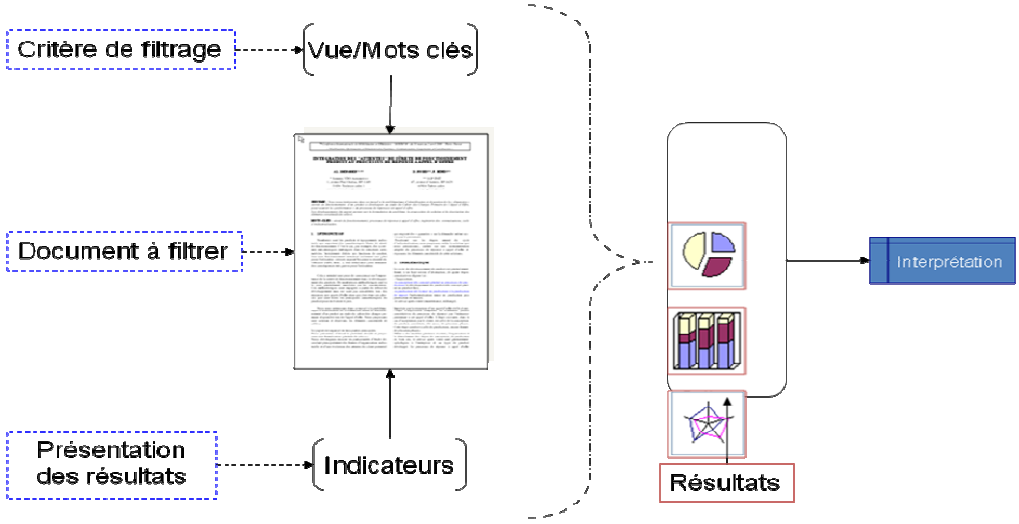


Figure II-7 : Caractéristiques du Filtrage

- *Objectifs*

Un débat existe sur la différence entre recherche d'informations et recherche de l'information. La seconde approche représente l'ensemble des méthodes, procédures et techniques ayant pour objectif d'extraire d'un document ou d'un ensemble de documents les informations pertinentes.

Le filtrage peut être effectué à différents niveaux de finesse, avec :

- à un premier niveau, l'affichage d'un aperçu global du cahier des charges et de son contenu
- à un second niveau, la fourniture d'informations quantitatives concernant un CdC donné via notamment les indicateurs statistiques : nombre de mots clés relatifs à la SdF présents dans le document, nombre d'occurrences de chaque mot, placement de ces mots,...,

Nous qualifierons ces deux approches respectivement d'approche élémentaire pour caractériser la démarche d'extraction simple d'information relative au contenu et d'approche analytique celle correspondant à une compilation chiffrée des informations élémentaires contenues dans le document.

- *Documents cibles*

Les documents objets du filtrage (espace d'entrée) sont pour nous des cahiers de charges client. Ce type de document et les annexes qui lui sont associées sont le plus souvent des documents structurés (titres, parties, phrase,...). La dénomination de "document structuré" s'applique à des documents composés d'entités textuelles organisées principalement de façon hiérarchique. Le modèle d'un document structuré représente le document selon sa structure logique. Dans ce type de document, les entités textuelles fournissent des informations par leur contenu mais aussi par leur position hiérarchique.

Les documents à analyser ont plusieurs caractéristiques :

- la langue d'expression : les documents peuvent être rédigés dans la langue du client (français, anglais, allemand) ; même si la tendance est aujourd'hui à la rédaction de documents en anglais ceci n'est pas systématique et il faut donc posséder un outil multilingue,
- leur structure : en fonction du client et du type de produit, l'organisation du document sera différente ; généralement ce sont des documents structurés organisés en différentes parties séparées par des titres mais les logiques de découpage du document en partie pourront changer selon les clients (organisation du document par rapport au métier, par rapport aux fonctions du produit,...,),
- leur format : le format le plus répandu est le format "pdf" (portable document format) mais on peut trouver des documents Microsoft Word ou Excel. Il faut donc un outil capable d'étudier des documents multi-formats. La problématique ajoutée par le format "pdf" concerne le fait que ce format est destiné à l'échange d'information et a pour objectif de se limiter à la visualisation et à l'impression de document [Rigamonti&al, 04].

- *Caractérisation des filtres*

Pour obtenir des informations, les concepts du Text-Mining apparaissent pertinents, notamment par le biais de l'analyse statistique de texte. L'activité d'exploration pose toutefois un certain nombre d'interrogations [Minel, 04], découlant du constat que l'étape préalable à tout traitement informatique est la construction d'un modèle de représentation d'un document : "*Que décrire dans un texte ? Quelles organisations textuelles faut-il décrire ? Existe-t-il des unités textuelles élémentaires et comment celles-ci sont elles organisées ?".* Ce point est important car, contrairement aux hypothèses faites dans les travaux que nous avons consultés sur la recherche d'informations, nous ne savons pas à l'avance quelle sera la structure du document puisque celui-ci émane du client et est extérieur à l'entreprise. Malgré tout des invariants sur la logique de construction des filtres peuvent être établis.

Dans [Couto&al, 04], les auteurs s'intéressent à l'utilisation des structures d'un texte afin de guider la lecture ou de proposer des parcours de lecture en fonction de l'utilisateur. Cette préoccupation émane d'un constat réalisé par Souchier dans [Souchier&al, 03] qui considère qu'un texte fournit de multiples pistes d'interprétation, en fonction du lecteur concerné via les informations sémiotiques qu'il fournit ; il se démarque ainsi de la navigation hypertextuelle. Avec l'hypertexte, l'information dans les documents est présentée de façon à permettre une lecture non linéaire grâce à la présence de liens sémantiques activables. On peut ainsi sauter d'un paragraphe voire d'un document à un autre selon des chemins préétablis : les liens hypertextes, appelés aussi liens hypertextuels. La navigation hypertextuelle fixe l'information directement dans le document et de façon unique.

Souchier considère, selon un angle de vue différent, que la lecture d'un texte correspond à "*l'expression d'un processus cognitif qui convoque des connaissances qui sont propres à la finalité de la navigation*". La navigation dans un CdC est un processus cognitif dans la mesure où il est évident que les acteurs vont parcourir le CdC en fonction de leur besoin. Pour les entrées/sorties d'un système embarqué, par exemple, l'électronicien cherchera la nature des entrées afin de définir les dispositifs de mise en forme adaptés, l'informaticien visera le nombre d'entrées qu'il devra traiter dans les différents modules logiciels, le mécanicien cherchera, lui, à identifier si un type de connecteur est préconisé par le client pour l'acquisition de ces entrées. Les arguments avancés par Couto cadrent donc bien avec notre problématique et montrent en particulier que les filtres utilisés pour extraire les informations recherchées sont très liés à celui qui cherche à les récupérer.

Remarquons que peu de travaux s'intéressent à ces aspects hormis ceux de Couto et Minel. Nous nous appuierons donc sur leurs travaux dans la partie instrumentation de l'étape Filtrage. Plusieurs éléments sont à considérer pour mettre en place un outil de navigation textuelle. Nous les présentons dans le tableau ci-dessous et les instancions à la problématique de l'étude relative à l'entreprise partenaire.

Eléments à prendre en compte	Contexte considéré
Objectif de la navigation	assister la lecture d'un cahier des charges ou d'un document client d'un point de vue SdF
Informations recherchées	tous les éléments du (ou des) document(s) relatifs à la SdF
Types de documents analysés	documents structurés de description d'un produit dans des formats divers

Tableau II-1 : Caractérisation de la navigation textuelle

La caractérisation des filtres pour l'extraction des informations élémentaires (niveau 1) utiles requiert la prise en compte de différentes caractéristiques comme :

- le point de vue d'expression des exigences : la forme la plus courante des premiers échanges avec un fournisseur consiste généralement à lui faire part du besoin sur les fonctionnalités attendues du produit ; cependant, dans le cas où le client consulte un fournisseur, par exemple, pour une évolution d'un produit déjà existant, il peut s'exprimer d'un point de vue structurel,
- l'expression des unités concernant les performances du produit : ces unités pourront différer en fonction des clients et des pays d'origine,
- la forme d'expression des exigences : elles pourront se présenter de manière différente en fonction de l'expertise SdF du créateur du document ; par exemple, un client maîtrisant une norme pourra proposer une partie dédiée à l'explicitation de cette norme alors qu'un autre intégrera dans le document un extrait de cette norme ou uniquement une référence à cette dernière,
- la forme même des termes utilisés relatifs à la SdF : les termes pourront être écrits dans des langues différentes, mal orthographiés [Tuffery, 06], représentés sous forme d'abréviation, l'ordre des mots dans une phrase pourra ne pas être logique, etc.

Les filtres devront nécessairement prendre en compte ces disparités de formulation et de représentation. Ils s'appuient pour cela sur la notion de vues. Nous avons défini différentes "vues" du produit : vue fonctionnelle, vue structurelle et

vue SdF. Chaque vue est constituée d'un ensemble pertinent de termes descriptifs judicieusement choisis.
Remarquons que ces filtres basés sur les vues produit s'appliquent au niveau 1 d'analyse (approche élémentaire) pour l'extraction ou la visualisation de l'information dans le CdC par le biais d'un utilitaire de recherche de mots clés ou de combinaisons de mots clés permettant d'identifier les exigences SdF. Ils s'appliquent également au niveau 2 (approche analytique) en permettant d'évaluer le nombre d'occurrences dans le CdC client puis d'identifier les parties du document où apparaissent ces termes.

Au niveau second niveau d'analyse il est intéressant, en effet, de remarquer que l'étude du positionnement de l'information dans le document peut revêtir un certain intérêt. Une entité textuelle recherchée qui apparaît dans un titre diffère ainsi en termes d'importance, de la même entité située dans le corps d'un paragraphe. Un mot clé ou un terme référencé n'aura pas, par exemple, la même portée s'il figure dans un titre, une note de bas de page ou dans une annexe de document.
Dans [Ho-Dac&al, 04], les auteurs s'intéressent à la fonction des titres dans un document qu'ils définissent comme ayant un rôle de segmentation, de hiérarchisation et d'organisation du discours. Les titres ont, de plus, un rôle visuel important puisqu'ils permettent d'avoir un aperçu rapide du contenu du document.
A ce niveau d'analyse, les filtres établis basés sur les vues considérées devront permettre, par une interprétation statistique (nombre d'occurrence des mots clés) ou de positionnement (placement des mots clés au sein du CdC) de faciliter la lecture de l'utilisateur et de l'orienter vers des recherches plus approfondies. Par exemple, s'il apparaît que les exigences sont concentrées dans un périmètre réduit du CdC, il sera conseillé à l'utilisateur une lecture attentive de cette partie du CdC. Si des mots non recherchés dans la première analyse figurent souvent dans les exigences extraites, il lui sera conseillé d'affiner la recherche à partir de ces mots.

La définition de différentes vues présente plusieurs intérêts. Dans le contexte de l'étude abordée on peut noter que mise à part la vue fonctionnelle, les autres vues peuvent encore être affinées :

- vue structurelle : différentiation des métiers (électronique, logiciel, mécanique),
- vue SdF : identification des connotations générales ou en lien avec les performances, la démarche, les normes, …

Le passage de différents filtres et l'ordre considéré conduit à des résultats très différents. La démarche est donc réellement définie par l'utilisateur et interactive puisqu'elle permettra d'adapter la démarche de filtrage en fonction des résultats intermédiaires obtenus.

Remarquons enfin que cette approche de filtrage par vues n'est pas limitée à l'analyse d'un cahier des charges mais offre la possibilité d'explorer tout type de document. Dans le cadre de l'étude conduite ici on pourra imaginer utiliser ces filtres pour extraire les informations pertinentes contenues dans les supports de connaissances que nous avons identifiés comme, par exemple, la recherche dans les supports d'expériences S_E d'une problématique déjà rencontrée dans un AO ou encore, dans les supports normatifs S_N, d'un point de règlementation particulier.

Nous illustrons sur la Figure II-8 les différentes vues définies ainsi que les résultats obtenus sur un exemple. L'intérêt de

l'illustration réside dans l'affichage des différentes caractéristiques contenues dans un CdC et que l'on va pouvoir combiner. Les vues recherchées sont ici, d'un point de vue SdF :

- une vue générale : on recherche les mots qui caractérisent la SdF : sûreté de fonctionnement, fiabilité, sécurité,...,
- une vue attributs SdF et métriques : lambda, taux de défaillances, niveau de sécurité,...,
- une vue méthodes avec les objets manipulés : analyse préliminaire des risques, évènements redoutés,...,

Les autres vues recherchées concernent :

- la vue fonctionnelle du produit,
- les vues structurelles pour différents métiers.

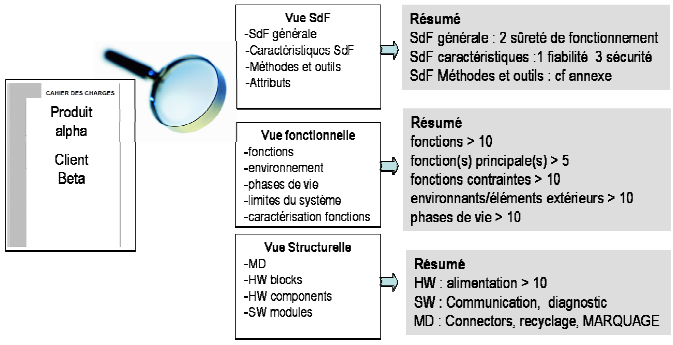


Figure II-8 : Exemple de vues et résultats

Cette approche sera appliquée à chaque métier de l'entreprise par la création de vues spécifiques permettant des filtrages multi-vues afin de lier le métier à la SdF ou identifier les exigences SdF plus particulièrement destinées au métier.

- *Outils de filtrage*

Il existe différents outils de recherche d'informations. Plutôt que de présenter un panorama des outils existants, aux fonctionnalités bien plus puissantes que celles dont nous avons besoin, nous préférons faire un bilan des fonctionnalités existantes dans les différents outils afin d'identifier celles utiles pour la solution. En fait, comme nous l'avons vu dans le paragraphe précédent, nous voulons effectuer, dans un premier temps, une analyse statistique du document (analyse quantitative) puis, dans un second temps, traiter le texte de façon à permettre la navigation textuelle et identifier les entités pertinentes. Pour la première partie, les fonctionnalités d'analyse statistiques des outils du Text-Mining pourront être utilisées ; pour la seconde partie, nous proposons de reprendre les concepts développés par Couto et Minel dans leurs différents travaux.

Le Text-Mining est destiné à quantifier un texte ou les parties d'un texte pour en extraire les structures signifiantes les plus fortes, établir des liens entre les termes et les documents, analyser les documents en leur associant des informations qualitatives et quantitatives structurées,... Un outil de Text-Mining ajoute de l'information (information non explicite ou présente au départ) au contenu d'un document [Faure, 07] dans l'objectif de classifier des documents et de matérialiser visuellement le contenu du document sans le lire. Ce type d'outil propose généralement deux types d'approches : statistique et sémantique. L'approche statistique a pour objectif d'étudier le texte de façon quantitative. Les fonctionnalités sont le calcul du nombre d'occurrences d'un terme ou de co-occurrences de termes, le classement d'apparition des termes présents dans le document.

Les principales fonctionnalités des outils du commerce (SPAD, SAS, TEMIS,...) sont, à ce niveau :

- le traitement simultané d'une ou de plusieurs variables textuelles : recherche du nombre d'occurrences de différents termes,
- la construction du vocabulaire d'un ensemble de documents par l'étude des segments répétés : mot, suite de mots,...,
- le filtrage multicritères et sélection de mots,
- l'édition de statistiques sur les mots et segments répétés,…

La plupart des logiciels de ce type proposent maintenant la personnalisation des programmes en fonction du besoin de l'entreprise en mettant à disposition des interfaces de programmation simplifiés. Le principal inconvénient de ces logiciels reste cependant leur coût. Le lecteur intéressé trouvera plus de renseignements dans [Quatrain&al, 04] ou sur le site des différents logiciels.

Nous avons également considéré les fonctionnalités des outils de recherche fournis dans les logiciels de traitement de texte (fonction "Search" d'Adobe ou "Rechercher" de Microsoft). Ces outils permettent d'obtenir des résultats visuels proches de ceux que nous recherchons (texte d'origine, différentes occurrences du terme et surlignage dans le texte d'origine) sans offrir toutefois la possibilité de prédéfinition de filtres d'informations complexes, c'est le cas notamment d'Adobe. Dans les logiciels Microsoft, la fonction "rechercher" permet de naviguer entre les différentes occurrences du mot dans le texte et ne permet pas de prédéfinir des filtres. Il est cependant possible de définir des "Macros" par le biais du langage VISUAL BASIC intégrant des fonctions de recherche de chaîne de caractères, de surlignage et qui permet de traiter le document en conservant son état d'origine agrémenté d'informations supplémentaires. Cette solution est intéressante même si elle se heurte au problème des fichiers au format pdf[7].

Le dernier produit étudié dans notre travail et sur lequel nous avons effectué de nombreux tests est le logiciel POWERGREP. Cet outil permet de réaliser l'ensemble des tâches nécessaires à notre étude, sa limite réside dans la transformation initiale du pdf en fichier texte. Les fonctionnalités sont multiples : recherche de mots, de mots proches, d'expressions régulières[8], de nombre d'occurrences d'un terme, etc. L'annexe II- A propose une présentation de l'outil et de ses fonctionnalités.

- *Présentation des résultats*

La présentation des résultats peut être à deux niveaux dans la même logique que celle ayant conduit à séparer les approches élémentaire et analytique. On trouvera ainsi en éléments de sortie du filtrage :

- les informations brutes issues directement du texte via l'analyse de niveau 1,
- les informations quantifiées relatives au traitement statistique issu de l'analyse de niveau 2.

Notons que les opérations de visualisation peuvent être de deux types selon qu'elles concernent la mise en relief d'une

[7] Dans le cadre de tests réalisés pour la thèse, nous avons converti des fichiers pdf en document Word et les avons traités avec des macros : les résultats sont intéressants.

[8] Des exemples d'expressions régulières sont donnés en annexe II-A.

information (modification de l'apparence de l'unité textuelle recherchée : surlignage, taille de police,...,) ou l'aide contextuelle (affichage d'informations sur l'unité textuelle).

Rappelons ici que l'objectif de la thèse est d'abord la définition d'une méthodologie. Dans cette logique, notre cible ne concerne pas le développement d'une suite logicielle complète. Les exemples proposés permettent de vérifier la faisabilité des principes établis. Nous avons développé tout au long de nos travaux des démonstrateurs ponctuels dans l'objectif de proposer un cadre concret à l'application et tester nos propositions.
En final de cette étape importante d'analyse du filtrage des documents client, les investigations que nous avons menées sur les outils nous ont assurés de l'applicabilité des principes que nous proposions. L'étape Filtrage est primordiale puisqu'elle permet de créer le lien entre le client et le fournisseur en identifiant les besoins du client qu'il faudra prendre en compte. En sortie de l'étape Filtrage, les exigences SdF client sont identifiées dans le CdC.

3.2.2. Etape Traduction

Cette étape est destinée à caractériser une interface de conversion permettant d'étudier les exigences du client dans un format propre à l'entreprise et conforme à ses habitudes. Les traductions effectuées seront donc de différents types mais devront être réversibles pour permettre de revenir aux termes employés par le client dans le dossier de réponse à l'appel d'offre.
Dans les types de traductions envisagées, nous considérons :

- l'adaptation de vocabulaire par le biais de tables de correspondances ou d'ontologies du domaine (il se peut que pour un concept particulier chaque client ait une expression propre),
- la conversion d'unité pour les exigences de performance,
- la reformulation d'exigences.

Si le vocabulaire utilisé dans l'ensemble des entreprises du secteur automobile est globalement unifié, lorsqu'on s'intéresse aux évènements redoutés[9] qui sont les évènements relatifs à la sécurité du produit, ceux-ci peuvent être exprimés en termes :

- d'évènements redoutés ou évènement redoutés client,
- d'événements indésirables ou d'évènements indésirables client ou évènements indésirés,
- d'événements inacceptables,...,

et revêtir des formes très variables.
A ce sujet, dans [Mazouni&al, 08], les auteurs font le constat que les termes de la sûreté de fonctionnement sont souvent mal utilisés par les industriels :

- utilisation de plusieurs termes pour le même concept et inversement,
- aléas dus à la traduction français/anglais (exemple classique de la sécurité qui peut apparaître sous la forme safety ou security),...

Cela pose le problème de l'identification des différents termes relatifs à chaque concept de la SdF. Ces termes peuvent être obtenus par le biais d'une ontologie du domaine de la SdF ou d'une étude de l'ensemble des documents client afin

[9] Les évènements redoutés sont décrits dans le chapitre 4.

d'extraire les termes relatifs à la SdF dans les CdC. Cela est réalisable, par exemple, à partir de l'utilisation d'ontologie du risque [Mercantini, 08], [Assali&al, 08] ou de différents logiciels spécialisés tel que "Protegé[10]", " SWOOP[11]". On peut aussi envisager d'utiliser les outils de Text-Mining sur un corpus assez important de documents ayant trait à la SdF pour définir les termes employés.

L'étape Traduction apporte, en plus de ces fonctionnalités, des possibilités d'interopérabilité dans la mesure où elle permet l'adaptation entre les éléments issus du filtrage (côté client) et le vocabulaire courant de l'entreprise (s'appuyant sur l'expertise interne). Dans cette mesure, toute entreprise utilisant un vocabulaire particulier pourra le conserver grâce à ce type de traducteur.

On obtient, en sortie, l'ensemble des exigences clients dans un format directement exploitable par les étapes aval.

Afin d'identifier les besoins pour cette étape Traduction, nous avons réalisé une série de tests sur les CdC disponibles au sein de l'entreprise partenaire. Deux types de tests ont été effectués : des tests manuels (recherche dans les CdC d'éléments relatifs à la SdF) et des tests de recherche semi-automatique pour rechercher les différentes déclinaisons de certains termes. L'analyse des recherches effectuées met en relief les différentes déclinaisons de chaque concept SdF. Une analyse plus fouillée sur un échantillon plus important que celui utilisé dans nos tests, permettrait d'établir des fiches de traduction correspondant aux différentes déclinaisons des termes relatifs à la SdF.

Nous proposons sur la Figure II-9 une illustration de la diversité de termes pouvant être observée sur un concept particulier. L'exemple proposé concerne la classification des termes employés autour de la notion de danger à laquelle s'est intéressé l'auteur dans [Beugin, 06].

<table>
<tr><td colspan="2">1. Evénement source</td><td>-Événement initiateur
-Événement d'origine
-Événement déclencheur
-Événement dangereux</td></tr>
<tr><td rowspan="2">2. Danger (état de danger)</td><td>interne</td><td>-Situation dangereuse (du système)
-Activité dangereuse
-Nuisance</td></tr>
<tr><td>externe</td><td>-Situation dangereuse (de l'environnement)
-Phénomènes dangereux
-Menace, situation mnaçante
-Comportement dévié
-Agression externe</td></tr>
<tr><td colspan="2">3. Evénement résultant</td><td>-Événement redouté
-Événement potentiellement redouté
-Événement indésiré
-Événement inacceptable
-Accident</td></tr>
<tr><td colspan="2">4. Etat résultant</td><td>-Dommage
-Conséquence néfaste
-Effet redouté
-Préjudice</td></tr>
</table>

Figure II-9 : Termes relatifs à la notion de danger issu de [Beugin, 06]

[10] http://protege.stanford.edu/

[11] http://code.google.com/p/swoop/

Cet exemple orienté sécurité d'un produit montre l'étendue des termes employés pour les différents éléments caractéristiques du danger.

3.2.3. Etape Projection

L'objectif de la projection est d'analyser l'impact des exigences SdF au niveau du produit (résultat) et de la démarche à mettre en place (allocation, vérification et validation). Pour réaliser cette analyse, il faut identifier, dans le cycle de vie du produit, les éléments ayant trait à la SdF pour définir ce qui doit être réalisé durant le PRAO et ce qui est à prévoir dans le développement futur ainsi que les modèles nécessaires pour la mise en place de la démarche dans le PRAO. Nous illustrons sur le schéma de la Figure II-10 l'ensemble des principes de la projection que nous développerons ensuite.

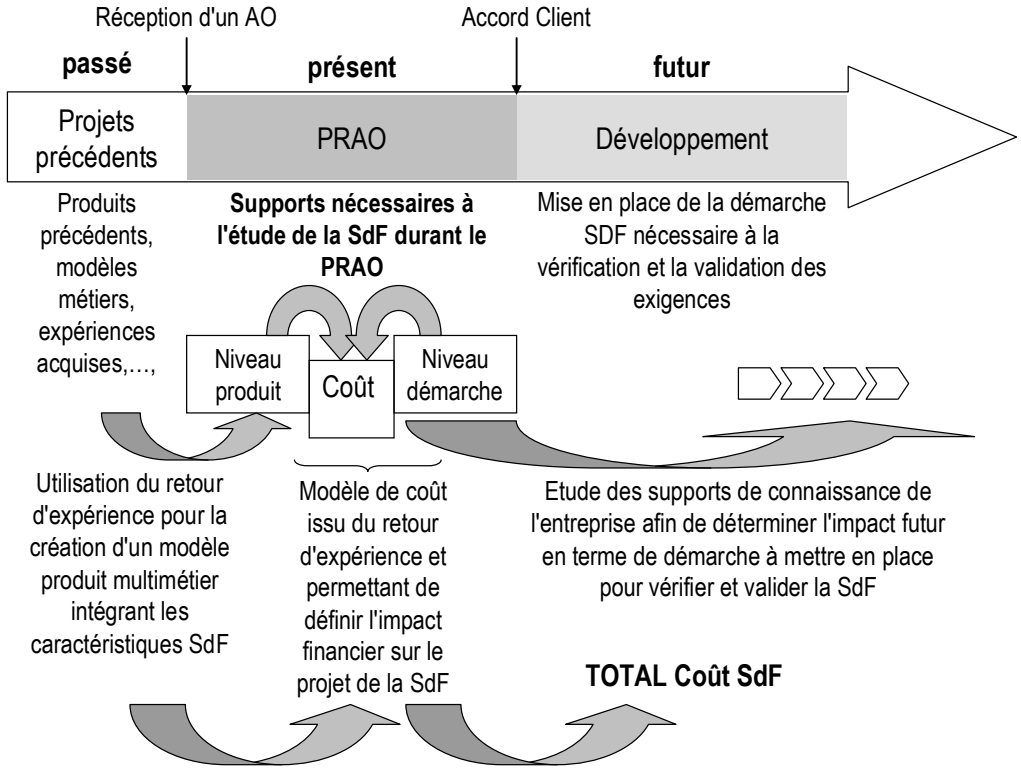


Figure II-10 : Principes de la projection et connaissances associées

Nous retrouvons sur la Figure II-10 les trois horizons de temps impliqués dans l'étape Projection : le passé par l'utilisation des connaissances sur les projets précédents, le présent pour la définition de l'impact des exigences SdF à un instant t dans le PRAO et, enfin, le futur sur lequel il faudra prévoir les actions à engager pour un traitement efficace de la SdF. Nous mettons aussi l'accent sur les supports nécessaires à l'instrumentation de la projection au niveau modèle produit pour l'étude de la SdF dans le PRAO, au niveau modèle de coût pour l'estimation de l'impact financier du traitement des exigences SdF et, enfin, au niveau modèle démarche pour la définition des activités qui devront être engagées dans un développement futur.

Concernant les supports nécessaires, nous avons identifié au sein de l'entreprise partenaire les éléments déjà disponibles et utilisables tels quels ou à adapter. L'état des lieux préliminaire présenté au chapitre 1 a permis de mettre en évidence les éléments relatifs à la SdF bien maitrisés par l'entreprise partenaire, notamment, la panoplie des outils et méthodes identifiée comme complète mais engagée uniquement dans les phases de développement (et non dans le

PRAO). Dans cette panoplie, notons l'existence de procédures relatives à l'engagement d'une démarche SdF complète comportant une panoplie de méthodes et outils quasi-complète (pour les phases de développement du produit, pas d'engagement dans le PRAO initialement) dont le manque résidait dans la définition de la finalité des différentes méthodes et de leur chainage. Cette panoplie est la base que nous avons utilisée afin de définir et d'améliorer la démarche en place. Le principal constat concernant la démarche SdF est le manque de visibilité des objectifs, intrants et extrants de chaque méthode. Dans ce contexte, nous proposons l'analyse de différents travaux sur les méthodes SdF et une démarche chainée de différentes méthodes. Cette démarche est présentée avec les informations de sorties de chaque méthode qui seront utilisées dans celle qui suit.

La réalisation de la SdF permettant d'analyser, vérifier et valider les exigences SdF est assurée par l'engagement séquentiel ou combiné de méthodes SdF organisées dans une démarche d'analyse, générale ou propre à l'entreprise, orientée autour des axes fonctionnel et dysfonctionnel, matérialisant un processus devenu classique en maîtrise des risques [Noyes&al, 07].

D'après l'auteur, dans [Mortureux, 01], il n'existe pas de règle qui définisse la méthode idéale ; ce sont les caractéristiques des méthodes qui justifient leur emploi. Nous nous sommes intéressés aux différentes descriptions liant la SdF à un cycle de développement de produit. Dans [Mallard, 07], l'auteur propose un schéma d'organisation en faisant apparaître les différentes activités SdF en fonction des phases du cycle de vie. Nous en faisons une adaptation simplifiée sur la Figure II-11.

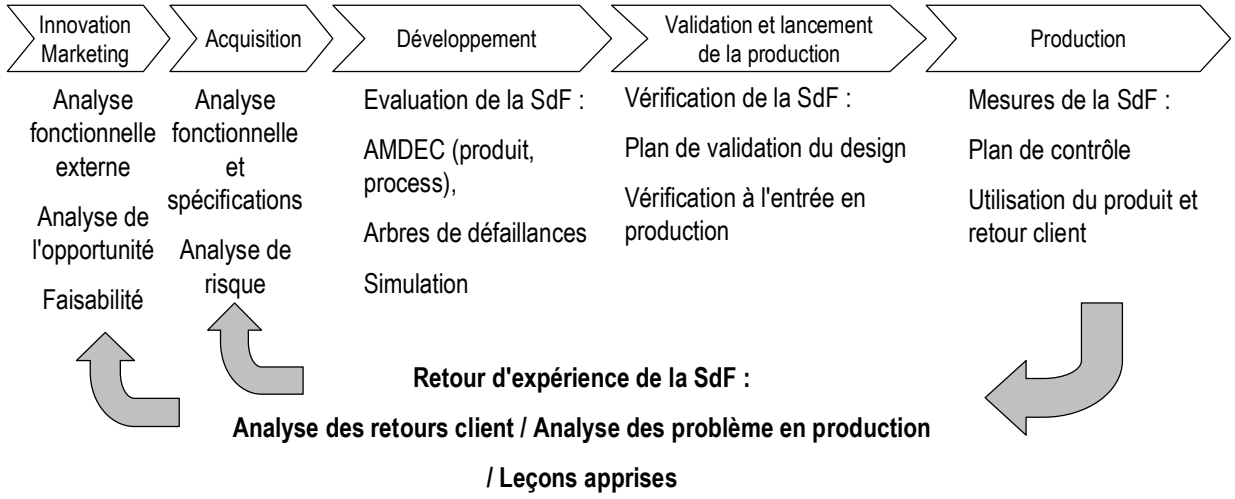


Figure II-11 : Eléments relatifs à la SdF dans le cycle de vie

Cette figure permet de situer les principales méthodes SdF rencontrées fréquemment en milieu industriel dans le cycle de vie du produit (cycle de vie composé ici de cinq phases). Elle met aussi en évidence le fait que l'évaluation de la SdF est généralement réalisée dans les phases de développement et que les phases amont ont seulement, d'un point de vue SdF, un objectif d'identification des risques.

Dans [Noyes&al, 07], les auteurs proposent la formalisation d'une démarche SdF en différentes étapes (Figure II-12) pour lesquelles les méthodes utilisables sont présentées au niveau de chaque étape.

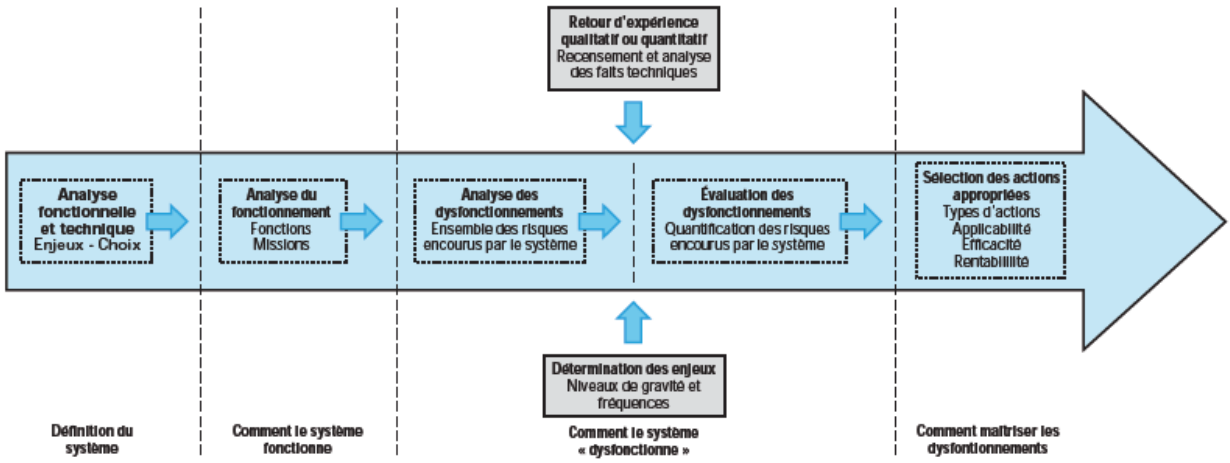


Figure II-12 : Démarche d'analyse de la Sdf d'après [Noyes&al, 07]

Nous allons maintenant nous intéresser à la définition d'une démarche SdF afin de pouvoir établir par la suite les activités qui devront être réalisées durant le développement.

Pour définir cette démarche, nous nous appuyons sur les travaux présentés précédemment ainsi que sur les travaux plus particulièrement appliqués dans des contextes industriels afin de pouvoir dresser un état des méthodes [IMDR_SdF_07] les plus utilisées dans l'industrie.

Nous insisterons à chaque étape sur les informations de sortie fournies par chaque méthode afin d'assurer la cohérence de la démarche. Nous considérons en effet que l'efficacité de la démarche repose aussi sur une bonne utilisation des informations entre les différentes méthodes et que la fluidité d'une démarche facilite son emploi car les acteurs ont, à chaque instant, conscience que la réalisation rigoureuse de la méthode permettra de faciliter l'analyse suivante.

L'ensemble des travaux sur la SdF sont unanimes sur le fait que la phase préalable à toute analyse SdF est la réalisation d'une analyse fonctionnelle [Demri&al, 07a], [Noyes&al, 07] afin de bien cerner les besoins, l'environnement du produit et ses fonctionnalités. Cette analyse fonctionnelle est décomposée dans certains travaux en une analyse fonctionnelle externe (AFE) suivie d'une analyse fonctionnelle interne (AFI) [Medjoudj, 06]. L'AFE a pour objectif de définir les limites du système ainsi que la définition des fonctions de services (ce pour quoi le système est conçu) et les fonctions contraintes (matérialisant l'intégration du système dans son environnement). L'AFI a pour but de raffiner les fonctions définies dans l'AFE afin d'atteindre un niveau de détail suffisant pour la définition des solutions techniques.

Les méthodes utilisables pour la réalisation de ces études sont variées (APTE[12], IDEFØ[13], RESEAU,...,). En sortie de l'analyse fonctionnelle, nous disposons de l'ensemble des fonctions reliées à leurs supports matériels, ce qui permettra dans les étapes d'analyse suivantes de pouvoir identifier, pour un mode de défaillance particulier, les causes et les effets de cette défaillance.

L'étape suivante consiste à identifier les risques ; pour cela plusieurs méthodes peuvent être engagées, l'analyse préliminaire des risques (APR) étant la plus courante. L'APR consiste à identifier les points du système qui peuvent être

[12] Méthode APTE : http://www.methode-apte.com/methode_apte.htm

[13] Méthode IDEFØ : http://www.idef.com/IDEF0.html

critiques en terme de sécurité, à évaluer les risques correspondants, les scénarios associés et à définir des critères de conception à respecter (critères qui serviront à l'étude plus poussée réalisée par la suite).

Enfin, pour l'étude des défaillances d'un système, l'analyse des modes de défaillances, de leurs effets et de leur criticité (AMDEC) est une méthode très répandue dans l'industrie [Wagner, 07], [VEMS, 05]. L'AMDEC a pour objectif, dans une démarche inductive rigoureuse, d'identifier les défaillances dont les conséquences peuvent affecter le fonctionnement d'un système et de les hiérarchiser selon leur niveau de criticité afin de les maîtriser. On obtient en sortie l'ensemble des dysfonctionnements potentiels associés à leur criticité (fréquence d'apparition, gravité des effets et probabilité de détection de la défaillance) ainsi que les plans d'actions à mettre en œuvre afin de diminuer la criticité en faisant varier un des trois facteurs.

On peut compléter cette démarche, notamment pour la gestion de l'aspect sécurité, par l'utilisation des arbres de défaillances (AdD) qui permettront pour un évènement donné, d'étudier les combinaisons de défaillances pouvant conduire à cet évènement. On obtient en sortie les scénarios de défaillances menant à l'événement dans le cas d'une étude qualitative et la fréquence d'apparition de l'évènement dans le cas d'une étude quantitative. Un des objectifs est d'étudier ce type de graphes par les coupes minimales qui ont pour vocation de vérifier le nombre de défaillances élémentaires induisant l'apparition de l'évènement.

Concernant le chaînage des outils, dans [Gouriveau, 03], l'auteur s'est intéressé à cet aspect en proposant pour une méthode donnée, les méthodes compatibles. Il part pour cela d'un ensemble de chaînages possibles puis il crée des fiches pour chaque méthode intégrant les méthodes compatibles à celle considérée. On trouve par exemple le chaînage présenté sur la Figure II-13. Les abréviations utilisées correspondent à : Graphes de Markov (GM), Hazard and Operability studies (HAZOP), Méthode de l'Arbre des Conséquences (MACQ) et Méthode l'Arbre de Fautes (MAF).

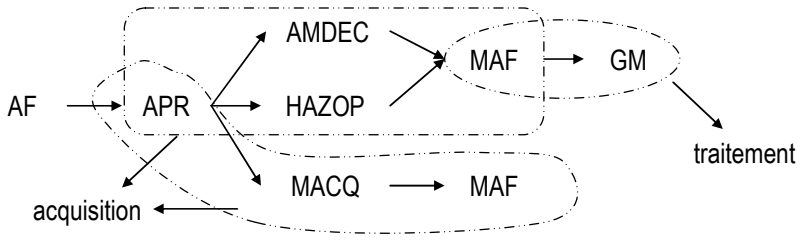


Figure II-13 : Chaînage de méthodes de SdF issu de [Gouriveau, 03]

Dans cette organisation générale, le choix des méthodes reste fonction de l'objectif visé, on peut envisager un autre chaînage tant que la cohérence d'ensemble est assurée. Nous proposons un schéma récapitulatif de la démarche proposée intégrant les liens entre les outils.

Sur la Figure II-14, le chaînage proposé permet d'illustrer la progression de la connaissance dans l'étude de la SdF. Les premières étapes AFE et AFI permettent la compréhension du produit complet, de ses fonctionnalités et de leurs supports. L'APR a pour objectif d'identifier ensuite les principaux ER à traiter et leurs causes à un niveau macroscopique. L'AMDEC et l'AdD ont un rôle d'analyse détaillée des ER ainsi que des défaillances du produit afin de s'assurer du respect des exigences SdF. Bien sûr, l'exhaustivité dans l'analyse de la SdF dépendra directement du niveau de connaissance sur le produit et de son état d'avancement (concept défini, solutions définies, solutions figées,...,).

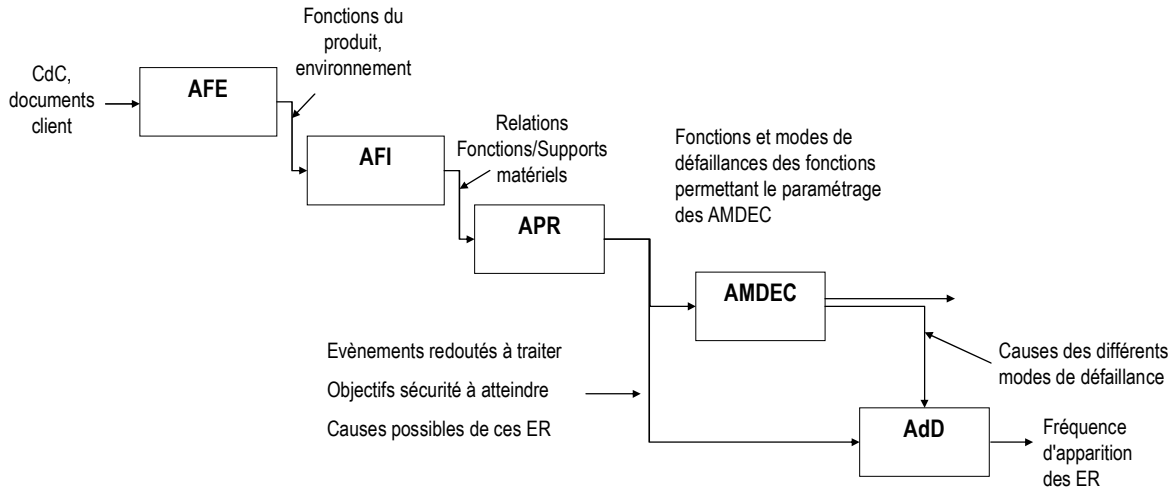


Figure II-14 : Chaînage des méthodes pour une démarche SdF

Une question importante concernant l'étude de la SdF au niveau du PRAO est : pourquoi ne pas utiliser une méthodologie SdF existante en l'adaptant pour le PRAO ?

Cette question a été, bien sûr, considérée dans le cadre de nos développements mais plusieurs constats rendent difficilement réalisables cette solution :

- la durée du PRAO ne permet pas d'investigation fouillée au regard de la durée disponible mais plutôt une pré-étude des caractéristiques SdF,
- le niveau de définition du produit dans le PRAO nécessite un haut-niveau d'abstraction,
- les modèles utilisés dans les méthodologies SdF classiques ne correspondent pas à des "standards" connus de tous les acteurs projet ou acquisition alors que nous souhaitons disposer d'un modèle intelligible par tous (les modèles académiques sont souvent peu exploités et difficilement utilisables en entreprise [Scaravetti, 04]). C'est pour cette raison que nous avons exprimé sur la Figure II-10 le besoin de modèle produit multimétier intégrant les caractéristiques SdF,
- l'objectif visé est d'estimer l'impact des exigences SdF sur la base des principaux mécanismes de défaillances et des évènements redoutés et non l'étude exhaustive de ceux-ci.

L'étape Projection dispose en entrée des exigences à traiter (traduites) et a trois objectifs :

1) permettre, durant le PRAO, la réalisation d'études pour affiner ou compléter une exigence particulière, non analysable en l'état (utilisation des méthodes et outils des phases de développement (analyse préliminaire des risques, AMDEC,...) adaptés à des études rapides) à l'aide des modèles produit développés que nous présentons dans le chapitre 3,

2) propager sur le produit l'impact de la prise en compte des exigences SdF par l'utilisation des supports de connaissance existants ou développés, notamment, en termes de choix de solutions,

3) définir l'impact sur le développement futur de la vérification et de la validation de ces exigences par une démarche SdF complète et à appliquer.

Les supports représentent la connaissance et les modèles disponibles dans l'entreprise. Ils permettront d'assister l'analyse de l'impact SdF. Ces supports seront décrits succinctement dans le paragraphe 4 puis plus en détail dans le chapitre 3.

Les résultats fournis seront de plusieurs types en sortie de l'étape Projection : identification de modes d'actions, définition d'études à réaliser obligatoirement en développement, expression de contraintes sur le produit, choix de principes, caractérisation de tests,...

3.2.4. Etape Evaluation

L'étape Evaluation a pour but de dimensionner, en termes "d'effort" et de coût, les éléments identifiés par la projection pour estimer la charge de travail qu'induira la prise en compte et la satisfaction des exigences SdF. Deux niveaux de résultats sont visés :

1) le dimensionnement de l'ingénierie nécessaire aux actions SdF spécifiques (AMDEC, calculs,...) via les ressources afférentes et les durées estimées,
2) la cotation économique de ces actions et celle des solutions identifiées dans les choix de principe.

Cette étape apporte une information technique supplémentaire qui aidera à évaluer la faisabilité du projet en caractérisant :

- le coût d'obtention de la solution satisfaisant les critères du CdC,
- le délai nécessaire à sa réalisation,
- les performances envisagées pour le produit.

Les modes de calcul et les hypothèses retenues (en cas d'absence d'information correspondante dans le CdC) doivent être explicitement formulés afin d'éviter toute interprétation erronée par la personne en charge du dépouillement de la réponse à l'AO.

Le coût du produit, au cours de son cycle de vie, a été largement traité dans la littérature. Le premier constat émanant de ces études est l'importance des premières phases dans lesquelles sont fixés les principaux coûts constitutifs du coût produit. De nombreuses représentations existent reliant le coût à l'avancement d'un projet ; nous proposons une illustration sur la Figure II-15 issue de [Gautier&al, 00] que nous avons sélectionnée pour son niveau de détail élevé (visualisation notamment de la phase de faisabilité).

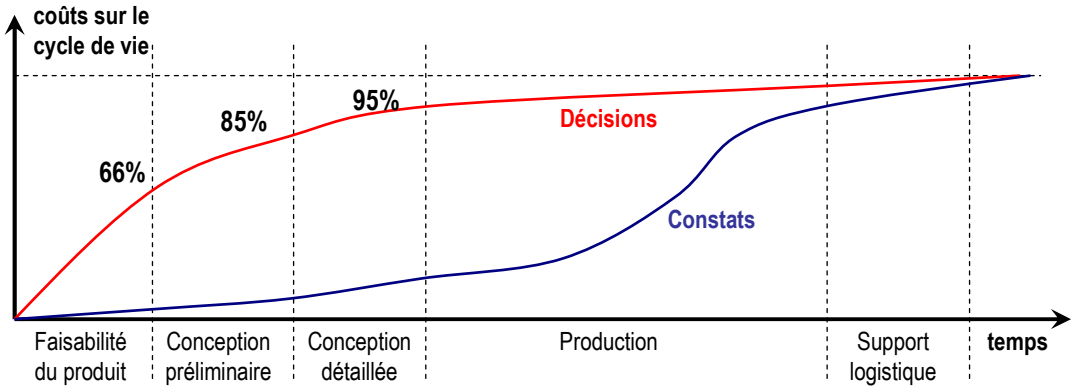


Figure II-15 : Evolution des coûts sur le cycle de vie

Ce graphique montre bien que les décisions prises durant les premières phases conditionnent entre 70% et 80% du coût du produit.

Dans un contexte industriel fortement concurrentiel, le coût est un élément primordial car il est nécessaire pour l'entreprise de connaître dès la conception le prix maximum de vente d'un produit par rapport au marché pour lequel il

est destiné [Lonchampt, 04]. Cela est encore plus vrai dans le milieu automobile et au niveau des situations qui nous intéressent. D'une part, la proposition initiale de prix est fournie au client dès la réponse à appel d'offre (cette estimation doit être la plus précise possible puisqu'elle constitue un premier engagement de la part du fournisseur) et, d'autre part, l'augmentation du nombre de calculateurs dans le véhicule (quelques unités il y a quelques années mais plusieurs dizaines aujourd'hui) rend indispensable le contrôle du coût de chaque système pour conserver un coût global acceptable pour le véhicule.

Il existe différentes méthodes d'estimation des coûts :

- les méthodes analogiques : ces méthodes sont basées sur le fait que "deux produits ayant des fonctionnalités similaires ont des coûts similaires" [Lonchampt, 04] ; ces méthodes sont utilisables dans le cas où les produits développés sont limités en diversité. L'avantage principal de ces méthodes réside dans le fait qu'elles fournissent des résultats assez fiables (si elles sont appliquées avec rigueur) à faible coût [Perry, 07] ; leur inconvénient est qu'elles nécessitent des informations formalisées concernant les coûts des produits précédents ou un savoir-faire d'expert (qui peut être subjectif). Ces méthodes sont tout de même assez bien adaptées aux phases amont du cycle de vie [Lonchampt, 04] et, plus particulièrement, à l'estimation des coûts de l'électronique, ce qui correspond en partie aux situations qui nous intéressent,
- les méthodes paramétriques : ces méthodes sont basées sur les relations qui existent entre des paramètres physiques ou de performance du produit (volume, surface,...) et des paramètres de coût (euros, taux horaires,...,) [HMida&al, 07]. La pertinence du résultat obtenu est directement liée aux relations définies (propres à un domaine particulier). Dans notre application, ces méthodes semblent adaptées à l'estimation du coût mécanique du produit par analogie aux applications du bâtiment, domaine dans lequel le coût d'un bâtiment peut être estimé en fonction de sa surface au sol et de sa hauteur [Lonchampt, 04]. Dans le cas mécanique, la relation serait basée sur le prix de la matière et les dimensions du produit.
- les méthodes analytiques : ces méthodes considèrent que le coût du produit peut être assimilé à celui des opérations nécessaires à son obtention, ce qui consiste "à décrire précisément les processus avals et à recenser les sources de coûts intervenant lors de leur déroulement" [Lonchampt, 04]. Les estimations, dans ce cas là, sont basées sur l'équation : "Coût de l'opération = Temps x Taux horaire" [HMida&al, 07]. Dans notre cas, cette méthode paraît applicable au traitement du logiciel en disposant à l'avance du temps de codage en fonction de la complexité du produit ou du nombre de modules.

Ces différentes approches considèrent le coût global du produit mais dans notre cas, ce n'est pas la totalité du coût du produit qui nous intéresse mais le coût SdF. Celui-ci peut être décomposé en deux postes de dépenses :

- les coûts des solutions SdF sur le produit,
- les coûts de la démarche à mettre en place pour gérer la SdF et établir ces solutions.

Le coût SdF sur le produit peut être vu comme le surcoût lié à la fiabilisation et à la sécurisation du produit. Cela entraîne la nécessité de définir le coût de base de la solution hors SdF (la solution fonctionnelle) et de calculer le surcoût engendré par l'introduction de solution SdF :

$Coût_{SdF\_Produit}$ = (Coût solution définie) – (Coût de la solution fonctionnelle)

Pour ce qui est du coût de la charge de travail, la méthode analytique est tout à fait adaptée, on a alors :

$Coût_{SdF\_Demarche}$ = (durée des études) x (nombre de ressources) x (coût horaire)

On obtient le coût total de la SdF par :

$Coût_{SDF} = Coût_{SdF\_Produit} + Coût_{SdF\_Demarche}$

Dans l'entreprise partenaire, les coûts sont estimés, pour le produit, à partir du retour d'expérience. Les principaux coûts sont relatifs à :

- l'électronique : le coût est estimé à partir des composants constituant le produit, l'entreprise a développé un utilitaire basé sur des modules fonctionnels existants. Chaque module est décrit par les composants qui le constituent (chacun étant lié à un coût unitaire récupéré dans les bases commerciales de l'entreprise). Pour le chiffrage d'un nouveau produit, l'analyste sélectionne les modules fonctionnels dont il a besoin et l'outil (tableur excel) fournit le prix total en fonction de ses choix,
- la mécanique : l'estimation est réalisée à partir d'une estimation de la surface de la carte électronique qui devra être conditionnée. Une fois cette surface définie, l'analyste calcule alors la quantité de matière ainsi que le matériau le plus adapté pour le produit considéré,
- le logiciel : le coût est estimé par rapport au nombre de modules logiciels à implémenter et s'appuie sur une estimation de la durée de codage en fonction du nombre prévisionnel de lignes.

Pour l'évaluation des coûts relatifs à la charge de travail, plusieurs supports seront utilisés. L'objectif est de définir la durée et les ressources nécessaires à la réalisation des études SdF durant le développement mais aussi durant le PRAO pour les études préliminaires.

Lorsque l'étape Evaluation est terminée, on dispose de l'ensemble des activités liées à la SdF, de l'ensemble des coûts associés ainsi que d'un suivi des réflexions menées pour les obtenir ; on peut alors aborder l'étape Restitution.

3.2.5. Etape Restitution

L'étape Restitution permet d'établir sous forme synthétique :

- les solutions techniques retenues pour satisfaire aux critères du cahier des charges,
- les éléments issus de l'évaluation.

Elle a aussi deux finalités :

1) la fourniture d'un état chiffré de la gestion de la SdF dans le projet (état qui pourra être intégré au dossier de réponse à l'AO après révision par l'équipe d'acquisition),

2) l'affichage, dans une forme accessible au client, des dispositions qui seront prises pour atteindre les résultats SdF requis pour permettre à ce client de s'assurer des garanties d'action.

Cette étape est une étape clé au niveau de la réponse à appel d'offre puisqu'elle vise à montrer au client la façon dont sont prises en compte ses exigences dès le premier contact. En effet, les constructeurs sont de plus en plus exigeants envers la gestion de la SdF par leurs fournisseurs. Dans [Bracquemond, 07], l'auteur présente les exigences d'un constructeur vis à vis de la SdF parmi lesquelles, on trouve notamment : l'affichage de la capacité à maitriser les risques, la mise à disposition des informations relatives à cette maîtrise (contrainte, exigences de sécurité) et la justification de la tenue des exigences.

L'instrumentation de cette étape passe par la définition d'un standard de compte-rendu ne contenant que les informations qu'on souhaite fournir au client.

L'idée principale est de consigner l'ensemble des conclusions des analyses réalisées durant les quatre étapes précédentes, i.e. :

- les exigences à traiter et les éléments relatifs à la SdF identifiés durant le filtrage,
- les traductions ou conversions effectuées afin de pouvoir répondre au client en utilisant son vocabulaire,
- les conclusions de la projection : impact SdF sur le produit, traitement des évènements redoutés, identification des principaux mécanismes de défaillances,
- l'estimation du coût sur le plan produit et démarche.

Pour l'entreprise, l'objectif est de capitaliser un maximum d'informations afin d'améliorer les réponses pour les AO suivants et faciliter l'analyse des exigences SdF. Cependant, l'entreprise, dans l'objectif de conserver son savoir-faire, ne proposera pas au client ce bilan détaillé mais plutôt un bilan ou un résumé en fonction de la demande du client. Les éléments qui figureront dans le dossier SdF destiné au client pourront être :

- la démarche de traitement des ER du client que l'entreprise mettra en place,
- les ressources affectées aux analyses SdF,
- la démonstration, dès le PRAO, de la prise en compte des principaux mécanismes de défaillance,
- la durée, non détaillée, des analyses SdF tout au long du cycle de développement.

Dans le paragraphe suivant, nous dressons un bilan des différents modèles et supports de connaissances existants sur lesquels s'appuiera la démarche proposée. Nous proposons ensuite un classement de ces supports en quatre familles correspondant aux objectifs visés.

4. Supports d'instrumentation

Nous avons insisté, tout au long des développements, sur l'importance de définir une méthodologie s'intégrant au contexte plutôt que d'adapter l'existant pour la méthodologie proposée. Pour rendre cette approche possible et applicable à un autre contexte, il est nécessaire d'identifier, dans le cas général, les supports de connaissance disponibles dans une entreprise. Les connaissances disponibles formalisées sont généralement regroupées dans les champs "Mémoire d'entreprise ou de projet" et "gestion des connaissances" qui sont généralement définis dans le cadre de la mise en place des processus de retour d'expérience. Dans notre application, l'utilisation des connaissances disponibles est primordiale dans la mesure où le produit n'existe pas encore et qu'il faut identifier les développements futurs. Le schéma illustratif de l'étape Projection (Figure II-10) comporte bien les boucles de retour d'expérience nécessaires à l'instrumentation de la solution.

En reprenant le schéma de la Figure II-1, il nous faut maintenant détailler le plan supports d'instrumentation qui correspond à la connaissance disponible ou à créer.

Nous dressons d'abord un état des ressources supports de connaissances disponibles dans une entreprise et nous intéressons ensuite aux supports généralement considérés dans un système de retour d'expérience. Nous proposons une classification de ces différents supports dans le cadre de l'application considérée.

Différents types de ressources supports de connaissances peuvent être disponibles au sein d'une entreprise [Dieng, 00]

(Figure II-16) :

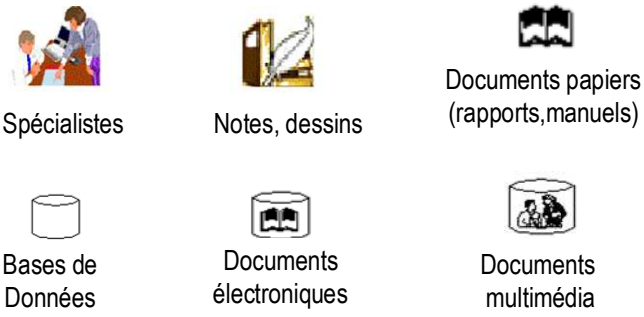


Figure II-16 : Ressources de connaissances

L'ensemble des ressources matérielles peut être exploité facilement en fonction du degré de formalisation des contenus. La connaissance possédée par les spécialistes ou les experts est plus difficile à expliciter et dépend des facultés de ces derniers à la retranscrire.

Chaque type de ressource peut être considéré pour chacun des métiers de l'entreprise. Dans le cadre d'un produit mécatronique, sont à considérer la mécanique, l'électronique, le logiciel, la qualité, la gestion de projet, la production, la comptabilité,... Cela peut induire un nombre très important de supports disponibles. Nous n'avons pas l'ambition de caractériser pour chaque métier les ressources dont il dispose mais plutôt d'organiser ces supports en catégories indépendamment du métier considéré.

Lorsqu'on souhaite mettre en place un système de retour d'expérience en général ou utiliser, comme dans notre cas, le retour d'expérience en support de solution, quatre composantes essentielles sont à considérer [Geneste&al, 06], [Rakoto&al, 04] :

- une composante "processus et activités" qui consiste en la description des processus d'alimentation du Rex et les processus d'exploitation du Rex,
- une composante "informations et connaissances" qui définit les standards et règles pour la capitalisation de l'expérience,
- une composante "acteurs et compétences" qui permet l'adaptation des mécanismes d'ajout et de recherche d'expériences dans le Rex en fonction du profil de l'utilisateur,
- une composante "techniques et outils" consacrée aux moyens permettant l'instrumentation du retour d'expérience.

Par comparaison à notre problématique, il apparait que l'organisation du PRAO proposée est assimilable à la composante : "processus et activités", l'instrumentation des différentes étapes de cette organisation à la composante "techniques et outils". La composante "acteurs et compétences" sera indirectement prise en compte dans le chapitre 3 par la définition d'un modèle permettant à tout acteur (quel que soit son domaine d'expertise) de comprendre le modèle. Enfin, la composante "informations et connaissances" est décrite ci-après par la présentation des types de connaissances disponibles dans un cadre entreprise ou projet.

Afin de définir cette composante, nous nous sommes intéressés à la constitution d'une mémoire projet, celle-ci pouvant être définie comme une mémoire des connaissances et des informations acquises et produites au cours de la réalisation des projets [Ribiere&al, 99]. Dans ces travaux, les auteurs décrivent l'ensemble des sources d'informations qui peuvent alimenter une mémoire de projet.

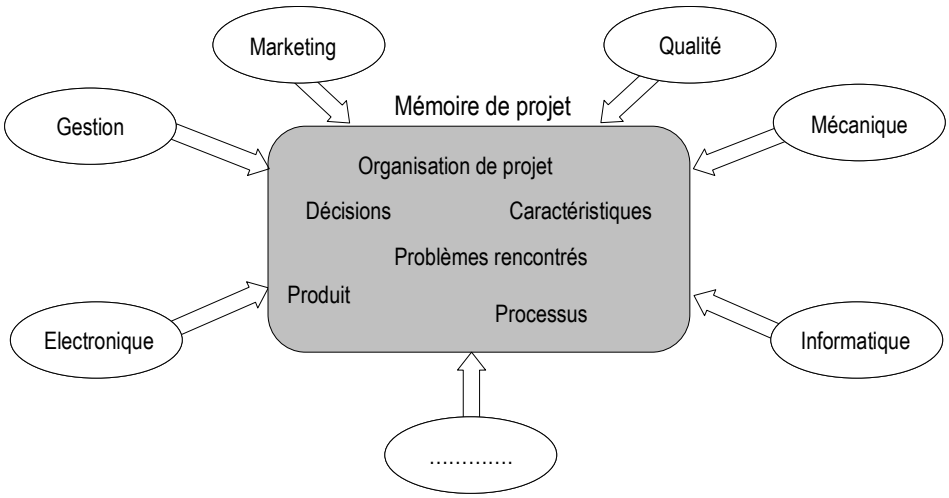


Figure II-17 : Sources d'informations pour une mémoire de projet [Ribiere&al, 99]

Appliquons cet inventaire des différentes sources d'informations au cadre de la SdF. L'objectif visé par l'utilisation des supports est l'évaluation de l'impact SdF au niveau du produit et de la démarche à mettre en place. Il faut identifier tous les éléments relatifs à la SdF disponibles ainsi que tous les éléments non directement liés à la SdF mais qu'il est nécessaire de connaître.

Jusque-là, nous avons identifié :

- la démarche SdF qui est un processus de l'entreprise,
- les caractéristiques SdF du produit issues des connaissances métier.

D'autres connaissances sont à appréhender pour la mise en place de la démarche. Nous proposons sur la Figure II-18 un schéma récapitulatif de la connaissance à formaliser.

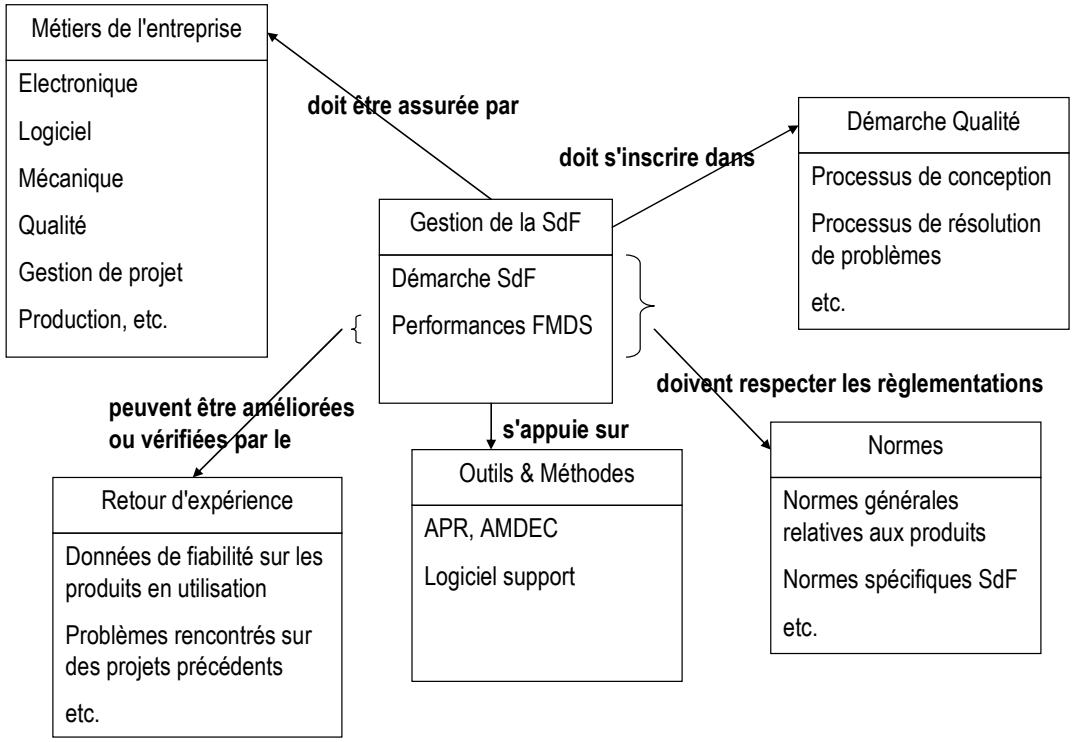


Figure II-18 : Gestion de la SdF et connaissances utilisées

A partir de cette cartographie sur la connaissance nécessaire à la gestion SdF, nous avons établi une classification des différents supports de connaissances que nous présentons en définissant les connaissances introduites précédemment

et intégrées à chaque type de support :

- les supports normatifs S_N, relatifs aux préconisations à respecter au niveau du produit, des analyses, des essais et des validations. Nous intégrons à cette catégorie les normes relatives au produit et à la SdF : citons parmi celles relatives au contexte, la norme de sécurité fonctionnelle du produit IEC 61508 et la norme ISO 26262 (déclinaison pour le contexte automobile, à paraître), les normes relatives aux émissions électromagnétiques du produit,..,.
- les supports procéduriers S_P, éléments extraits des procédures en vigueur sur la conduite de projet, le cycle de développement et les procédures SdF : date de livraison d'un document particulier, étape du projet, gestion des exigences, démarche imposée dans une situation donnée (criticité du projet, d'une technologie,...). Cette catégorie de support intègre l'ensemble des documents relatifs à la démarche qualité ainsi que les outils et méthodes de la SdF,
- les supports métiers S_M, liés à l'expertise de l'entreprise : règles métiers (sur le choix d'élément, l'organisation d'une fonction,...) et utilitaires métiers (calcul du "worst-case" d'une fonction,...). On trouve dans cette catégorie, l'ensemble des connaissances de chaque métier quelle que soit leur finalité (estimation d'un coût, vérification d'une propriété SdF ou non SdF),
- les supports de retour d'expériences S_E, liés à l'expérience acquise dans la résolution de problèmes déjà rencontrés (causes, conséquences, solution). Cette catégorie inclut toute la connaissance issue des projets précédents[14].

Cette classification même si elle découle de l'état des lieux préliminaire dans l'entreprise partenaire est assez générique. Ces quatre familles de supports peuvent facilement être généralisées à un autre contexte dans la mesure où toute entreprise possède un système de management de la qualité dans lequel on trouvera les supports procéduriers, les supports normatifs seront fonction des règlementations applicables dans ce nouveau contexte. Les deux autres familles de supports trouveront aussi un équivalent dans un autre contexte : les supports métiers concernent le savoir-faire explicite d'une entreprise qu'il soit mono ou multimétier et les supports de retour d'expérience concernent l'ensemble de la connaissance acquise sur des projets précédents. Nous complétons la solution d'organisation du PRAO par les liens avec les supports de connaissance que nous venons d'identifier (Figure II-19)

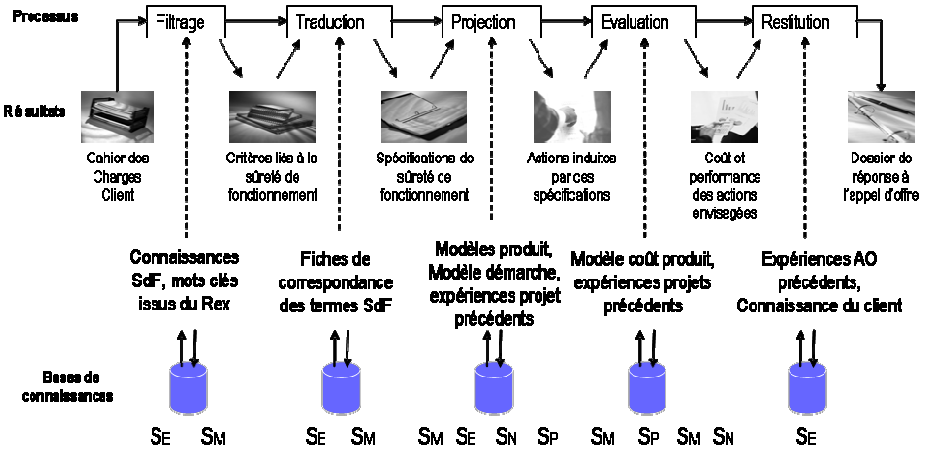


Figure II-19 : Lien entre les étapes et les supports de connaissance

[14] Bien qu'il existe certaines similitudes entre les deux types de supports S_M et S_E, nous distinguons ceux-ci eu égard aux formalismes propres à chacun. Le retour d'expérience est généralement capitalisé sous forme de base de données ce qui n'est pas le cas pour les supports métiers.

Les supports d'expérience contenant les connaissances et savoir-faire de l'entreprise sont utilisés à chaque étape de l'instrumentation. Les supports procéduriers et normatifs seront utiles pour les étapes Projection et Evaluation pour la définition des études à mener dans le développement futur et leur placement dans les phases du cycle de vie. Les supports normatifs ont aussi un rôle pour l'analyse de l'impact des exigences SdF sur le produit. Enfin, les supports métiers seront employés dans les quatre premières étapes pour la prise en compte notamment des routines de conception et des habitudes des différents métiers de l'entreprise.

L'état des lieux préliminaire a permis d'inventorier l'ensemble des supports. Cette cartographie comporte :

- le nom du support communément employé dans l'entreprise,
- son type : E, M, N, P,
- une description succincte du support (contenu),
- son emplacement pour y accéder,
- diverses caractéristiques : format (word, excel, powerpoint,…), nombre de pages,…

Nous proposons un aperçu des supports disponibles dans l'entreprise partenaire pour chaque famille.
Parmi les supports procéduriers de l'entreprise, différents types existent :

- les supports relatifs à la démarche SdF mise sous contrôle par l'entreprise : démarche complète, description des différentes méthodes de la démarche, manuel utilisateur des différents outils de SdF,…,
- les supports relatifs au système de management de la qualité : procédure de développement, suivi de projet, documents à fournir en fonction des phases du cycle de vie,…,
- les supports ayant un lien avec la SdF : notamment les procédures de gestion des risques projets qui devront prendre en compte les objectifs SdF ou les risques techniques ayant une forte criticité,
- les supports procéduriers métiers qui régissent les méthodes de travail à mettre en œuvre en fonction du produit considéré ou de ses caractéristiques.

Les supports d'expériences relatifs à la SdF peuvent être :

- des analyses SdF précédentes : AMDEC, APR,…,
- des exigences SdF client sur les projets précédents,
- des problèmes rencontrés relatifs à la SdF : difficulté sur une exigence particulière et manière avec laquelle cette difficulté a été levée.

.

Concernant les supports normatifs, deux types de documents peuvent être considérés dans l'application :

- les supports normatifs relatifs à la SdF,
- les supports normatifs relatifs au type de produit (hors SdF).

Nous décrivons les supports relatifs à la SdF. Actuellement, deux normes relatives à la sécurité fonctionnelle du produit existent :

- l'IEC 61508 : Sécurité fonctionnelle des systèmes électriques, électroniques et électro-programmables relatifs à la sécurité,

- l'ISO 26262 : Road vehicles : Functional Safety ou Véhicules routiers : Sécurité fonctionnelle.

La première est la norme en vigueur et est générique, la seconde est une déclinaison de la première dans le milieu automobile qui sera en vigueur fin 2009 ou début 2010.

Ces deux normes sont déclinées en différents volumes ayant chacun des caractéristiques dont nous donnons quelques exemples. La norme ISO 26262 est déclinée en neuf volumes : Partie 1 Glossaire, Partie 2 Gestion de la sécurité fonctionnelle, Partie 3 Phase de conception, Partie 4 Développement du produit : niveau système, Partie 5 Développement du produit : niveau matériel, Partie 6 Développement du produit : niveau logiciel, Partie 7 Production et utilisation, maintenance et recyclage, Partie 8 Processus d'appui, Partie 9 Analyses liées aux ASIL et à la sécurité.

Les caractéristiques communes de ces documents normatifs sont : leur format (pdf), leur taille (chacun compte entre 27 et 75 pages), leur organisation et leur structure (parties, sous-parties et paragraphes).

Ces exemples ne sont pas exhaustifs mais permettent de matérialiser l'application et d'avoir un aperçu de la diversité de supports à considérer.

5. Conclusion

La démarche de construction de la solution est articulée autour de quatre plans d'abstraction que nous avons présentée dans ce chapitre :

- le plan contexte de l'organisation pour l'intégration de l'ensemble de contraintes liées à la mise en place de l'organisation,
- le plan organisation du PRAO qui structure la démarche de prise en compte des exigences SdF et la rend reproductible,
- le plan instrumentation de l'organisation qui présente les principes engagés dans les différentes étapes de l'organisation,
- le plan support d'instrumentation qui permet l'application des principes de la couche précédente par l'utilisation des connaissances disponibles dans une entreprise.

Cette définition en plan successif confère un caractère méthodologique et structurant pour la mise en place de l'organisation proposée.

Ce chapitre a permis de présenter l'organisation du PRAO préconisée pour la prise en compte de la sûreté de fonctionnement dès l'appel d'offre. Nous avons présenté de façon générale les principes définis pour chaque étape puis proposé une instrumentation de ces différentes étapes dans un cadre plus applicatif. Le caractère structuré et reproductible de l'approche proposée facilite le traitement de la SdF au niveau du PRAO, phase peu considérée jusqu'alors.

L'ensemble des développements a pour objectif :

- de définir une démarche permettant le traitement de la dimension SdF dès le PRAO : démarche que nous avons présentée ici,
- de définir les bases pour mettre en place cette démarche dans un contexte par l'identification des connaissances et supports associés nécessaires : nous avons présenté dans ce chapitre les supports existants dont nous aurons besoin. Les supports manquants seront introduits par la suite.

Le chapitre suivant est consacré aux étapes Projection et Evaluation pour lesquelles nous allons détailler les supports d'instrumentation et définir des modèles "produit" fonctionnels et structurels.

III. Chapitre III : Modèles et supports pour les étapes Projection et Evaluation

1. Introduction

Nous avons présenté dans le chapitre précédent l'organisation du processus de réponse à appel d'offre permettant la prise en compte des exigences sûreté de fonctionnement dans cette phase amont du cycle de développement du produit. Afin de pouvoir instrumenter les étapes Projection et Evaluation du PRAO, il est nécessaire de disposer de modèles de connaissances sur le produit permettant d'évaluer l'impact de ces exigences.

L'étape Projection doit permettre l'étude du système considéré d'un point de vue sûreté de fonctionnement (ou dysfonctionnel). Les difficultés inhérentes à la modélisation du comportement dysfonctionnel de systèmes automobiles ont été abordées dans de nombreux travaux. En effet, ces systèmes ont des particularités que l'on ne retrouve pas dans d'autres systèmes embarqués. On peut noter en particulier le nombre important de séquences de défaillances conduisant à un événement indésirable client, la présence de composants de diagnostic embarqués qui nécessite de considérer simultanément le bon fonctionnement du système et l'état de ces composants dédiés au diagnostic, le couplage d'éléments matériels et logiciels pour la réalisation des fonctions qui complexifie l'analyse des dysfonctionnements.

De plus, de nombreuses méthodes ou méthodologies développées pour la sûreté de fonctionnement s'appuient sur des représentations du produit assez éloignées des représentations métiers classiques alors même que l'étude de la sûreté de fonctionnement ne peut être décorrélée des connaissances métiers intervenant pour la réalisation d'un système.

Il n'existe pas au sein de l'entreprise de modèles produit intégrant la dimension sûreté de fonctionnement ce qui nous a conduits à définir nos besoins en représentation de produits pour l'étape Projection.

Notre objectif dans ce chapitre est d'établir, à partir de l'étude des produits et des besoins pour l'étape Projection, les modèles les plus pertinents répondant à nos attentes.

Nous présentons d'abord les différents positionnements scientifiques relatifs à l'étape Projection qui a pour objet :

- de corréler les exigences du client, plutôt exprimées d'un point de vue fonctionnel, aux connaissances et savoir-faire du concepteur, plutôt exprimés sous la forme de solutions d'architecture,
- de prévoir l'impact du traitement des exigences SdF en se basant sur des représentations du produit,
- de conserver les routines de conception de l'entreprise afin de ne pas perturber le concepteur dans sa démarche de définition d'un nouveau produit.

Nous retraçons ensuite la démarche suivie pour l'étude des produits de l'entreprise, les différentes vues considérées

et l'identification des connaissances à modéliser.

Nous étudions les différents types de modélisation existant pour les systèmes, en portant notre attention sur les modèles permettant une appropriation rapide par les acteurs projet. Nous décrivons, en le justifiant, notre choix pour le formalisme matriciel que nous présentons ensuite plus en détail.

Enfin, nous présentons les modèles développés en explicitant les connaissances qu'ils contiennent : celles directement représentées par les entités modélisées dans le formalisme général et celles, complémentaires, disponibles via la forme d'attributs associés à ces mêmes entités.

2. L'étape Projection

Nos travaux sont placés à l'intersection des domaines de la sûreté de fonctionnement et de la conception de produit et concernent les phases amont du cycle de développement du produit, au stade des négociations client-prestataire.

Les méthodes de prise en compte et d'analyse de la SdF s'intéressent peu aux phases d'acquisition et les méthodes de conception, assez diversifiées, couvrent essentiellement les phases aval du PRAO comme le montre l'état de l'art sur les processus de conception présenté dans [Hadj-Hamou, 02].

D'une manière résumée, la problématique soulevée par l'étape Projection est de faire le lien entre les exigences client, généralement déclinées selon une vue fonctionnelle, et les connaissances / compétences des acteurs projet (exigences métier, expertise SdF), souvent implicites mais généralement corrélées aux modèles structurels.

Il est essentiel de pouvoir rapprocher cette vue client (privilégiant les exigences fonctionnelles) aux modes de réflexion du concepteur (s'appuyant sur des vues structurelles formant la solution physique).

Dans une conception classique, deux approches peuvent être déployées [McCorquodale&al, 03] :

- la conception descendante (ou "Top-Down") qui consiste à partir des spécifications fonctionnelles du système pour établir par décompositions successives les solutions répondant à ces spécifications [Menand, 02], [Alhajj, 08].
- la conception ascendante (ou "Bottom-Up") qui consiste à étudier l'espace des solutions existantes afin de définir, par composition, celles qui pourraient répondre aux spécifications du système [Kundert, 01], [Hamon, 05]. Cette démarche suit néanmoins un alignement descendant des spécifications.

Schématiquement, ces deux approches peuvent être représentées comme l'a proposé Martin, dans [Martin, 01], dont la thèse s'intéresse aux décompositions du processus de conception. Nous adaptons sa proposition de décomposition dans le cadre du développement de produit sur la Figure III-1.

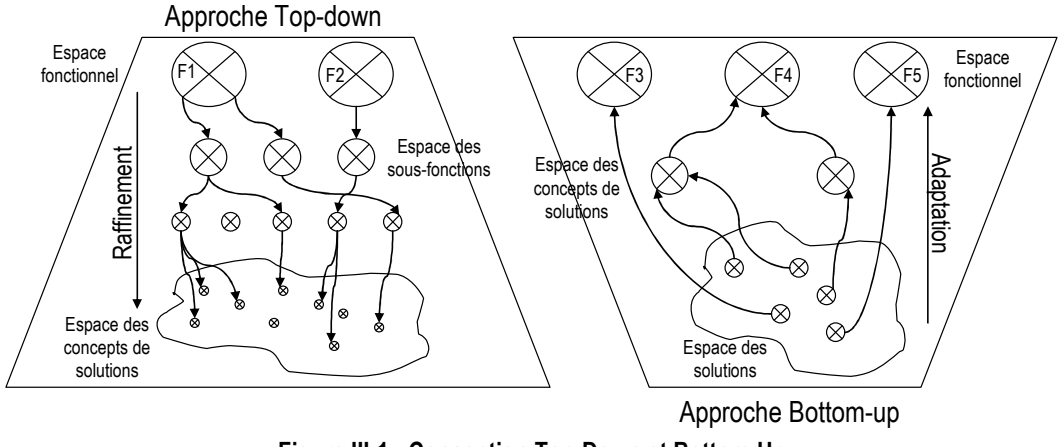


Figure III-1 : Conception Top-Down et Bottom-Up

Chacune de ces approches peut présenter des inconvénients.

La conception descendante peut conduire au redéveloppement de solutions déjà existantes si celles ci ont été spécifiées trop précisément pour des projets précédents et que leur identification comme solution pertinente soit donc difficilement envisageable.

La conception ascendante nécessite de disposer d'une spécification formelle des composants de base afin de pouvoir les réutiliser efficacement et limiter les coûts de développement. L'adaptation à une nouvelle application de modules existants peut induire des études coûteuses et, surtout, conduire à une solution non optimale. Cette approche, enfin, peut freiner l'innovation. On trouve notamment, dans [Kundert, 01] un constat sur les problèmes associés à ce type d'approche : l'absence d'étude et d'optimisation sur l'architecture et des coûts de redéveloppement (adaptation) élevés pour l'adaptation des solutions existantes.

De nouvelles approches, qualifiées de "Plateform-Based Design" (ou développement à base de plateforme), ont été proposées ces dernières années, notamment, pour le développement des systèmes embarqués.

Cette forme d'approche consiste à définir une plateforme qui permet d'établir un lien formel entre l'espace application et l'espace des solutions (Figure III-2).

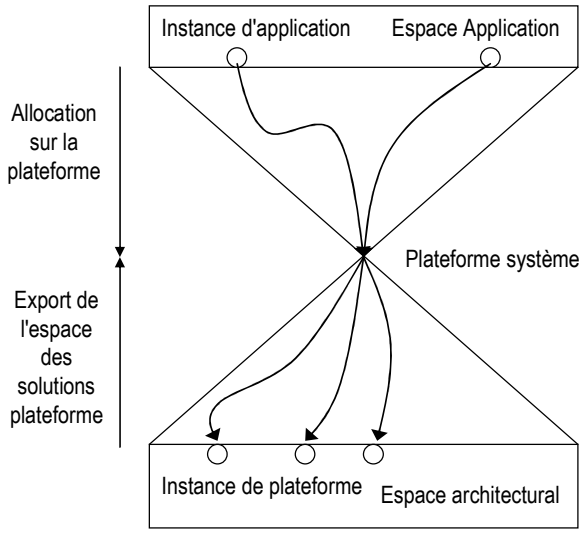


Figure III-2 : Conception à base de plateforme issue et traduite de [Lavagno&al, 03]

Dans la mise en place de ce type de méthodologie, la définition de la plateforme système utilise certains concepts du "Meet-in-the-Middle". Ce type d'approche est devenu une problématique cible de certaines communautés scientifiques qui souhaitent coupler les approches "Top-Down" et "Bottom-Up" dans la méthodologie même de développement et non dans la seule mise en place de la méthodologie. Nous présentons ci-après les principaux concepts de cette démarche.

L'approche "Meet-in-the-Middle" consiste à trouver la forme de rencontre idéale entre l'approche descendante qui part d'un haut niveau d'abstraction pour aller vers les principes de la solution et celle ascendante qui s'appuie sur les solutions existantes pour répondre aux exigences du client. Nous proposons un aperçu des travaux relatifs à la notion de Meet-in-the-Middle dans l'objectif d'en dégager les concepts qui nous permettront ensuite de proposer une adaptation à notre problème.

La démarche du Meet-in-the-Middle est abordée dans différents domaines comme celui du développement logiciel [Perepletichov, 05]. Dans ce cadre, le développement est considéré comme la rencontre entre les raffinements successifs des spécifications et des abstractions des implémentations potentielles. Dans [Gendreau&al, 07], les auteurs

proposent une application de ces concepts pour la conception de microsystèmes de production.

Dans [Bonivento, 07], l'auteur propose l'adaptation d'une méthodologie de développement à base de plateforme existante (initialement dédiée au développement de systèmes embarqués) pour le développement de réseaux de capteurs sans fil dans le cadre de l'amélioration de la fiabilité et de l'interopérabilité entre différentes applications ou implémentations. L'auteur définit une méthodologie à base de plateforme en tant que méthodologie Meet-in-the-Middle dans laquelle les contraintes systèmes sont raffinées selon un principe descendant (Top-Down) alors que les caractéristiques d'implémentation sont explorées selon un principe ascendant (Bottom-Up). La solution proposée est une méthodologie à base de plateforme dont chaque étape combine une phase basée sur une réflexion Top-Down et une réflexion Bottom-Up ainsi qu'une phase de Meet-in-the-Middle qui décide de l'implémentation à choisir par la résolution d'un problème d'optimisation de contraintes. Le principe de l'approche est basé sur la définition de trois niveaux d'abstraction permettant la mise en œuvre de l'approche.

De la même façon, on retrouve dans [Joannon&al, 06], la résolution d'une problématique de développement de systèmes hétérogènes par la mise en place d'une approche à base de plateforme qualifiée de méthodologie Meet-in-the-Middle. Les auteurs s'intéressent particulièrement au développement d'émetteur/récepteur formés de composants analogiques et digitaux généralement développés selon une approche Top-Down et de composants radio-fréquentiels généralement développés selon une approche Bottom-Up. Dans ces conditions, les auteurs cherchent à combler le fossé existant entre les modèles fonctionnels considérés pour les deux premiers types de composants et les modèles structurels de transistors. Pour ces travaux, l'approche développée consiste à proposer une approche descendante pour le développement et ascendante pour la validation tout en intégrant les caractéristiques des niveaux fonctions et composants dans des modèles communs.

Dans [Oliveira&al, 06], les auteurs traitent d'un problème d'exploration multi-objectif d'un espace de conception. Ils définissent, dans ce cadre, une méthodologie à base de plateforme comme une stratégie Meet-in-the-Middle utilisée pour maximiser la réutilisation des composants déjà définis et fournir la meilleure personnalisation possible en regard des exigences d'une application. Les concepts utilisés pour la résolution consistent en l'adaptation d'un modèle générique de plateforme à un cas particulier.

On peut citer d'autres travaux qui explicitent la notion de Meet-in-the-Middle tels que ceux trouvés dans [Wu&al, 08] dans le cadre de la proposition d'une méthodologie de développement de logiciel embarqué, ou encore dans [Turner&al, 05] où les auteurs proposent un cadre pour le développement de nouveaux systèmes.

Cet aperçu des travaux existants permet la mise en relief de la notion de Meet-in-the-Middle dont l'idée principale est de définir, d'une part, des modules élémentaires de composants, et, d'autre part, des modules fonctionnels ; lors du développement d'un nouveau projet, on fera le lien entre ces modules afin d'arriver au meilleur compromis entre les besoins et les solutions existantes. L'intérêt de l'approche proposée réside surtout dans le fait que :

1) on peut choisir le niveau d'abstraction des différents modules de base,

2) ces modules peuvent être déclinés, avec une fonctionnalité commune, dans différentes solutions.

Nous proposons, dans le cadre de la problématique abordée, l'utilisation qui est faite de cette notion. Dans notre cas, nous ne considérons pas le spectre complet des contraintes qui président le processus de conception classique. Nous

nous intéressons essentiellement aux caractéristiques sûreté de fonctionnement mais nous retrouvons la même préoccupation de faire correspondre les exigences SdF client, exprimées suivant des vues fonctionnelles, et les connaissances/expertises métier de l'entreprise, exprimées sous forme de solutions.

Nous proposons sur la Figure III-3 une illustration de l'application de ces concepts en liant cette approche à la solution d'organisation du PRAO que nous avons définie dans le chapitre 2.

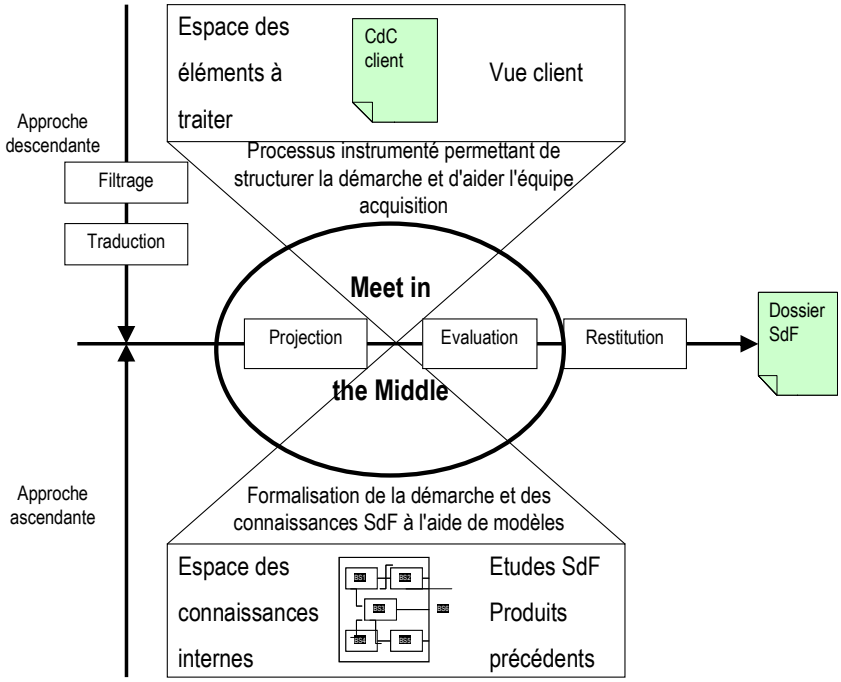


Figure III-3 : Articulation de la méthode

Nous montrons sur ce schéma comment les développements que nous avons proposés dans le chapitre II sur le PRAO s'inscrivent dans ce type de démarche.

Les premiers liens sont au niveau de l'assistance à l'équipe Acquisition pour l'analyse des besoins client. Deux appuis complémentaires sont offerts pour l'identification des exigences SdF (Etape **Filtrage**) et pour leur expression dans un vocabulaire/formalisme propre à l'entreprise (Etape **Traduction**) permettant à l'équipe, même si les exigences sont décorrélées de ses habitudes, de les prendre en compte.

Les autres liens figurent dans les propositions de formalisation de la connaissance des acteurs projets permettant de définir des modules élémentaires fonctionnels et matériels qui aideront, par le biais des étapes **Projection** et **Evaluation**, à établir l'impact des exigences SdF.

Une difficulté soulevée par l'étape Projection réside dans la modélisation de la connaissance sûreté de fonctionnement. En effet, il n'existe pas dans l'entreprise partenaire de représentation du produit considérant explicitement la SdF, notamment, au niveau d'abstraction requis dans le PRAO.

Nous avons donc dû analyser les produits concernés par ce travail et identifier la connaissance entreprise qui leur était associée (ceci constituant le point de départ de l'étude SdF). Nous avons ensuite choisi un formalisme d'expression puis établi différents modèles par rapport à la connaissance disponible et aux objectifs de cette étape Projection.

3. Produits et connaissances associées

3.1. Définition des concepts liés aux systèmes considérés et application

Nous présentons d'abord différentes notions que nous allons considérer durant l'étude des produits.

Nous introduisons dans un premier temps le concept de système et les notions associées. Le groupe de travail "Ingénierie Système" de l'AFIS (Association française d'ingénierie système : www.afis.fr) a proposé un glossaire adapté des travaux de l'INCOSE (International Council on Systems Engineering : www.incose.com) sur lequel nous nous appuyons [AFIS, 04].

Un système est un ensemble d'éléments en interaction, organisés pour atteindre un ou plusieurs résultats déclarés. La norme AFNOR NF Z67-288 PR (Ingénierie systèmes – Processus de cycle de vie des systèmes) précise qu'un système peut être considéré comme un produit ou comme les services qu'il délivre.

Dans la suite du document, nous désignerons par le terme "produit" les systèmes que nous étudions dans la mesure où un produit est défini comme le résultat d'activités ou de processus, ce qui correspond bien aux situations que nous considérons.

Nous considérons sur la Figure III-4 la représentation des relations qui caractérisent un système. Les éléments avec lesquels il est en relation sont :

- la finalité : fonction principale du système,
- le contexte : environnement dans lequel le système évolue,
- les systèmes extérieurs : systèmes avec lesquels le système pourra être en relation (environnants du système [Tassinari, 06],
- les fonctions : actions que le système exécute pour fournir ce pour quoi il a été conçu,
- les constituants : supports nécessaires à la réalisation des fonctions,
- les entités : éléments traités dans le système : énergie, information ou matière.

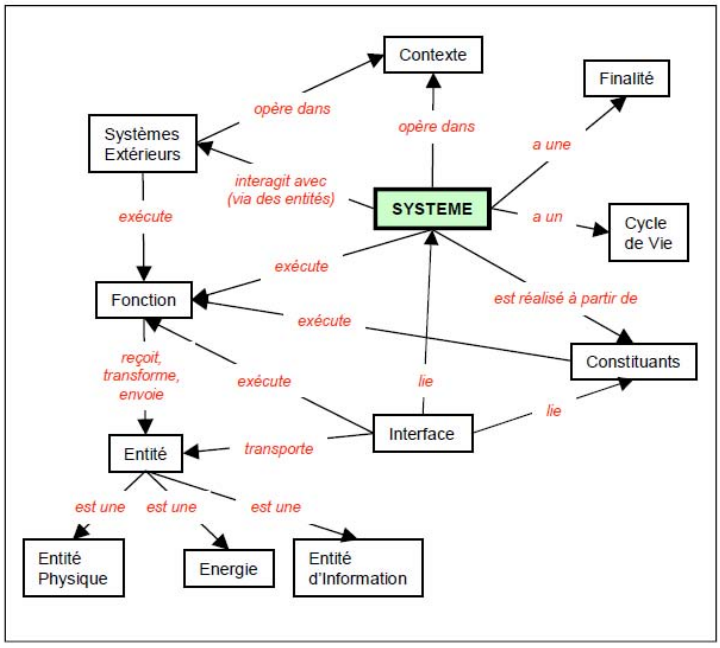


Figure III-4 : Relation caractérisant un système tiré de [AFIS, 04]

Nous allons appliquer cette description à notre cas d'étude.

3.2. Les produits considérés

3.2.1. Approche fonctionnelle

Les produits étudiés sont des systèmes mécatroniques automobiles embarqués, disposant de caractéristiques sécuritaires par les fonctions qu'ils remplissent dans le véhicule.

Ces systèmes appartiennent à quatre familles de produit :

- ABS ("Anti-Lock Braking system" ou "antiblocage des roues") : système dont l'objectif est d'éviter un blocage des roues en cas de freinage d'urgence, il est composé d'un calculateur, de plusieurs capteurs et de quatre actionneurs. Le calculateur analyse continûment la vitesse du véhicule et ses variations ainsi que la vitesse de chaque roue. Lorsqu'un blocage est détecté, le système commande les actionneurs de façon à diminuer le freinage sur la roue désignée. La fiabilité du système est augmentée par des stratégies de reconfiguration comme, par exemple, l'estimation de la vitesse d'une roue, si le capteur correspondant est défaillant, par rapport à celle des trois autres [Khalfaoui, 03],
- Suspension : système ayant pour but de réduire les désagréments dus aux imperfections des routes dans l'habitacle, améliorant ainsi le confort et protégeant les autres systèmes du véhicule des vibrations. Il améliore aussi la tenue de route en optimisant le contact entre les roues et le sol [Ziegler, 05]. Ce type de système est composé d'un calculateur électronique et de divers capteurs/actionneurs en fonction du type de suspension considéré,
- Direction assistée (ou steering) : système dont l'objectif est de fournir une assistance au conducteur en fonction de l'effort de sollicitation sur le volant. Ce type de système est composé d'un calculateur électronique, d'un moteur et d'un ou plusieurs capteurs en fonction du type de direction considéré,
- Autres cas : ensemble des systèmes n'appartenant pas aux trois autres familles et satisfaisant à des opportunités de marché par réutilisation de fonctions connues de par leur présence sur d'autres systèmes ou intégration de nouvelles fonctionnalités (exemple : couplage d'un ABS et de fonctions complémentaires dans un même système, assistance de freinage,..).

Nous illustrons sur la Figure III-5 la situation des trois premiers types de systèmes dans l'environnement véhicule.

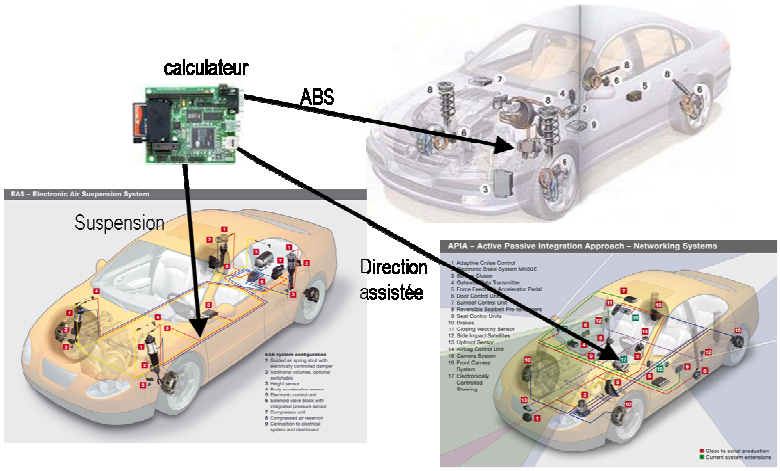


Figure III-5 : Systèmes dans leur environnement

L'information tirée de cette présentation des familles de produits permet de proposer une typologie fondée sur les correspondances entre les entrées et sorties du système :

- systèmes mono-entrée/mono-sortie : direction assistée,

- systèmes mono-entrée/multi-sorties : boîtier de servitude (gestion d'énergie),
- systèmes multi-entrées/mono-sortie : airbag,
- systèmes multi-entrées/multi-sorties : suspension, ABS, ...

Présentons maintenant l'étude réalisée dans l'entreprise partenaire.

Les principaux développements faits par l'entreprise portent sur le calculateur électronique des "produits" (illustré sur la Figure III-5). Nous désignerons par "ECU" ce calculateur (ECU : Electronic Control Unit).

L'objectif est de faire un bilan des connaissances disponibles pour les différents métiers impliqués dans la réalisation des produits.

Nous débutons par une étude fonctionnelle du produit.

Nous avons effectué, dans un premier temps, une Analyse Fonctionnelle Externe. Nous représentons le modèle fonctionnel par le biais d'un diagramme pieuvre dans lequel apparaissent les éléments extérieurs, les fonctions de service et les contraintes associées [Zwingmann, 05]. Cette méthode a pour objectif de définir les limites du système, d'étudier ses relations avec son environnement et d'exprimer ses liens en termes de fonctions à remplir.

Deux types de fonctions peuvent être définis : 1) les fonctions de service qui expriment ce pour quoi le système a été conçu [AFNOR NF X50-150], 2) les fonctions contraintes qui expriment les exigences liées à l'intégration du système à son environnement.

Nous proposons en annexe (Annexe III-A), le détail de la méthode d'analyse fonctionnelle issue de [Tassinari, 06]. Nous montrons sur la Figure III-6 le résultat de cette analyse généralisée à l'ensemble des produits.

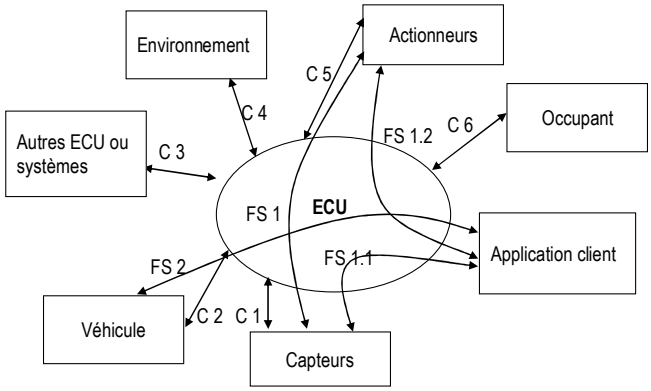


Figure III-6 : Analyse fonctionnelle externe

Nous explicitons ci-après les différentes fonctions de service :

FS 1 : Commander les sorties en fonction de l'état des entrées,

FS 1.1[15] : Fournir les informations issues des capteurs à l'application client,

FS 1.2 : Commander les sorties en fonction de la consigne fournie par l'application client,

FS 2 : Fournir les données issues du véhicule à l'application client et inversement.

[15] La considération de l'application client comme un élément extérieur s'explique par le fait que le client peut développer sa propre application, cela lui permet de ne pas dévoiler son savoir-faire concernant les lois de commande et les paramètres qu'il utilise (ainsi que les calculs) pour la construction de la loi de pilotage. Cependant, dans certains cas, l'entreprise prestataire peut être chargée de développer cette application. Toutefois, même si cette application est réalisée par le responsable de l'ECU, l'expérience montre qu'elle est développée indépendamment du reste du système.

Nous donnons aussi les fonctions contraintes :

C1 : être compatible avec les capteurs (i.e. nombre d'entrées, nature des signaux,...,),

C2 : être compatible avec le véhicule (alimentation, type de bus de données,...,),

C3 : être compatible avec les autres systèmes ou ECU en relation (ne pas mettre en danger,..),

C4 : résister à l'environnement,

C5 : être compatible avec les actionneurs (i.e. nombre, type,...,),

C6 : respecter les occupants (sécurité assurée, ...).

Nous effectuons ensuite une analyse fonctionnelle interne du système qui permettra une représentation structurée hiérarchique du système. Cette décomposition permettra d'identifier les fonctions techniques [Medjoudj, 06]. L'ensemble des fonctions de service est décomposé en sous-fonctions.

Considérons d'abord la fonction de service FS1 qui sera étudiée par le biais des fonctions FS 1.1 et FS 1.2. Cette fonction peut être décrite dans le formalisme SADT (Structured Analysis and Design Technique) (voir [Nancy, WEB], [Berger, WEB], [IDEF, WEB] suivant le schéma de la Figure III-7.

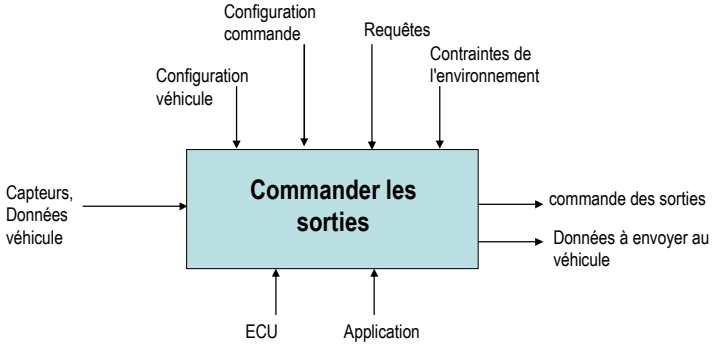


Figure III-7 : Diagramme SADT A_0

Le niveau de décomposition[16] suivant est donné sur le schéma de la Figure III-8.

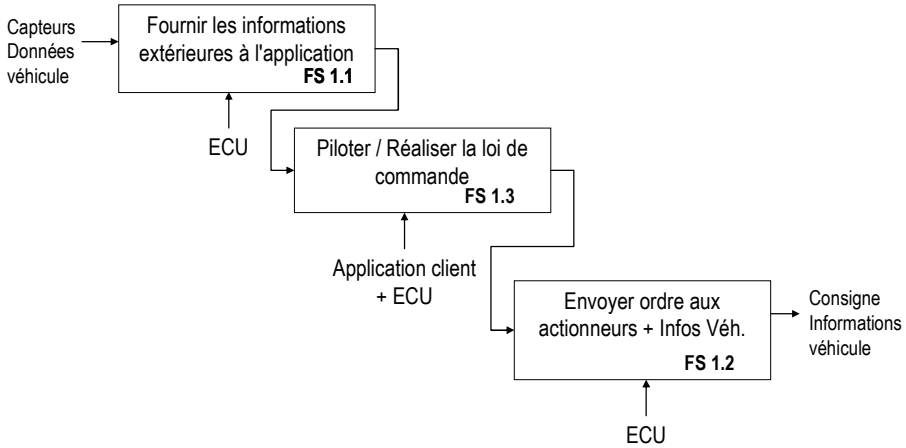


Figure III-8 : Diagramme SADT A-1

Suite à cette description de la fonction principale en trois sous fonctions, nous allons nous intéresser plus particulièrement à la décomposition des fonctions FS 1.1 et FS 1.2. Pour la fonction "Piloter", seuls certains détails

[16] Les décompositions fonctionnelles sont volontairement données sans certains détails afin de ne pas divulguer d'information confidentielle appartenant au savoir-faire de l'entreprise. Le niveau de détail est suffisant pour la compréhension de l'étude réalisée et des différentes caractéristiques des produits.

seront donnés à titre informatif pour permettre la compréhension globale.

Les fonctions FS 1.1 et FS 1.2 ont la même structure et pourront être décomposées comme indiqué sur le diagramme de la Figure III-9.

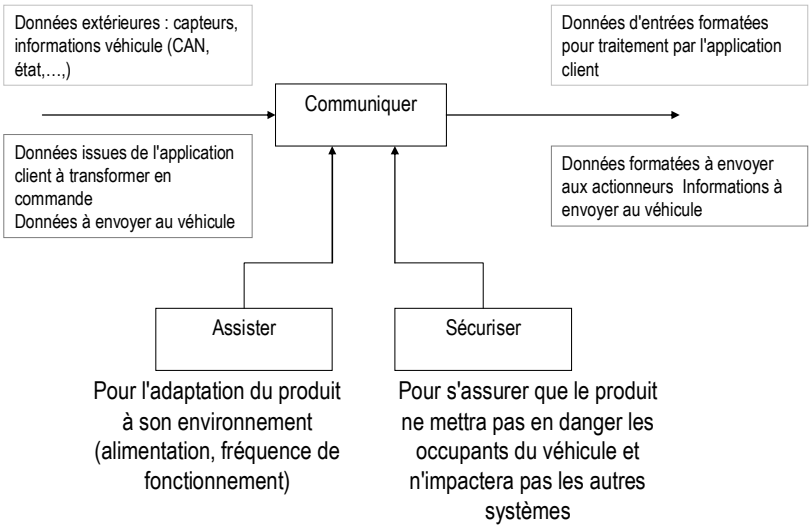


Figure III-9 : Décomposition des fonctions FS 1.1 et FS 1.2

Cette décomposition met en évidence les premiers niveaux des fonctions techniques[17] et offre un premier aperçu de la composition du système.

L'étape suivante consiste à définir la décomposition des fonctions "Communiquer", "Assister" et "Sécuriser". Ces trois fonctions correspondent respectivement à :

- Communiquer = "Acquérir" + "Traiter" (i.e. mise en forme, conversion) + "Transmettre",
- Assister = "Alimenter" + "Synchroniser" (ou séquencer),
- Sécuriser = "Contrôler le fonctionnement" + "Mettre en sécurité".

La fonction "Piloter" peut être décrite de la même façon que les deux autres dans le sens où elle nécessite, elle aussi, l'appui des fonctions "Assister" et "Sécuriser".

Enfin, une autre fonction d'assistance est nécessaire ; c'est la fonction "Stocker l'information" utile à "Piloter" pour assurer le stockage de programmes divers et à "Sécuriser " afin de mémoriser certaines informations de défaillances.

Nous proposons un diagramme récapitulatif de l'ensemble de ces fonctions sur la Figure III-10.

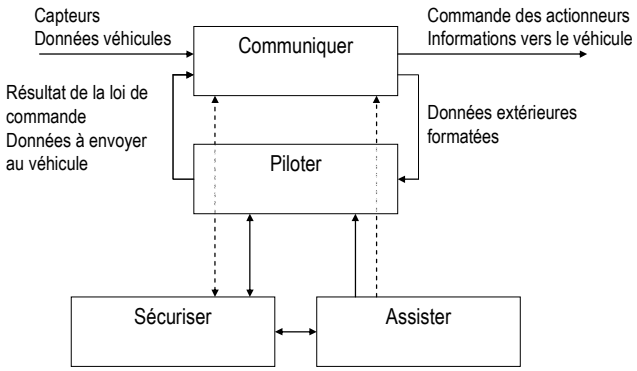


Figure III-10 : Récapitulatif "Organisation fonctionnelle"

[17] Les fonctions techniques correspondent à des actions internes au produit (entre ses constituants), choisies par le concepteur réalisateur, dans le cadre d'une solution, pour assurer des fonctions de service [Menand, 02].

Bien qu'élémentaire, l'étude fonctionnelle précédente présente deux intérêts majeurs.

Il n'existe pas de représentation fonctionnelle formelle d'une ECU (Electronic Control Unit) dans les travaux menés sur les systèmes embarqués intégrant notamment, dans une même étude, les aspects logiciels et matériels ; les projets ayant trait aux ECU ne s'intéressent qu'à l'un des deux aspects ou bien les considèrent séparément. Nous citons, par exemple, le projet AUTOSAR[18], développé par un consortium composé de constructeurs et d'équipementiers, dont l'objectif est d'élaborer et de normaliser une architecture logicielle ouverte destinée aux calculateurs des systèmes embarqués automobiles [AUTOSAR, 06] et qui fait référence dans le domaine automobile. Citons aussi le projet EASIS[19], développé lui aussi par un consortium de constructeurs, d'équipementiers, de laboratoires de recherche et de fournisseurs d'outils logiciel et dont l'objectif le développement d'une architecture standard dans le véhicule ainsi que la standardisation de l'approche système pour les systèmes intégrés de sécurité [EASIS_Presentation]. Ces deux projets sont présentés en annexe III-B.

Les calculateurs considérés présentent la particularité de ne pas être entièrement développés par la même entreprise. L'entreprise prestataire doit cependant en assurer la sécurité sans en connaître le fonctionnement exact ; la fonction "Piloter" est assimilée à une boîte noire interne au système développé et nous n'avons pas identifié dans les travaux correspondants de modèles intégrant cette particularité.

Après avoir défini les fonctions du système, il est important d'étudier leurs supports de réalisation.

3.2.2. Approche structurelle

L'objectif est d'établir un état le plus général possible de la structure du produit afin d'établir, par la suite, des modèles de représentation permettant l'étude de la sûreté de fonctionnement du système en s'appuyant sur ces modèles.

Trois métiers principaux contribuent à la réalisation des fonctions d'un calculateur électronique : électronicien, informaticien et mécanicien.

Nous proposons tout d'abord une décomposition structurelle impliquant le vocabulaire propre à chaque métier. Nous détaillons ensuite les entités considérées par les différents métiers, à partir de l'analyse approfondie de différents projets et travaux ayant trait à l'étude des calculateurs du monde automobile ([EASIS, WEB], [AUTOSAR, WEB]. Certains détails de l'étude, non pertinents pour la compréhension, sont disponibles en annexe (Annexe III-C).

Nous proposons sur le schéma de la Figure III-11une représentation d'un calculateur dans son environnement.

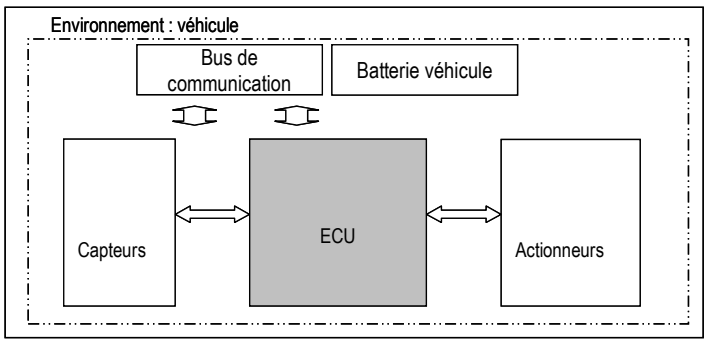


Figure III-11 : Représentation d'une ECU dans son environnement

[18] [AUTOSAR, WEB] : www.autosar.org

[19] [EASIS, WEB] : www.easis.org

Nous proposons ensuite sur la Figure III-12 une décomposition de la structure du produit par métier.

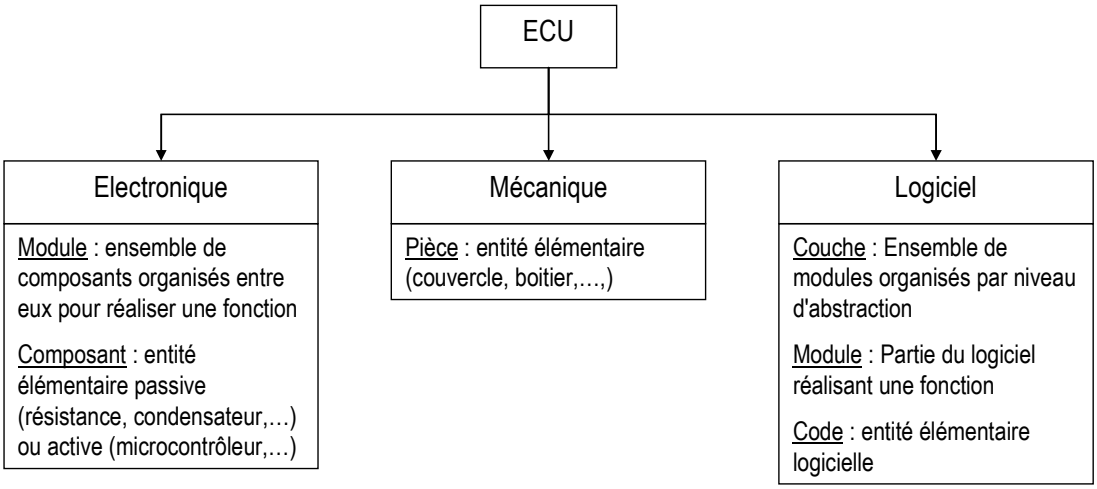


Figure III-12 : Composition d'un calculateur

Nous donnons sur le schéma de la Figure III-13 la décomposition finale obtenue pour les familles de composants électroniques et mécaniques. Concernant la partie électronique, on retrouve le cœur commun aux systèmes embarqués automobile : le microcontrôleur ainsi que l'ensemble des périphériques qui vont permettre de faire le lien avec l'extérieur du système (comme l'alimentation, les interfaces d'entrées (pour les capteurs), de sorties (pour les actionneurs) et de communication avec le véhicule (réseau véhicule)). Enfin, on retrouve les modules destinés à la sécurité du produit : le superviseur et le module de mise en sécurité. Pour la partie mécanique, on retrouve les pièces qui vont permettre le conditionnement des parties logicielles et matérielles : un couvercle, un boîtier et un joint. Le connecteur permet lui de relier le produit au véhicule.

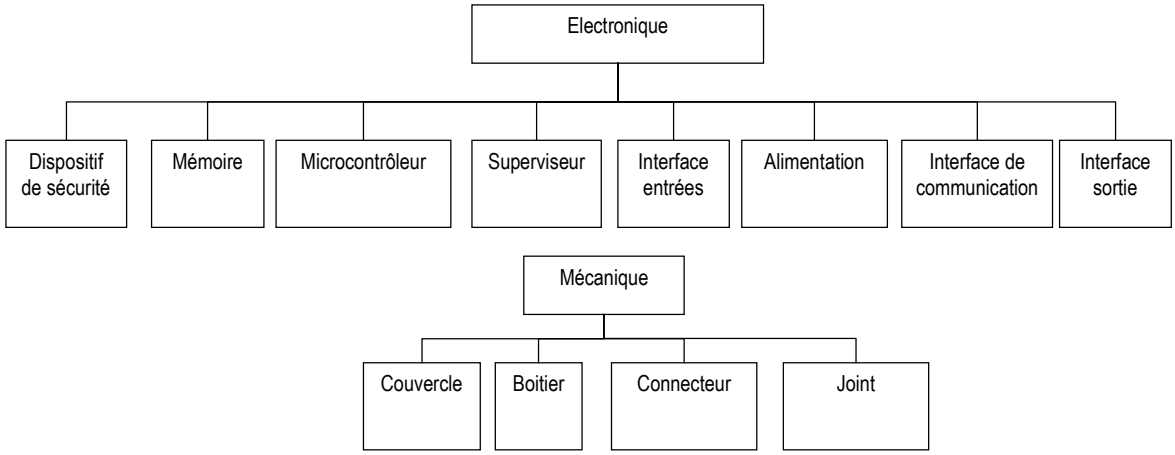


Figure III-13 : Décomposition en modules électroniques et en pièces mécaniques

Le logiciel est organisé en couches d'abstraction allant du support matériel à l'application du client. Nous reprenons sur le schéma de la Figure III-14 la représentation proposée par AUTOSAR dans [AUTOSAR_PRESENTATION].

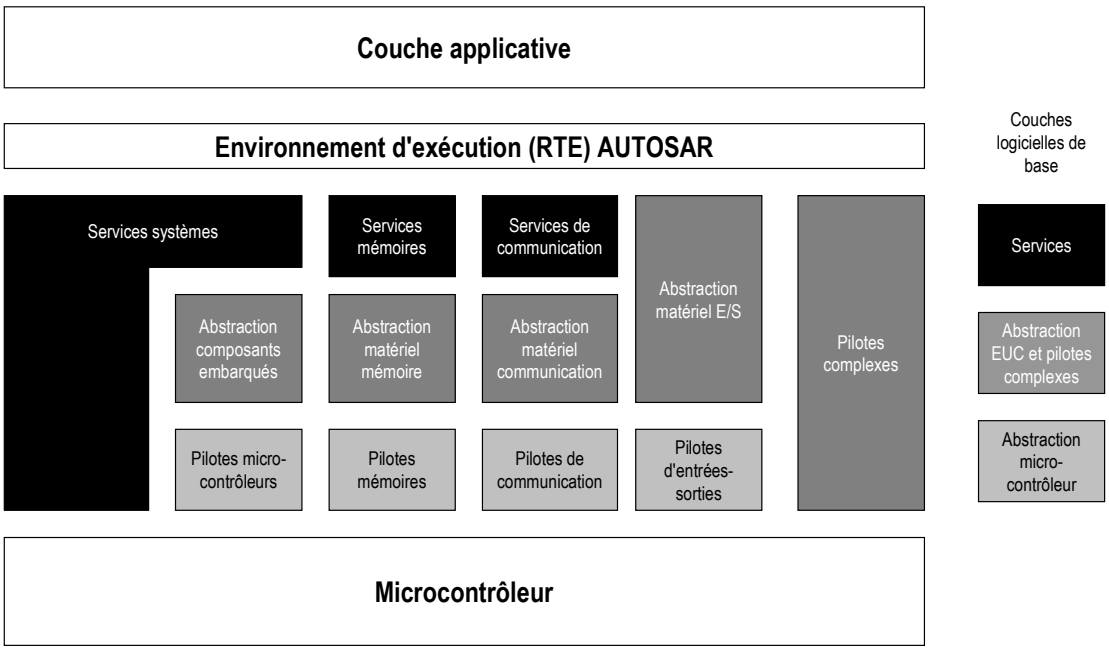


Figure III-14 : Couche logicielle et modules (issu de [AUTOSAR, 06])

La partie logicielle peut être décomposée en couches, chacune de ces couches contenant des modules prédéfinis (les couches et le type de modules contenu dans celle-ci sont présentés en annexe III-B).

Ce bilan de la composition d'un calculateur est nécessaire pour la suite car il permet d'identifier les modèles à même d'intégrer les différentes caractéristiques présentées.
Nous proposons maintenant de décrire l'organisation des différents éléments présentés pour la création de l'ECU.

3.2.3. Organisation d'un calculateur

L'objectif est de montrer ici les relations existantes :

- entre les différentes familles de composants appartenant aux différents métiers,
- entre les différents éléments dans un même métier,

afin de dégager les caractéristiques des systèmes étudiés, ce qui permettra de justifier de l'emploi d'un type de modèle.
Nous nous intéressons tout d'abord aux liens existants entre les différents métiers ; ces liens sont représentés schématiquement sur la Figure III-15.

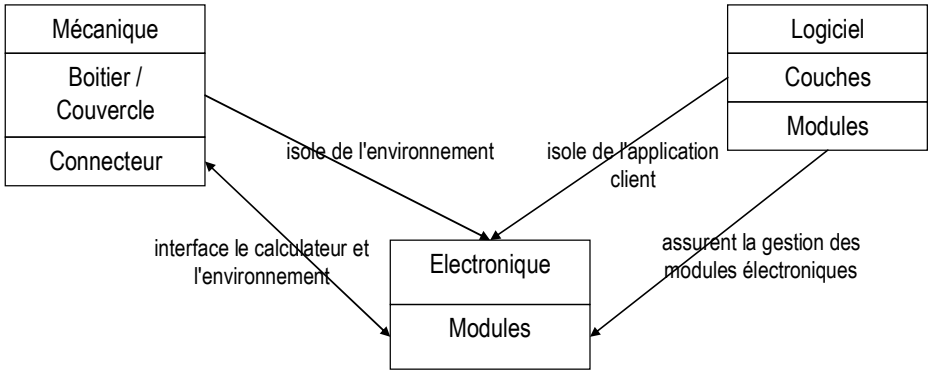


Figure III-15 : Relation entre les différents métiers

Ce schéma illustre bien la principale difficulté rencontrée dans l'étude des calculateurs constituée par l'interdépendance entre les éléments constitutifs.

Au niveau des relations entre les entités d'un même métier, nous nous limitons à l'étude du logiciel et de l'électronique car, excepté l'assemblage (par exemple entre le boîtier et le couvercle), il n'y a pas d'autres types de liens sur le plan mécanique.

Pour le logiciel, les liens existants entre les différentes couches sont décrits en détail dans [AUTOSAR_PRESENTATION] ainsi que les règles de relations entre les différents modules en fonction de la couche à laquelle ils appartiennent. Nous rappelons sur la Figure III-16 le schéma représentant les relations possibles.

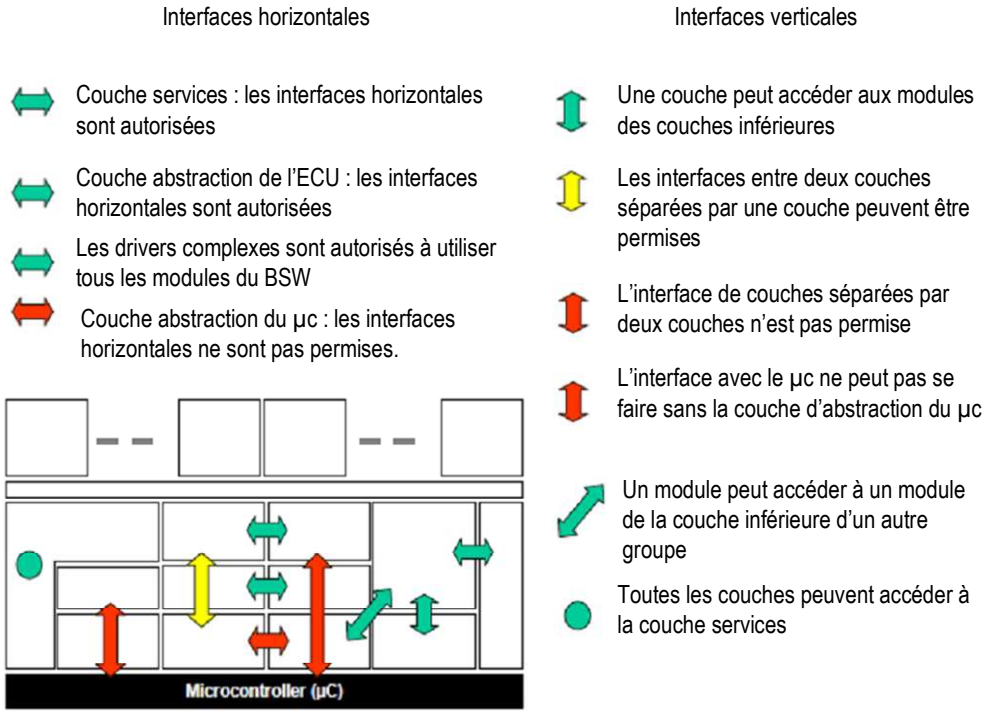


Figure III-16 : Relations entre couches logicielles et modules

La part la plus importante de l'étude concerne les composants électroniques qui, couplés au logiciel, réalisent la majorité des fonctions du produit car les coûts direct du produit (composants, matière,..,) sont principalement des coûts électroniques.

Pour cette famille de composants, le coût est directement fonction du nombre de modules de chaque type ; c'est pourquoi, nous devons étudier en détail les possibilités de choix offertes au concepteur lors de la réalisation d'un nouveau produit.

A partir de l'étude des configurations de produit existants et le questionnement des acteurs des différents métiers, nous avons explicité les degrés de liberté existants lors de la conception d'un nouveau produit afin d'identifier les règles de conception relatives aux métiers et celles relatives à la sûreté de fonctionnement.

Nous adoptons la démarche suivante (Figure III-17) : 1) nous établissons d'abord la configuration minimale du produit (hors considération spécifique SdF et exigences client), 2) nous formalisons ensuite l'expertise engagée pour définir l'architecture du produit en fonction des décisions métier et des considérations SdF.

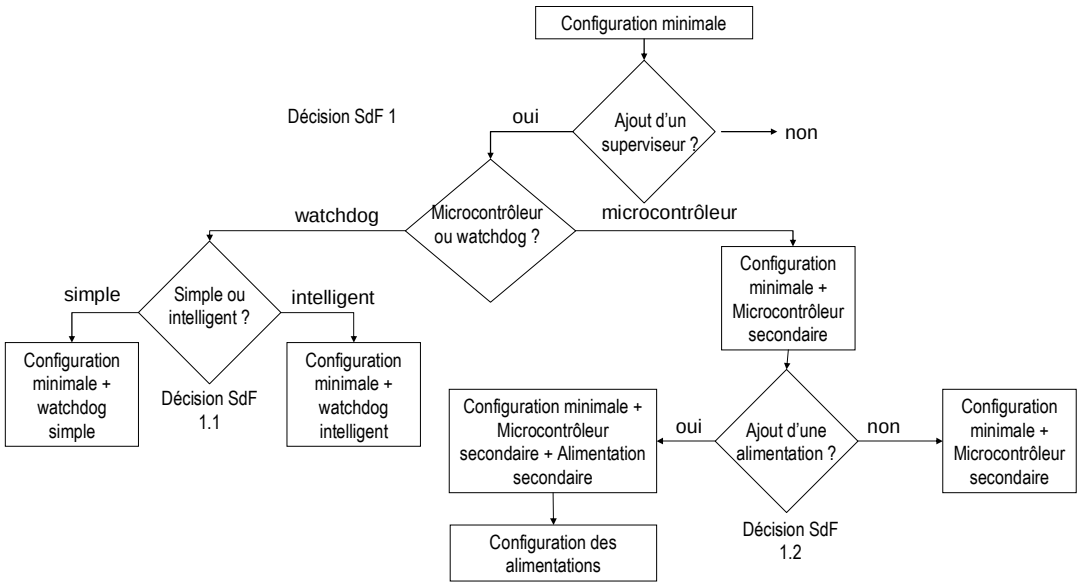


Figure III-17 : Choix de conception

Des choix de conception (décisions) sont effectués pour répondre aux exigences de sûreté de fonctionnement, ces choix sont implicitement engagées, nous les avons identifiées et proposons de les expliciter ci-dessous.

La première décision SdF 1 concerne l'ajout ou non d'un superviseur en regard des niveaux de sécurité à atteindre pour le produit considéré. Dans le cas où la décision est négative, on sort de l'arbre de décision. Si la décision est prise d'ajouter un superviseur, il faut définir si on ajoute un "chien de garde" (ou "watchdog[20]") ou un second microcontrôleur.

Dans le cas où la décision est d'ajouter un watchdog, la décision SdF 1.1 consiste à définir si on met un watchdog simple ou un watchdog intelligent, le watchdog donne au microcontrôleur principal la possibilité de lui envoyer une trame de contrôle à alors que le watchdog simple peut recevoir uniquement un signal simple.

Dans le cas où la décision est l'ajout d'un second microcontrôleur, la décision SdF 1.2 à prendre concerne l'ajout d'une alimentation supplémentaire de manière à rendre plus indépendant les deux microcontrôleurs.

Si le choix d'une alimentation supplémentaire est effectué, il faut définir quels seront les blocs structurels que l'on rattachera à chacune d'elles.

De nombreux choix sont possibles pour le développement du calculateur au niveau, notamment, de l'implémentation de chaque module. Parmi ceux-ci, nous nous intéressons essentiellement à ceux qui induisent l'adjonction de modules supplémentaires par rapport à la configuration minimale ou qui entraînent des modifications des relations entre modules.

Les situations suivantes entraînent des choix influant les relations entre modules.

1- Une ou plusieurs entrées "critiques" doivent être continûment observées.

Deux solutions sont possibles :

- adresser le(s) signal (aux) concerné(s) à deux entrées différentes du microcontrôleur ; cette solution permet une fonction diagnostic couvrant un spectre de défaillances plus important que dans le cas où le signal est envoyé à un seul microcontrôleur,

[20] L'appellation "watchdog" sera utilisée par la suite dans la mesure où il est très rare de rencontrer le terme "chien de garde".

- adresser le signal sur les deux microcontrôleurs pour les mêmes raisons que précédemment ; cette solution présente l'avantage d'assurer l'affectation du signal de l'entrée critique même si l'un des deux microcontrôleurs est défaillant.

2- Les spécifications de la "mise en sécurité" sont particulières. Les relations du bloc de sécurité avec les autres modules du calculateur dépendent directement de l'état de sécurité déterminé par le client ou par l'expertise. Pour certains produits, les actuateurs devront être en fonctionnement continu dans la position de repli rendant nécessaire le maintien de leur alimentation dans cette situation alors que dans d'autres situations la position de repli pourra être associée à des actuateurs à l'arrêt. Pour l'illustration, l'exemple de la suspension est intéressant car les normes européennes imposent une position de repli dans laquelle les actuateurs sont désactivés alors que les normes américaines imposent une position de repli dans laquelle les actuateurs sont activés.

Les résultats que nous venons de présenter dans cette étude particulière et, notamment, les règles SdF que nous avons proposées recoupent bien ceux de différents projets "phare" faisant référence dans le domaine de la configuration de produits automobiles. Les projets AUTOSAR et EASIS considèrent eux aussi les solutions impliquant un microcontrôleur et un watchdog et celles intégrant deux microcontrôleurs comme illustré sur la Figure III-18 et la Figure III-19.

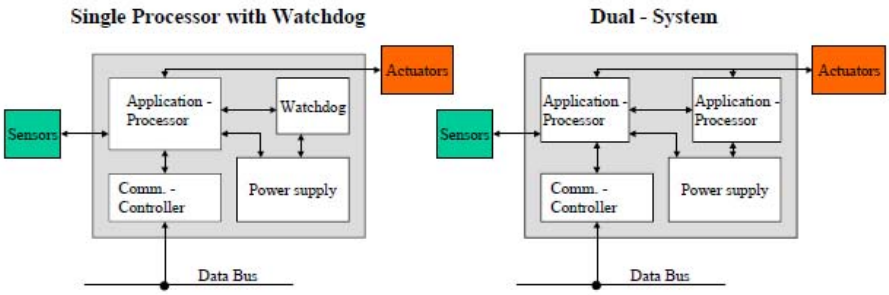


Figure III-18 : Configurations de produits issus de [EASIS D0.1.2]

Sur la figure précédente, nous montrons deux solutions proposées dans le projet EASIS (document [EASIS D0.1.2]). La première solution est composée d'un microcontrôleur (CPU) et d'un watchdog. Dans cette configuration, la détection des défaillances est réalisée par le watchdog qui positionne le microcontrôleur en position off ou qui remet à 0 le processeur en cas de défaillances. La seconde solution composée de deux microcontrôleurs (CPU) consiste à implémenter du logiciel sur les deux entités, chacune d'entre elles étant à même de réaliser la détection des défaillances et de mettre le système dans un état sûr en cas de défaillances.

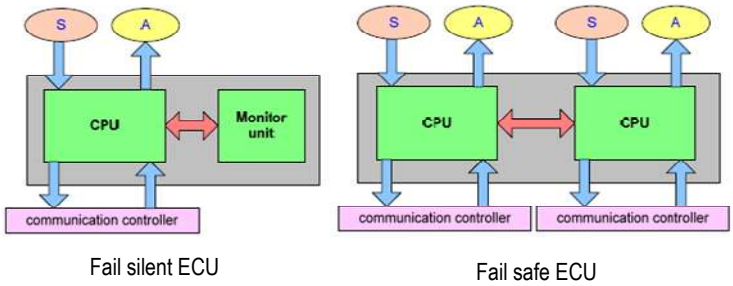


Figure III-19 : Configurations de produits issus de [Chen, 08]

Dans [Chen, 08], l'auteur s'intéresse aux spécifications et aux concepts pour les futures architectures électroniques d'un point de vue de la sécurité intégrée. Dans ce cadre, deux configurations sont proposées. La première est composée

d'un microcontrôleur et d'un watchdog (monitoring unit) ; dans ce cas, le watchdog surveille la cohérence d'un signal et agit en conséquence (arrêt du microcontrôleur ou mise en état sûr). La seconde solution composée de deux microcontrôleurs consiste ici à implémenter le même logiciel dans les deux entités et à comparer les résultats (pour vérifier la cohérence) par le biais d'une communication interne.

Les éléments que nous venons de présenter sont importants dans le sens où ils constituent la panoplie des constituants des systèmes que nous allons modéliser pour mener l'étape Projection.
Nous nous intéressons maintenant aux modèles représentatifs de ce type de système ainsi qu'à ceux permettant l'étude de la sûreté de fonctionnement.

4. Modèles de représentation pour l'étape Projection

4.1. Rappel des contraintes

Nous devons étudier l'impact des exigences SdF client sur le produit et la démarche à mettre en place. Les modèles que nous allons établir doivent permettre d'étudier les dysfonctionnements du produit, rendant indispensable la modélisation des relations entre les différentes entités.
Les modèles doivent satisfaire à des exigences :

- de modularisation, afin de permettre la représentation des différentes architectures envisageables pour le produit (i.e. configurations particulières des modules constitutifs et liens entre ceux-ci),
- d'abstraction, le niveau d'analyse étant celui du PRAO correspondant à un niveau d'abstraction élevé du produit, en distinguant cependant les aspects mécanique, électronique et logiciel,
- de simplicité, afin de respecter les habitudes de travail du concepteur à qui ces modèles seront proposés, lui permettant de "projeter" les exigences SdF sur les connaissances métier ; une conséquence sera la facilité d'appropriation et de prise en main,
- de suivi des choix effectués afin de pouvoir capitaliser l'historique des choix en fonction des exigences du CdC.

4.2. L'étude de la sûreté de fonctionnement sur les modèles de produit

Nous nous intéressons aux caractéristiques de fiabilité et de sécurité du produit que nous allons considérer à travers ses caractéristiques fonctionnelles (corrélées à la vue client), structurelles (proches de l'expertise métier) et comportementales (liées aux exigences SdF).
Nous retrouvons cette approche dans [Zwingmann, 05] où l'auteur s'intéresse à l'intégration de la validation dans le processus de conception. Zwingmann fait état d'un manque de travaux concernant l'évaluation des performances dans la conception. Il propose une approche "FSC" couplant les mêmes caractéristiques fonctionnelles, structurelles et comportementales du produit afin d'en évaluer la fiabilité et la maintenabilité au stade de la conception.

De plus, comme présenté dans le paragraphe 3.2.3 du chapitre 2, l'étude de la SdF d'un système consiste à étudier ses défaillances par le biais de méthodes appliquées qui partent soit d'une défaillance fonctionnelle pour déterminer les causes potentielles au niveau structurel soit d'une défaillance structurelle afin de définir l'impact sur le système complet

au niveau fonctionnel. L'étude de la SdF nécessite donc au minimum une vue fonctionnelle, une vue structurelle et des informations concernant le lien entre les fonctions et leurs supports de réalisation.

Des modèles adaptés à la modélisation d'architecture à base de module....

Nous cherchons des modèles permettant de représenter l'organisation entre les éléments constitutifs d'un système : fonctions ou modules. Dans cette logique, nous nous sommes intéressés aux modèles permettant de représenter les architectures. Harmel, dans [Harmel, 07], propose un état non exhaustif des méthodes existantes et conclut sur le fait que pour représenter des architectures à base de modules, il est nécessaire de posséder un outil de modélisation visuel et simple d'utilisation. Ces deux critères vont dans le sens de nos besoins i.e. proposer un formalisme facile à prendre en compte par n'importe quel acteur projet.

...permettant le choix d'un niveau d'abstraction

Nous voulons pouvoir choisir le niveau d'abstraction du modèle tout en conservant la possibilité de raffinements pour mettre en évidence certaines parties du système. Le modèle doit donc permettre de représenter sous le même formalisme plusieurs niveaux d'abstraction.

Au stade de la conception, nous cherchons à modéliser l'architecture fonctionnelle, structurelle et les liens d'allocations entre ces deux espaces de réalisation. Dans [Dumas&al, 08], les auteurs proposent des définitions pour ces trois éléments, nous les présentons ci-dessous.
La représentation de l'architecture fonctionnelle consiste à décomposer les fonctions en sous-fonctions, en interaction par rapport aux données échangées. De façon formelle, l'architecture fonctionnelle peut être assimilée à un graphe orienté (F, AF) dans lequel les nœuds Fi représentent les fonctions et les arcs AFi→Fj les échanges de données de Fi à Fj. Sur le premier schéma de la Figure III-20, nous illustrons le cas de trois fonctions en série, chacune fournissant des données à la suivante, toutes les trois étant surveillées par une fonction supplémentaire.
De la même façon, l'architecture matérielle peut être vue comme un graphe orienté (BS, As) dans lequel les nœuds BS représentent les supports ou "Blocs Structurels" réalisant les fonctions et les arcs ASi → BSj représentent les connexions entre les différents blocs du système. Nous illustrons sur le deuxième schéma de la Figure III-20 l'exemple d'une architecture matérielle dans laquelle un composant central BS2 échange des données avec trois composants BS1, BS3 et BS4, ces quatre Blocs Structurels étant alimentés par un cinquième BS5.

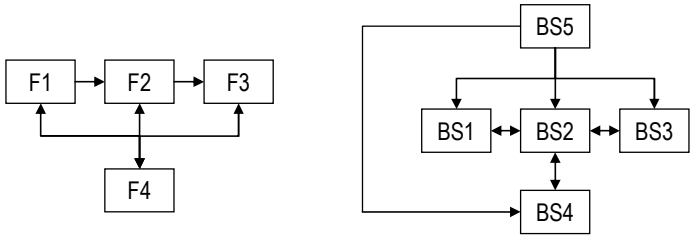


Figure III-20 : Architecture d'un système

La dernière information que l'on doit modéliser est la façon dont les fonctions sont supportées par les solutions

matérielles : on parle d'allocation quand on s'intéresse au lien fonction/matériel.

L'allocation peut être définie comme une application qui associe à chaque fonction F la ressource BS qui la réalise. Pour que cette allocation soit cohérente, il faut que les moyens de communication entre les ressources permettent le flot de données entre les fonctions.

Il existe différents types d'allocation entre les fonctions et les blocs structurels. En effet, comme proposé par l'auteur dans [Chakrabarti, 01], quatre types de relations sont possibles entre les fonctions et les blocs structurels qui les réalisent. Ces types de relations sont schématisés sur la Figure III-21.

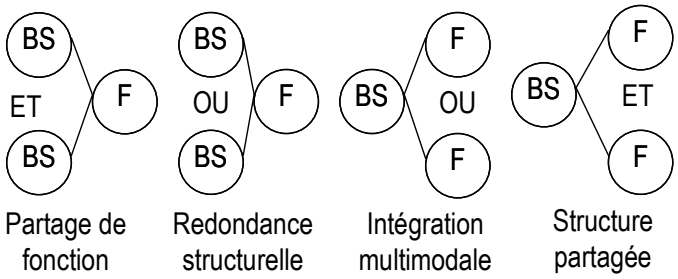


Figure III-21 : Types de relations entre fonctions et blocs structurels adaptés de [Chakrabarti, 01]

Dans [Jose-Flores, 05], l'auteur donne les caractéristiques de ces différentes relations :

- le partage de fonction correspond à l'utilisation de deux (ou plusieurs) composants pour la réalisation d'une fonction,
- la redondance structurelle correspond à la réalisation d'une fonction par un bloc structurel ou un autre,
- la relation intégration multimodale représente une organisation dans laquelle un composant peut assurer une fonction ou une autre,
- la relation structure partagée correspond à l'utilisation d'un composant dans deux fonctions (ou plus).

En généralisant cette proposition, cela correspond à matérialiser les allocations suivantes :

- une fonction réalisée par un bloc structurel,
- une fonction réalisée par plusieurs blocs structurels,
- un bloc structurel supportant plusieurs fonctions,
- plusieurs blocs structurels supportant plusieurs fonctions.

Il faut donc proposer une représentation supportant ces différents types d'allocations.

... tout en permettant à n'importe quel acteur projet de s'approprier le modèle

Les modèles généralement exploités par les acteurs projets sont des représentations « métier » : schéma électronique, plan mécanique, modèles UML pour le logiciel,... ; cependant, aucun de ces modèles n'intègre explicitement la vue SdF.

Afin d'éviter l'emploi de formalismes non familiers aux acteurs projet (usage de modèles éloignés des préoccupations métier), nous nous sommes concentrés, d'une part, sur les seuls modèles (ou éléments de modèles) existants et, d'autre part, sur les activités réalisées par le concepteur (étapes de son raisonnement présentées dans la partie formalisation du PRAO) lui permettant de lier une proposition de solution aux exigences client. Nous nous sommes appuyés simultanément sur des modèles de conception et sur les modèles de connaissances.

4.3. Choix d'un modèle de représentation des produits

Le choix du modèle de représentation des produits s'inscrit dans une démarche de modélisation de connaissance. [Ben-Ahmed, 05] définit la modélisation des connaissances comme : "*un processus de construction intentionnelle (résoudre des problèmes), à partir d'expérience (savoir-faire), informations et savoir, de modèles susceptibles de rendre intelligible (ayant un sens dans un contexte donné) cette connaissance et d'amplifier le raisonnement de l'acteur projetant une intervention délibérée sur elle pour résoudre des problèmes.*"

A notre niveau, nous cherchons un modèle permettant d'étudier la SdF en nous basant sur la connaissance des acteurs projet et en les adaptant à l'étude SdF permettant ainsi à l'acteur projet de traiter presque à son insu cette dimension. La notion d'étude de la SdF via les connaissances métier va dans le sens des idées proposées dans [Harmel&al, 06] où les auteurs expliquent que la conception de produits complexes fiables (tels que ceux considérés ici) passe par une explicitation de leur complexité et de leur organisation.

Il existe différents types de représentation d'architecture fonctionnelle ou structurelle. Nous proposons ici un aperçu des représentations possibles d'organisation de fonctions ou de blocs structurels. Nous discuterons ensuite de la modélisation de l'allocation des fonctions aux blocs structurels.

Dans [Harmel, 07], les travaux présentés traitent de la conception conjointe d'une architecture du produit et de l'organisation du projet associé. Dans ce cadre, l'auteur s'intéresse aux représentations existantes pour modéliser une architecture, qu'elle soit fonctionnelle ou structurelle :

- la modélisation par arborescence hiérarchique qui permet de décomposer un système en sous-systèmes jusqu'au composant de base (démarche identique pour les fonctions),
- les modèles de représentation de l'architecture fonctionnelle : d'un point de vue statique par le biais de diagrammes SADT (Structured Analysis Design Technique) pour la représentation des relations et flux entre fonctions, dynamique par le biais des diagrammes de flux fonctionnels, de diagrammes d'état ou de la méthode SA-RT par exemple,
- les modèles de représentation de l'architecture structurelle : les modèles à base d'arborescence permettant de décomposer successivement le produit en sous-systèmes successifs jusqu'à atteindre le niveau de détail souhaité ou les modèles graphiques comme les représentations par schémas-blocs par exemple.

Dans [Malmqvist, 02], l'auteur présente un panorama des méthodes à base de matrice (DSM[21]) réalisé dans le contexte du développement de produits complexes qui permet de fixer le principal objectif de ce type de méthodes : faciliter l'étude des interactions dans les systèmes complexes. Les problèmes suivants peuvent être résolus :

- l'analyse des interactions entre constituant d'un système,
- l'analyse de la conception,
- la modélisation des produits,
- l'étude de l'impact des modifications pour un produit.

Notons que les activités supportées par ce type de modèle correspondent tout à fait à celles que nous souhaitons mettre en place. La prise en compte de l'ensemble des contraintes s'exerçant sur la représentation du produit nous a fait

[21] DSM : Design Structure Matrix

converger vers l'étude des méthodologies matricielles qui répondent à tous nos besoins, notamment la matérialisation des relations entre les différentes entités manipulées.

Enfin, dans [Dekeyser, 05], l'auteur définit les différentes caractéristiques d'un modèle pour un système. Nous les reprenons une à une afin de montrer que la représentation matricielle répond bien à ces caractéristiques dans le cadre de nos besoins.

La première caractéristique est l'abstraction. Un modèle doit permettre d'éliminer des détails et de focaliser sur un point de vue du système ainsi que de travailler dans différentes échelles de complexité et de temps :

→ la représentation matricielle inclut la possibilité de définir différents niveaux d'abstraction, les éléments matérialisés dans les lignes et les colonnes pouvant être fonction de l'étude à réaliser (module, composant...).

La seconde caractéristique concerne l'analyse. Un modèle doit permettre l'étude des propriétés du système réel par extrapolation :

→ les informations modélisées dans les matrices, aux intersections lignes-colonnes, représentent le fonctionnement du système (échange de données, réalisation de fonction,...,) et la façon dont sont organisés les éléments qui le constituent ; on peut donc étudier le système réel par le biais de cette représentation.

La troisième caractéristique concerne la propriété de communication d'un modèle qui doit permettre la discussion et l'échange entre acteurs par la compréhension du modèle par tout le monde :

→ le modèle matriciel est un rendu de la théorie des graphes et, à ce titre là, est un support visuel que tout acteur projet peut s'approprier.

La dernière caractéristique concerne le fait que le modèle à choisir est fonction de l'objectif visé :

→ nous avons montré que le modèle matriciel répondait à toutes nos exigences et à tous nos besoins et nous faisons donc le choix de ce formalisme dans la suite des développements.

Nous proposons par la suite, une présentation des différentes méthodes matricielles ainsi que des différentes formes de matrices existantes.

5. Méthodes matricielles

5.1. Typologie des méthodes matricielles

On trouve, dans [Malmqvist, 02], une présentation des différents types de méthodes de modélisation à base de matrices. Nous reprenons son bilan sur les types de modélisation matricielle.

Il définit trois classes de matrices :

- les matrices au niveau élément dont l'objectif est de représenter les liens existants entre différents éléments d'un système ou projet, ces liens pouvant être définis entre des éléments de même type (cas des matrices intra-domaines) ou de type différent (cas des matrices inter-domaines),
- les matrices au niveau produit qui permettent de considérer dans les colonnes le système entier et non une décomposition de ce dernier (au contraire des matrices de la classe précédente), et dans les lignes des caractéristiques ou des propriétés du produit,
- les méthodologies matricielles qui ont pour particularité d'utiliser de façon définie un ensemble de méthodes matricielles pour la résolution de problèmes complexes.

Nous nous intéressons plus particulièrement aux matrices au niveau élément ainsi qu'aux méthodologies matricielles. Nous allons détailler les caractéristiques des matrices niveau élément ainsi que la façon dont nous les utilisons dans le cadre de la définition des modèles. Les méthodologies matricielles seront considérées dans le chapitre 4.

5.2. Matrices au niveau élément

Comme nous l'avons présenté dans le paragraphe 4.2, les relations à matérialiser sont des interactions Fonction/Fonction, Bloc Structurel/Bloc Structurel mais aussi les relations entre Fonction/Bloc Structurel qui matérialisent l'allocation des fonctions aux supports appropriés.

Les matrices éléments ont pour objectif la modélisation de lien entre éléments de même type ou de types différents.
La première catégorie, dénommée "matrice intra-domaine", a pour finalité la matérialisation des couplages entre éléments de même type (fonction, bloc structurel...) à différents niveaux d'abstraction (interaction dans le système complet, interaction entre composant d'un module,...).
La seconde catégorie, dénommée "matrice inter-domaine", a pour objectif la modélisation des liens entre éléments de différents types (fonction/bloc structurel,...).

Afin d'identifier les informations que nous rapporterons aux intersections lignes-colonnes des matrices, nous nous intéressons aux différents types de lien qui doivent être considérés ainsi qu'à la façon dont ces liens peuvent être modélisés. Dans [Malmqvist, 02], l'auteur définit deux familles d'interactions : les relations fonctionnelles et les relations intentionnelles de conception qui représentent des choix effectués durant le processus de conception :

- la première famille d'interactions concerne les relations de transfert (énergie, matériel ou information), les relations structurelles nécessaires au fonctionnement du système, les relations passives qui ne contribuent pas aux fonctions mais qui sont volontaires (mesures de protection, de surveillance,...,), les relations spatiales et de position ;
- la seconde famille concerne les relations d'allocation fonction/solution qui matérialisent la façon dont les solutions participent à une fonction donnée, les relations d'alternative qui modélisent la solution choisie dans le cas de solutions concurrentes, les relations de décomposition (par exemple, l'allocation des fonctions sur les différentes solutions), les relations comportementales (relation entre un composant et une propriété du produit : le poids, par exemple).

Enfin, Malmqvist définit les représentations envisageables pour ces liens dans les matrices :

- relations existantes ou non : matérialisées par la présence/absence d'un symbole ou par la présence d'un 1/0 selon qu'il existe une relation ou non,
- texte descriptif : description de la raison pour laquelle le lien existe (transfert des signaux de X vers Y,...),
- relations d'alternative : représentation des éléments de solutions possibles pour une fonction par exemple,
- importance qualitative de la relation : nécessaire, optionnelle, recommandée,...,
- importance quantitative selon une échelle déterminée : -3,-2,..,+1,+2,...

Nous venons de présenter les différents liens modélisables dans les matrices. Nous considérons maintenant les liens que nous souhaitons modéliser dans les matrices intra-domaine et inter-domaine.

5.2.1. Matrices intra-domaine

Dans cette famille, nous modélisons les liens Fonction/Fonction et Bloc Structurel/ Bloc Structurel.

Plusieurs types de matrices intra-domaines ont été définis. Nous présentons rapidement ces différents types puis nous développerons ceux qui nous paraissent pertinents pour notre étude. Dans un premier classement, deux types de matrices sont distinguées :

- les matrices symétriques lorsque la matrice n'a pas de sens de lecture, ces matrices sont appelées « matrices statiques »,
- les matrices asymétriques lorsque les éléments en interactions doivent être hiérarchisés ou lorsqu'il existe des relations d'ordre entre ces éléments de types précédence (i.e. ordonné), on parle alors de « matrice temporelle ».

La modélisation la plus simple consiste à utiliser des matrices binaires [Harmel, 07] de façon à matérialiser l'existence ou non d'un lien. Ces matrices peuvent être symétriques (équivalent à des graphes non orientés) ou non symétriques (permettant la modélisation de relation de hiérarchie, de précédence,...,). Nous présentons, sur la Figure III-22, les liens modélisables.

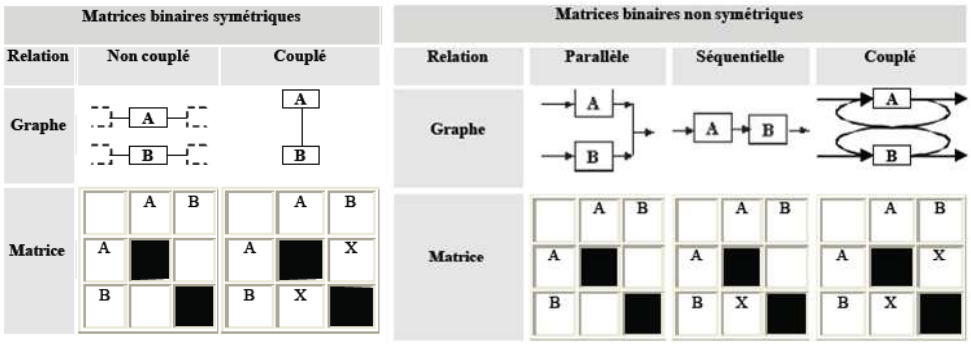


Figure III-22 : Modélisation des liens par matrices binaires[22]

A partir des liens modélisables par le biais des matrices binaires, nous analysons les liens correspondant dans le cas de liens fonctionnels puis de liens structurels.

Tout d'abord, deux éléments semblables peuvent être liés par une relation fonctionnelle. Comme nous l'avons vu au début du paragraphe 5.2, ce type de relation inclut les fonctions de transfert : information, énergie, matériel. De plus, les interactions dans un produit (fonctionnel et structurel) d'après les auteurs, dans [Eppinger&al, 94], peuvent être définies par un vecteur à quatre dimensions à valeur binaire : la première dimension est spatiale, la seconde concerne le transfert d'énergie, la troisième le transfert d'information et la dernière le transfert de matériel.

Nous adaptons ces interactions au cas des fonctions que nous considérons. Deux fonctions F1 et F2 peuvent être liées par un lien de type :

- échange d'informations : soit F1 envoie des informations à F2, soit F2 envoie des informations à F1, soit F1 et F2 échangent mutuellement des informations,
- assistance : F1 peut être alimentée par F2 (transfert d'énergie) et inversement, ou, F1 peut transférer à F2 de l'énergie.

[22] Les croix aux intersections ligne-colonne peuvent être remplacées par des « 1 », il faut alors placer des « 0 » aux intersections vides.

- surveillance : F1 peut contrôler F2 dans le cadre de la sécurité du système (par rapport à la cohérence des informations reçues ou à un état de certaines variables par exemple).

Ces trois formes d'interactions sont les seules que nous avons identifiées pour les produits étudiés.

Nous considérons maintenant les interactions entre modules. Comme précédemment, à partir des types de relations définis, deux blocs structurels BS1 et BS2 peuvent être liés par des liens de type :

- échange d'informations : de BS1 à BS2, de BS2 à BS1 ou de façon mutuelle,
- assistance : BS1 peut alimenter BS2 et inversement (transfert d'énergie),
- surveillance comme précédemment,
- redondance : deux blocs structurels dont l'un se substitue à l'autre en cas de défaillance de ce dernier,
- spatial (i.e. relation spatiale) : BS1 est lié physiquement à BS2 soit fonctionnellement (lien nécessaire au fonctionnement), soit de façon optionnelle (protection,...,).

Après l'étude des relations existantes dans les matrices intra-domaines, nous considérons maintenant l'étude des matrices inter-domaines.

5.2.2. Matrices inter-domaines

Ce type de matrice consiste à modéliser les allocations ou les choix de conception effectués, i.e. la manière avec laquelle les fonctions vont être réalisées par les blocs structurels.

Nous reprenons les relations présentées au paragraphe "matrice niveau élément",

Parmi les relations de type allocation fonctions/solutions, les relations peuvent représenter :

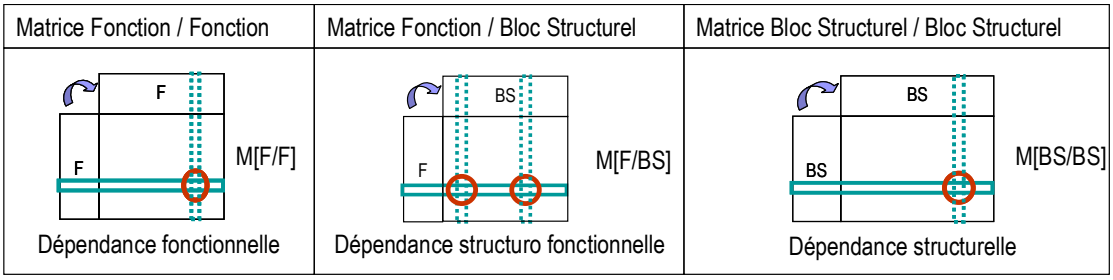
- la manière avec laquelle chaque bloc participe à la fonction,
- les alternatives de choix.

Dans notre cas, nous cherchons à identifier le rôle de chaque bloc structurel dans la réalisation de la fonction. Nous considérons qu'il existe des interactions de type :

- réalisation : la fonction nécessite le bloc structurel pour être réalisée,
- assistance : le bloc structurel ne réalise pas directement la fonction mais est nécessaire aux blocs qui la réalisent (exemple : alimentation),
- option : le bloc structurel n'est pas strictement nécessaire à la fonction mais il est volontairement introduit : protection de la fonction, surveillance,...

5.3. Choix de modélisation des interactions et notations utilisées

Nous allons présenter les notations que nous utiliserons dans la suite du document pour les différents types de matrices. De plus, nous souhaitons faire apparaître dans les matrices intra-domaines des relations orientées. Pour cela nous faisons le choix d'utilisation des matrices temporelles pour lesquelles nous devons définir le sens de lecture. Nous indiquons sur la Figure III-23 les notations choisies ainsi que le sens de lecture (des lignes vers les colonnes).



$I_{Ei \rightarrow Ej}$ signifie l'intersection entre la ligne contenant l'élément i et la colonne contenant l'élément j

Figure III-23 : Notation et sens de lecture des matrices

Le second choix concerne la modélisation des liens : soit à partir de la notation 0 et 1 traduit l'existence ou non d'un lien, soit par l'exploitation de davantage d'informations pouvant être formulées via les composantes d'un vecteur de lien. Nous retenons cette deuxième approche et décrivons les vecteurs en deux temps.

Tout d'abord, nous nous intéressons aux liens dans les matrices intra-domaine (Fonction/Fonction et Bloc Structurel/Bloc Structurel) qui caractériseront des relations de dépendance ou des relations d'ordre. Ensuite, nous définirons les relations de composition ou d'allocation pour les matrices inter-domaines (Fonction/Bloc Structurel).

5.3.1. Relations Fonctions/Fonctions et Blocs Structurels / Blocs Structurels

Nous caractérisons les liens existant entre deux fonctions ou deux blocs structurels à l'aide de vecteur de caractérisation à n composantes. Chaque composante représente une caractéristique du lien nécessaire à la compréhension du fonctionnement et de l'architecture du produit respectivement dans les matrices M[F/F] et M[F/BS]. Les relations existantes entre des éléments de même nature sont soit des relations d'ordre soit des relations de dépendance.

Le nombre et le type des composantes du vecteur de caractérisation dépendent directement du type de problème considéré. Nous présentons les composantes que nous définissons pour notre problématique. Le vecteur comporte trois composantes qui suffisent à caractériser les liens existant entre les fonctions et les blocs structurels auxquels nous nous intéressons.

Au niveau fonctionnel, le vecteur défini noté [L T N] est constitué de trois composantes :

- la première composante L indique s'il existe un lien entre deux fonctions et le sens de ce lien : L = 2 si le lien est bidirectionnel, L = 1 à l'intersection $I_{Ei \rightarrow Ej}$ si le lien existe de Ei vers Ej et L = 0 à l'intersection $I_{Ei \rightarrow Ej}$ si le lien existe de Ej vers Ei,
- la seconde composante T définit le type du lien : T = I à l'intersection $I_{Ei \rightarrow Ej}$ dans le cas où Ei envoie des informations à Ej, T = E dans le cas où Ei envoie de l'énergie à Ej et T = E/I dans le cas où Ei envoie des informations et de l'énergie à Ej,
- la troisième composante N définit la (ou les) nature(s) du lien et peut comporter deux informations. La première concerne l'existence du lien pour la réalisation R ou l'assistance A et la seconde l'existence d'un lien pour la sécurité S, le contrôle C ou la protection P. S'il existe les deux composantes, il y en a forcément une égale à R ou A, la seconde à S, C ou P, cette grandeur est notée N = R/S pour un lien de réalisation et de sécurité par exemple.

Nous illustrons sur la Figure III-24 différents vecteurs de caractérisation.

	Fournir les données à l'application client (F1)	Envoyer les commandes aux actionneurs (F2)	Alimenter (F3)	Sécuriser (F4)
Fournir les données à l'application client (F1)		[1 I R/.]	[0 . A/.]	[2 I ./C]
Envoyer les commandes aux actionneurs (F2)	[0 . R/.]		[0 . A/.]	[2 I ./C]
Alimenter (F3)	[1 E A/.]	[1 E A/.]		[2 E/I A/C]
Sécuriser (F4)	[2 I ./S]	[2 I ./S]	[2 I ./S]	

Figure III-24 : Exemple de vecteurs de caractérisation dans M[F/F]

Nous décrivons les vecteurs de la première ligne de la matrice :

- entre Fournir les données à l'application client et Envoyer les commandes aux actionneurs, il existe un lien unidirectionnel de F1 vers F2 (L=1), d'envoi d'information (T=I) dans le cadre de la réalisation de la mission (N=R/.),
- entre Fournir les données à l'application client et Alimenter, il existe un lien unidirectionnel de F3 à F1 (L=0) pour l'assistance de la fonction (N=A/.),
- entre Fournir les données à l'application client et Sécuriser, il existe un lien bidirectionnel (L=2) d'envoi d'information de F1 vers F4 (T=I) pour le contrôle de la fonction (N=./C).

Dans cet exemple, toutes les intersections comportent un vecteur de caractérisation ; s'il n'existe pas de lien entre deux éléments alors l'intersection correspondante est vide.

Au niveau structurel, on retrouvera des liens identiques. Nous les illustrons sur la Figure III-25

	Dispositif de mise en forme des entrées BS1	Microcontrôleur BS2	Driver de sortie BS3	Alimentation BS4	Superviseur BS5
Dispositif de mise en forme des entrées BS1		[1 I R/.]		[0 . A/.]	[0 . ./S]
Microcontrôleur BS2	[0 . R/.]		[1 I R/.]	[0 . A/.]	[0 . ./S]
Driver de sortie BS3		[0 . R/.]		[0 . A/.]	[0 . ./S]
Alimentation BS4	[1 E A/.]	[1 E A/.]	[1 E A/.]		[2 E A/.]
Superviseur BS5	[1 I ./S]	[1 I ./S]	[1 I ./S]	[2 I ./S]	

Figure III-25 : Exemple de vecteurs de caractérisation dans M[BS/BS]

Dans la matrice précédente, nous détaillons les vecteurs de la ligne correspondant au Microcontrôleur BS2 :

- entre BS2 et le Dispositif de mise en forme des entrées BS1, il existe un lien unidirectionnel de BS1 vers BS2 (L=0) dans le cadre de la réalisation de la mission (N=R/.),
- entre BS2 et le Driver de sortie BS3, il existe un lien unidirectionnel de BS2 vers BS3 (L=1) d'envoi d'information (T=I) dans le cadre de la réalisation (N=R/.),
- entre BS2 et l'alimentation BS4, il existe un lien unidirectionnel de BS4 vers BS2 pour l'assistance de la fonction (N=A/.),
- entre BS2 et le superviseur BS5, il existe un lien unidirectionnel de BS5 vers BS2 (L=0) dans un objectif de sécurité (N=./S).

Le vecteur que nous avons défini dans le cadre de l'application comporte seulement trois composantes. Au niveau d'abstraction retenu pour le PRAO, ces trois composantes suffisent à la description des liens existants mais on peut envisager la définition de nouvelles composantes soit pour une application différente, soit pour une analyse à un niveau de détail plus important.

Nous avons développé les vecteurs de caractérisation propres aux matrices intra-domaines M[F/F] et M[BS/BS], nous considérons maintenant les matrices inter-domaines M[F/BS].

5.3.2. Relations Fonctions/Blocs Structurels

Les matrices inter-domaines considérées dans l'application ont la particularité de représenter des liens de composition ou allocation des Fonctions sur les Blocs Structurels. Un vecteur à n composantes caractérise le lien entre une Fonction et le(ou les) Bloc(s) Structurel(s) qui participe(nt) à sa réalisation.

Dans le cas de l'application, seule une composante est considérée car elle suffit à la caractérisation des liens F/BS. Le vecteur défini est noté [N] et la composante N peut comporter deux informations i_1/i_2 :

- la première information i_1 représente l'existence d'un lien de réalisation R ou d'assistance A du BS envers la fonction ; si la fonction est réalisée par le BS i_1 est égale à R, si la fonction est assistée alors i_1 est égale à A,
- la seconde information i_2 représente l'existence d'un autre type de lien et est égale à S si le BS sécurise la fonction, à P s'il la protège, à D s'il détecte les défaillances de celle-ci ou à C s'il en contrôle le fonctionnement.

La notation utilisée est N = (R ou A ou .)/(S ou C ou P ou D ou .) comme illustré sur la Figure III-26 dans laquelle nous présentons une matrice simplifiée M[F/BS]

	Dispositif de mise en forme des entrées BS1	Microcontrôleur BS2	Driver de sortie BS3	Alimentation BS4	Superviseur BS5
Fournir les données à l'application client (F1)	[R/.]	[R/.]		[A/.]	[./S]
Envoyer les commandes aux actionneurs (F2)		[R/.]	[R/.]	[A/.]	[./S]
Alimenter (F3)				[R/.]	[./S]
Sécuriser (F4)				[A/.]	[R/.]

Figure III-26 : Exemple de vecteurs de caractérisation dans M[F/BS]

Dans la matrice simplifiée proposée, nous prenons l'exemple de la fonction F1 dont l'allocation sur les différents blocs est caractérisée sur la première ligne : F1 est réalisée par BS1 et BS2, assistée par BS4 et sécurisée par BS5.

Après avoir présenté les matrices intra-domaine et inter-domaines que nous avons développées dans le cadre de la problématique, précisons que d'autres matrices peuvent être utilisées dans la même logique d'emploi pour caractériser les liens Fonctions/Sous-Fonctions et Blocs structurels/Composants. Ces deux types de matrices apporteraient des informations sur l'organisation fonctionnelle et la composition du système et permettraient de passer d'un niveau d'abstraction à un autre. Même si les éléments considérés sont de même nature, les liens concerneraient plutôt des liens de composition permettant l'identification de sous-fonctions ou de composants critiques dans une application donnée.

Nous avons présenté des exemples de matrices simplifiés, les matrices complètes seront développées dans le chapitre 4.

5.4. Modélisation des connaissances et du savoir-faire

Nous avons insisté sur le fait que les modèles que nous définissons ont pour principal objectif d'exprimer la connaissance implicite des acteurs projets (ainsi que leur savoir-faire) afin de pouvoir « projeter » sur cette dernière la dimension sûreté de fonctionnement requise par le client. Les modèles produits présentés jusqu'ici permettent de formaliser les connaissances et les décisions prises par le concepteur dans la définition d'une architecture structurelle. Pour consigner l'ensemble des connaissances et du savoir-faire des acteurs, il faut pouvoir formaliser les différentes étapes réalisées durant le PRAO depuis l'analyse du CdC client à la sélection d'une solution particulière pour un BS donné.
Nous allons définir les notions que nous venons d'introduire puis nous identifierons les connaissances qui, par rapport à celles déjà formalisées par les étapes précédentes, restent à formaliser.

Tout d'abord, nous replaçons le concept de connaissance par rapport aux notions de donnée et d'information [Cortes-Robles, 06]. Une donnée est un résultat : un nombre, un schéma, une figure sans contexte (dans notre cas : une fonction ou un bloc structurel, par exemple). Une information est générée par l'interprétation des données (exemple : le modèle fonctionnel). Une information possède un contexte précis et permet l'acquisition de connaissance, c'est un moyen (ou support) permettant de produire de la connaissance. Enfin, la connaissance est créée par les flux d'informations et leurs interprétations par l'action humaine. [Tounkara, 02] propose une autre définition de la connaissance qui est : "*un ensemble de savoirs et savoir-faire mobilisés par les acteurs dans le cadre de leur activité*". Nous adhérons à cette définition car elle pose le fait que l'acteur projet doit être intégré à la réflexion puisque c'est lui qui détient la connaissance. Le savoir-faire, lui, représente la manière suivant laquelle pourra être créée la connaissance. Enfin, la dernière notion est celle de "compétence". Dans [Boumane&al, 06], les auteurs confrontent différentes définitions de la compétence. La définition qui en résulte présente la compétence comme "*la capacité d'une personne (acteur) à agir et réagir avec la pertinence requise pour réaliser une activité dans une situation de travail. L'acteur est au cœur d'un processus qui consiste à sélectionner, combiner et mobiliser ses connaissances, son savoir-faire, ses aptitudes et comportements d'une part, et des ressources de l'environnement d'autre part, en vue d'accomplir une mission définie par l'entreprise*". L'intérêt de cette définition réside dans le lien entre la connaissance et la compétence. La compétence consiste, en effet, en l'utilisation des connaissances des acteurs dans un contexte particulier pour une mission donnée. En proposant à l'acteur un mode d'expression et de formalisation de la connaissance implicite, on facilitera le développement et l'acquisition des compétences en SdF.

Jusqu'ici, nous avons formalisé les connaissances concernant :

- l'analyse du CdC client via le filtrage,
- le choix des fonctions via la matrice M[F/F],

- les choix de composition ou d'allocation via la consignation dans la matrice M[F/BS] des supports BS réalisant les fonctions,
- le choix de l'architecture matérielle via la matrice M[BS/BS].

Il manque ici la connaissance concernant la sélection de la solution particulière pour un BS donné ainsi que la connaissance disponible sur ce dernier. Dans l'objectif de terminer la formalisation des connaissances disponibles, nous avons analysé les blocs structurels pour identifier les connaissances mobilisées pour sa définition.

Cette étude nous a orientés vers la définition d'attributs permettant de capitaliser l'ensemble de la connaissance métier et SdF sur les BS.

Les attributs que nous définissons sont de deux types. Certains explicitent les connaissances métiers mobilisées pour la sélection du bloc et des informations sur le bloc, d'autres les connaissances et informations SdF disponibles. Nous avons identifié huit attributs pour la problématique considérée mais leur nombre peut être étendu pour formaliser une connaissance ou une information supplémentaire.

Nous présentons les attributs sur la Figure III-27 puis nous les détaillons.

	Bloc i	Commentaires
1	Paramètres de choix	Attribut pouvant être indépendant de la dimension SdF
2	Solution Standard	Solution de base répondant aux spécifications techniques sans considération de sécurité
3	Variantes	Solutions existantes prenant en compte les spécifications SdF (fiabilité + élevée, prise en compte position de repli..)
4	Coût du BS standard	Coût de la solution standard
5	Coût SdF	Coût SdF du BS
6	Fiabilité et/ou λ (prévisionnelle)	$\lambda = \sum \lambda$ (composants du BS)
7	Défaillances	Liste de défaillances connues sur le bloc considéré
8	Moyens de détection et DC associé	Mécanismes de détection de défaillance implémentables sur le bloc et couverture de diagnostic associé aux mécanismes

Figure III-27 : Attributs des Blocs Structurels

L'attribut 1 concerne les paramètres de sélection de la solution, ces paramètres sont fonctions des performances techniques à atteindre.

L'attribut 2 concerne la description de la solution la plus élémentaire permettant de répondre aux spécifications techniques i.e. la configuration de base nécessaire.

L'attribut 3 décrit l'ensemble des solutions existantes et déjà utilisées sur des produits précédents.

L'attribut 4 concerne l'information sur le coût du BS pour la solution standard identifiée dans l'attribut 2.

L'attribut 5 informe sur le coût SdF des différentes variantes en général et pour le cas d'un AO donné sur le coût SdF du BS sélectionné.

L'attribut 6 définit le taux de défaillance des différentes variantes existantes en général et sur le taux de défaillance du BS sélectionné pour un AO particulier. Cet attribut est une estimation de fiabilité calculée à partir des taux de défaillance des composants constitutifs du BS sélectionné.

L'attribut 7 renseigne sur les défaillances connues d'un BS particulier par la mise en évidence des défaillances connues et déjà rencontrées sur le bloc considéré par utilisation des projets précédents et, plus particulièrement, les analyses SdF précédentes : AMDEC,...

L'attribut 8 renseigne sur les moyens de protection, de détection ou les barrières de sécurité existant pour le type de BS considéré. Ces éléments peuvent notamment être extraits des expériences passées ou des normes relatives à la sécurité.

Nous donnons sur la Figure III-28 un exemple des attributs définis dans le cas de l'Alimentation du système et de son Microcontrôleur :

	Exemple 1 : Alimentation	Exemple 2 : Microcontrôleur
1	tension à fournir et état de sécurité	Puissance de calcul, capacité mémoire interne, nombre d'entrées du convertisseur A/D
2	1 régulateur/1 alimentation produit et 1 alimentation capteurs	Microcontrôleur type 1
3	2 régulateurs / 2 alimentations produit et 1 alimentation capteur	Microcontrôleur type 2 Microcontrôleur type 3
4	c1	c2
5	Csdf1	Csdf2
6	$\lambda = \sum \lambda$ (composants du BS)	$\lambda = \sum \lambda$ (composants du BS)
7	perte régulateur, perte tension batterie, perte alimentation	Perte convertisseur, perte mémoire interne, perte horloge interne
8	vérification de la tension batterie (entrée)/DC Low vérification de la tension à la sortie du régulateur/DC	test par la partie électronique/DC medium test par le logiciel avec échange d'informations entre deux unités indépendantes/DC medium test par le logiciel intégré au microcontrôleur avec un nombre limité de motifs/DC low …

Figure III-28 : Exemples d'attributs de l'Alimentation et du Microcontrôleur

Les connaissances et informations disponibles via les attributs sont obtenues par :

- les bases de données internes d'une entreprise,
- les outils d'estimation de coût,
- les normes de sécurité ou autres normes relatives aux produits considérés,
- les connaissances d'experts,
- le savoir-faire des acteurs de l'entreprise,
- le retour d'expérience sur les projets antérieurs, etc.

Nous avons présenté l'ensemble de la connaissance modélisée pour pouvoir définir et évaluer l'impact SdF. Il nous semble important de souligner ici que les modèles peuvent, outre leur utilisation pour l'évaluation de la valeur d'impact, servir pour l'étude du fonctionnement du système ou comme support à la réflexion du concepteur.
Notons aussi que la modularité des modèles proposés permet, notamment pour les systèmes considérés qui peuvent avoir différentes configurations, la modélisation d'une panoplie de situations différentes (ajout d'un BS, redondance d'un BS,…).

6. Conclusion

L'analyse des produits existants au sein de l'entreprise ainsi que des projets consacrés aux systèmes embarqués automobile a permis de mettre en évidence les principales caractéristiques de ces produits et d'expliciter des modèles

parfois non formalisés ou informels tel que celui de l'analyse fonctionnelle. A partir de la connaissance explicitée sur les produits, nous nous sommes intéressés aux représentations pouvant intégrer l'ensemble de cette connaissance pour déboucher sur le choix de modèles matriciels fonctionnels, structurels et structuro-fonctionnels complétés par les connaissances formalisées sous la forme d'attributs pour chaque type de Bloc Structurel.

L'ensemble de ces modèles fixe la connaissance jusque là implicite des acteurs projets ce qui facilitera l'acquisition et la formalisation de la compétence SdF jusque-là "masquée" dans les connaissances métiers. Le paramétrage des différents modèles permet de plus à ces derniers d'être adaptés à l'ensemble des projets développés dans l'entreprise et aux évolutions futures par l'adaptation des modèles (ajout de BS, modification des liens entre BS, etc). Ces modèles de haut-niveau, nécessaires au PRAO, pourront aussi être utilisés durant le développement en considérant des entités plus petites (une partie d'un bloc structurel par exemple).

Ces modèles sont évolutifs tant sur les modifications futures des produits que sur l'ajout de connaissances. En effet, les composantes des vecteurs de caractérisation non utilisées ici peuvent être définies pour un problème particulier, les éléments présents dans les matrices peuvent être différents, l'analyse des produits menés ici servant de méthodologie au développement de ces matrices pour des produits différents. Enfin, les attributs peuvent être adaptés pour des produits différents : ajout, suppression d'attributs non pertinents, etc.

Les matrices utilisées ici pour la modélisation de la structure et du fonctionnement des produits peuvent être utilisées à d'autres fins telles que la décomposition du produit à un niveau de détail supplémentaire via des matrices (à définir) Fonctions/Sous-Fonctions ou Blocs Structurels/Composants pour l'analyse d'une sous-fonction ou d'un composant critique.

Le dernier élément que nous souhaitons mettre en relief ici est l'utilisation de composantes dans les vecteurs de caractérisation relatives aux attributs. Il peut être envisagé de définir des composantes contenant des "mathématiques" d'association des attributs en fonction du lien reliant les deux éléments. L'exemple le plus simple consiste à associer les taux de défaillance en fonction du lien. Par exemple, dans M[F/BS] il peut être calculé la somme des taux de défaillance des BS réalisant ou assistant la fonction et à les associer sous la forme d'un facteur aux BS réalisant le contrôle ou la sécurité de la fonction.

Jusque ici, nous avons défini l'organisation du processus de réponse à appel d'offre (chapitre 2), les supports nécessaires à cette organisation (chapitre 2 et 3). Dans le chapitre suivant, nous appliquons les concepts définis jusqu'ici afin d'obtenir l'impact des exigences SdF sur le produit et la démarche à mettre en place.

IV. Chapitre 4 : Instrumentation des étapes Projection et Evaluation pour la définition de l'impact du traitement des exigences SdF sur le projet

1. Introduction

L'objectif de ce chapitre est de présenter la méthodologie matricielle développée afin d'évaluer l'impact de la prise en compte des exigences SdF dans un projet nommé "Impact SdF" par la suite. Plus précisément, nous présentons ici les modes d'utilisation des supports d'instrumentation introduits précédemment dans l'objectif d'exprimer l'impact SdF. Il s'agit donc de mettre en application les étapes Projection et Evaluation.
Il faut, dans cette optique, définir plus formellement la notion d'impact SdF ainsi que les attributs et grandeurs qui permettront son évaluation ; les trois composantes à prendre en compte sont la fiabilité, la sécurité du produit et la démarche de gestion de la SdF.

Les développements concernent la proposition d'une méthodologie matricielle permettant de projeter sur le produit et son développement futur les conséquences de la prise en compte de la SdF dans un projet. La méthodologie doit permettre d'analyser les principaux mécanismes de défaillance du produit à partir des modèles disponibles dans le PRAO. Ces développements complètent l'instrumentation de l'organisation du PRAO à l'aide des supports de connaissance. Nous avons en effet présenté dans le chapitre 2 l'instrumentation des étapes Filtrage, Traduction et Restitution. Le chapitre 3 a ensuite permis de développer les supports nécessaires à l'instrumentation des étapes Projection et Evaluation. Nous exposons finalement ici les principes de couplage entre les supports et les étapes Projection et Evaluation dans le cadre de l'instrumentation de ces étapes.

L'objectif de cette partie est double. Il s'agit tout d'abord de présenter, par le biais des étapes Projection et Evaluation, la méthodologie d'utilisation des matrices destinée à établir une valeur d'impact de la prise en compte des exigences sûreté de fonctionnement. Il s'agit ensuite d'illustrer par des exemples ces deux étapes clés (exemples qui seront présentés au fur et à mesure de la description de la méthodologie).

Le chapitre est organisé en quatre parties. Nous proposons d'abord une présentation générale de l'instrumentation des étapes Projection et Evaluation et un rappel des supports utiles pour ces étapes. Nous définissons ensuite les différents types d'impact ainsi que les grandeurs qui permettront de les évaluer. Nous explicitons les relations existant entre les impacts à définir et les modèles proposés dans le chapitre 3 qui permettront de faire le lien entre les exigences clients et les supports dont nous disposons. Enfin, nous présentons la méthodologie matricielle permettant la définition

de l'impact SdF suivie de la présentation de la méthode d'évaluation de cet impact.

2. Instrumentation des étapes Projection et Evaluation

L'instrumentation de l'étape Projection a pour objectif de permettre la définition de l'impact SdF. Le travail préliminaire pour atteindre cet objectif concerne le paramétrage des matrices présentées dans le chapitre précédent. Nous proposons ici les supports considérés pour les étapes Projection et Evaluation (Figure IV-1).

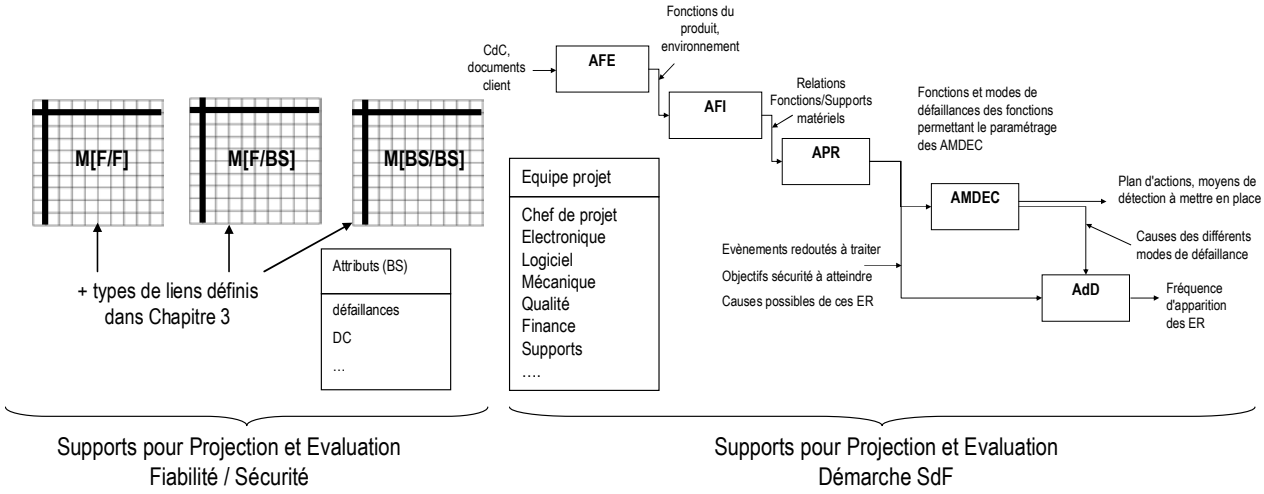


Figure IV-1 : Supports utilisés dans les étapes Projection et Evaluation

Nous utiliserons les matrices permettant d'analyser le produit ainsi que les liens de dépendance entre les éléments définis aux intersections entre lignes et colonnes de chaque matrice (nous montrerons par la suite la méthode de paramétrage de ces matrices). Les attributs rattachés aux différents blocs structurels seront eux aussi utilisés notamment dans l'analyse de la fiabilité et de la sécurité. Pour l'analyse de la démarche SdF à mettre en place, nous utiliserons les informations relatives à la démarche présentée dans le chapitre 2 et à la composition de l'équipe projet définie dans le chapitre 1.

Nous proposons sur la Figure IV-2 une vue d'ensemble de la méthode permettant la définition et l'évaluation des conséquences de la prise en compte des exigences SdF.

Paramétrage Matrices	Analyse fiabilité	Analyse Sécurité	Evaluation démarche	Evaluation impact produit
1.2. M[F/F]	2.1. Evaluation PPM	3.1. Calcul λ_{RF}	4.1. AFE	5.1. Coût Elec.
1.2. M[F/BS]	2.2. Evaluation λ	3.2. Fonctions	4.2. AFI	5.2. Coût Logiciel
1.3. M[BS/BS]		3.3. ER	4.3. APR	5.3. Coût Méca.
1.4. Attributs		3.4. Analyse TR	4.4. AMDEC	
		3.5. Mode commun	4.5. AdD	

Figure IV-2 : Présentation générale Projection et Evaluation

Les étapes Projection et Evaluation sont organisées en cinq étapes successives contenant différentes activités qui sont décrites sous une forme abrégées sur la figure précédente. Nous présenterons ces activités dans le détail par la suite.

La méthodologie s'appuiera également sur les supports introduits au chapitre 2 et que nous rappelons ici :

- supports normatifs S_N :
  - norme de sécurité fonctionnelle en vigueur IEC61508 [IEC 61508],
  - norme ISO 26262 (à paraître fin 2009/début 2010 mais déjà considérée par les constructeurs), déclinaison de la norme IEC61508 instanciée au contexte automobile [ISO 26262],
- supports procéduriers S_P :
  - démarche SdF entreprise (présentée de façon générale mais à instancier en fonction du contexte considéré),
  - procédures relatives au déploiement des méthodes de sûreté de fonctionnement (AMDEC, APR, …),
- supports métiers S_M :
  - schémas de solutions existantes,
  - modèles métiers,
- supports d'expériences S_E :
  - outil de chiffrage des différents coûts d'un produit,
  - bases de données fiabilité de l'entreprise (si existantes) ou supports équivalents (FIDES, UTEC,...,),
  - études SdF précédentes,
  - listes de défaillances,...,

Cette présentation générale de la démarche et des supports à sa réalisation permet de positionner les différents éléments développés par la suite.

3. Exigences à traiter

Les exigences que nous considérons dans le cadre de la problématique abordée sont de trois types : objectifs de fiabilité, objectifs de sécurité et exigences sur les méthodes de gestion préconisées pour répondre à ces objectifs. Avant de présenter la démarche complète, nous rappelons les trois types d'exigences à traiter ainsi que les grandeurs associées. Nous rappelons aussi, dans cette partie, les supports identifiés au chapitre 2 qui seront utilisés.

3.1. Objectifs de fiabilité

Nous avons rappelé la définition de la fiabilité dans le paragraphe 4.2.1 du chapitre 1. Par rapport au taux de défaillance du produit évaluée, lorsque le produit n'est pas encore en utilisation, par le biais de méthodes de fiabilité prévisionnelle, on peut calculer le taux de pièces par million (généralement employée dans l'industrie l'automobile) et peut être évaluée, lorsque le produit n'est pas encore en utilisation, par le biais de méthodes de fiabilité prévisionnelle. Nous proposons, dans cette partie, les différents moyens existants pour l'évaluation de ce type d'objectif.

Lorsqu'on s'intéresse à la fiabilité prévisionnelle, les grandeurs utilisées seront les taux de défaillance (notamment le taux de défaillances par heure, noté FIT par la suite pour Failure in Time). Afin de pouvoir calculer des grandeurs de fiabilité prévisionnelle, il faut disposer, pour chaque famille de produit, d'un profil de mission type. Ce profil de mission permet de calculer ensuite, pour chaque type de composants électroniques (composant passif, actif, etc.), un taux de défaillance prévisionnel comme présenté sur la Figure IV-3.

		Taux de défaillances (en défaillances par heure)		
Type de composants	Composants	Profil de mission ABS	Profil de mission direction assistée	Profil de mission Suspension
Passif	Résistances	λ1-1	λ1-2	λ1-3
	Capacités	λ2-1	λ2-2	λ2-3
	Oscillateur	λ3-1	λ3-2	λ3-3
	Quartz	λ4-1	λ4-2	λ4-3
	...	...	...	...
Actif	Comparateur	λ5-1	λ5-2	λ5-3
	Amplificateur	λ6-1	λ6-2	λ6-3
	Microcontrôleur	λ7-1	λ7-2	λ7-3
	Mémoire	λ8-1	λ8-2	λ8-3
	Diode	λ9-1	λ9-2	λ9-3
	Régulateur	λ10-1	λ10-2	λ10-3
	...	...	...	...
Opto-composant	LED	λ11-1	λ11-2	λ11-3
	Optocoupleur	λ12-1	λ12-2	λ12-3
	Composant photo-sensitif	λ13-1	λ13-2	λ13-3
Electromécanique	Relais	λ14-1	λ14-2	λ14-3
	Interrupteur	λ15-1	λ15-2	λ15-3
	Transformateur	λ16-1	λ16-2	λ16-3
	...	...	...	...

Figure IV-3 : Table des taux de défaillances prévisionnels

Cette table comporte les composants principaux considérés dans les applications automobiles ; le microcontrôleur figure ici parmi les composants alors qu'il apparaît dans le reste du document en tant que bloc structurel dans la mesure où son taux de défaillance est celui d'un composant actif.

Nous avons défini dans le chapitre 1 quatre familles de produits alors qu'il n'apparaît ici que trois profils de mission. Cela s'explique par le fait que les trois familles de produits citées ici correspondent au cœur de métier de l'entreprise partenaire. Pour la dernière famille correspondant aux produits n'appartenant pas aux trois premières, nous pourrons soit utiliser des informations précédemment établies au niveau des composants ABS, Direction Assistée ou Suspension soit recalculer les taux de défaillances par rapport à la définition d'un nouveau profil de mission.

La connaissance du taux de défaillance de chaque type de composant constituant un bloc structurel et leur nombre permet d'obtenir le taux de défaillance d'un bloc structurel, on peut écrire :

$$\lambda_{BS} = \sum_{composants \in BS} \lambda_{composant} \qquad (1)$$

Cette expression est basée sur l'hypothèse que la défaillance d'un seul composant provoque celle du bloc structurel complet, ce qui correspond au cas le plus pénalisant.

En utilisant cette approximation au niveau du produit, si on considère un produit comme un ensemble de blocs structurels tous indispensables au fonctionnement du système [FIDES, 04], le taux de défaillance du produit peut être exprimé par :

$$\lambda_{produit} = \sum_{BS \in produit} \lambda_{BS} \qquad (2)$$

Les hypothèses formulées précédemment font aboutir à un résultat qui doit être considéré comme une valeur limite dans la mesure où il correspond aux situations les plus défavorables d'un point de vue de la fiabilité du système. Au niveau de l'appel d'offre, l'objectif étant d'établir un ordre de grandeur pour le taux considéré, les hypothèses sont donc acceptables.

Nous montrerons dans le paragraphe 4 comment ces équations sont liées aux modèles développés.

3.2. Objectifs de sécurité

Nous présentons séparément les objectifs de fiabilité et de sécurité ; cependant, ces deux types d'objectifs sont liés, notamment, dans les fonctions de sécurité intégrées au produit dont les exigences de fiabilité sont sévères que ce soit en terme de durée de fonctionnement ou par rapport aux conditions dans lesquelles elles doivent être assurées [Mortureux, 01].

Soulignons qu'une particularité des produits considérés est qu'ils réalisent des fonctions de sécurité et qu'ils embarquent aussi des fonctions destinées à leur sécurité.

La sécurité fonctionnelle a été définie dans le chapitre 1 paragraphe 4.2.1. Elle est caractérisée par l'absence de risque inacceptable induit par un dysfonctionnement du système. Elle est mesurée sur une échelle discrète. Chaque échelon représente un niveau d'intégrité de sécurité. Selon la norme [IEC 60300-2], un niveau d'intégrité correspond à la délimitation d'une plage de valeurs pour une propriété d'entité donnée[23], nécessaire au maintien des risques d'un système donné dans des limites acceptables. Selon la norme [IEC 61508-4] : "*la sécurité fonctionnelle est un sous-ensemble de la sécurité globale se rapportant à l'EUC[24] et au système de commande de l'EUC qui dépend du fonctionnement correct des systèmes électriques, électroniques ou électro-programmables relatifs à la sécurité, des systèmes relatifs à la sécurité basés sur une autre technologie et des dispositifs externes de réduction de risque*". Enfin, pour la norme ISO 26262, c'est : « *l'absence de risque inacceptable du à un dysfonctionnement du système* » [ISO 26262].

La sécurité fonctionnelle est caractérisée par des niveaux d'intégrité de sécurité dits "SIL" (pour Safety Integrity Level) Dans le contexte automobile, on utilise maintenant les niveaux ASIL (le "A" représentant Automotive) avec la création de la norme ISO 26262, déclinaison dédiée à l'automobile à paraître mais déjà tacitement considérée comme valable par les acteurs de ce domaine.

La première façon de caractériser les SIL ou les ASIL consiste à définir des plages de valeur correspondant aux taux de défaillance tolérés (en défaillance par heure) pour la fonction étudiée. Les ASIL définis dans la nouvelle norme correspondent à une adaptation des niveaux de la norme IEC 61508. Nous rappelons ci-dessous la correspondance entre les SIL et les ASIL.

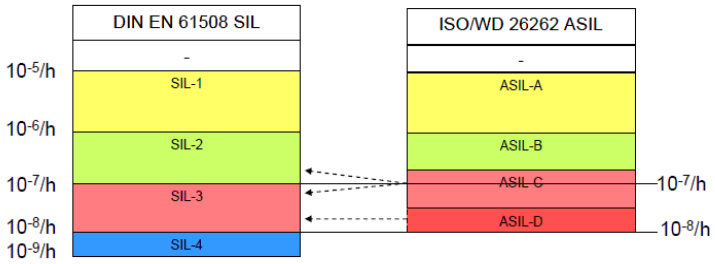


Figure IV-4 : Correspondance entre SIL et ASIL

[23] Pour des entités qui réalisent des fonctions de sécurité, la propriété est la fiabilité avec laquelle l'entité accomplit cette fonction de réduction des risques. Pour des entités dont la défaillance peut donner lieu à une menace, la propriété correspond à une plage de valeur définie de fréquence des défaillances.

[24] EUC : Element Under Consideration correspondant au système étudié

Pour le niveau SIL 3, par exemple, le nombre de défaillances par heure doit varier entre 10^{-7} défaillances/heure et 10^{-8} défaillances/heure. Le SIL 4 de l'IEC 61508 correspond à une conséquence maximum : "plusieurs personnes tuées", à une fréquence d'exposition : "fréquente et permanente", une possibilité d'éviter un évènement dangereux : "presque impossible", cela, avec : "une probabilité faible que des occurrences non souhaitées surviennent ou seulement quelques occurrences non souhaitées sont probables" [IEC 61508-5]. Dans la nouvelle norme ISO 26262, cette situation n'a pas été jugée pertinente pour le milieu automobile et le niveau maximum est donc l'ASIL D qui correspond, au plus, à un SIL 3.

Intéressons nous maintenant à la signification de ces différents niveaux. Ils sont définis par trois grandeurs :

- la sévérité (severity / S) :

Classe	S0	S1	S2	S3
Description	Pas de blessures	Blessures modérées et faible	Blessures sévères et grave (survie incertaine)	Blessures graves (survie incertaine), blessures mortelles

Tableau IV-1 : Sévérité de l'événement [ISO 26262-3]

- l'exposition (exposure / E) :

Classe	E1	E2	E3	E4
Description	Probabilité très faible	Probabilité faible	Probabilité moyenne	Probabilité haute

Tableau IV-2 : Exposition à l'évènement [ISO 26262-3]

- la contrôlabilité (controllability / C) :

Classe	C0	C1	C2	C3
Description	Contrôlable en général	Facilement contrôlable	Normalement contrôlable	Difficilement contrôlable ou incontrôlable

Tableau IV-3 : Contrôlabilité de l'évènement [ISO 26262-3]

Ces trois facteurs permettent de définir l'ASIL par leurs combinaisons à l'aide, par exemple, d'un graphe de risque[25] ou d'autres méthodes définies dans la norme. Nous proposons l'utilisation d'un tableau issu de la norme (Tableau IV-4).

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Tableau IV-4 : Table de détermination d'un ASIL issue de [ISO 26262-3]

La détermination du niveau ASIL d'un élément est déduite de la définition des grandeurs S, E et C. Par exemple, pour un

[25] Un exemple de graphe de risque est présenté dans le paragraphe 4.2 du chapitre 1.

élément ayant une sévérité S1, une exposition E4 et une contrôlabilité C3, la lecture du tableau permet de conclure que le niveau de sécurité de l'élément correspond à un ASIL B. Dans le tableau précédent, les lettres A, B, C, D correspondent respectivement aux différents niveaux ASIL. La désignation "QM" signifie "Quality Management" et correspond au cas où il n'y a pas d'exigences particulières de sécurité mais les exigences devront être traitées par le système de management de la qualité. La répartition des cas[26] en fonction des valeurs de C, E et S peut être exprimée en pourcentage : ASIL A (12,5%), ASIL B (9%), ASIL C (5%), ASIL D (1,5%), QM (72%).
L'allocation des ASIL incombe généralement au donneur d'ordre (le client) qui exprime ainsi ses besoins sécuritaires.

Après avoir présenté le concept de sécurité fonctionnelle, nous allons définir la façon dont ces exigences sont exprimées par le client et la nature des grandeurs utilisées pour la vérification de ces niveaux.

Le client exprime ses objectifs de sécurité par rapport à des évènements redoutés (ou évènements indésirables client). Ils sont alloués au niveau du système selon un point de vue fonctionnel.
La première difficulté concernant les événements redoutés réside dans leur expression. Un client peut en effet énoncer un évènement redouté sous la forme : "Perte de la fonction". Plusieurs interprétations sont possibles pour prendre en compte cette exigence. Le risque inacceptable correspond-il à :

- perte de la fonction non détectée ?
- perte de la fonction (i.e. que les mécanismes de sécurité fonctionnent ou non) ?

Afin de discuter cette notion, nous proposons de partir des différents états possibles d'un système. Dans [Lamy, 02], l'auteur considère quatre états :

- état normal : état dans lequel il n'existe pas de défaillances et pour lequel la fonction de sécurité est active et activable,
- état dégradé : état dans lequel le système peut avoir des composants défaillants tout en continuant à fonctionner mais dans lequel la fonction de sécurité est active et activable,
- état de sécurité : état du système après la détection d'une défaillance ayant nécessité la mise en sécurité du système (ce type de défaillance détectée est appelé défaillance sûre ou en sécurité dans la norme IEC 61508),
- état de défaillance dangereuse : état dans lequel la fonction de sécurité est désactivée ou défaillante et pour lequel l'apparition d'une défaillance peut entraîner des conséquences catastrophiques (ce type de défaillance est appelé défaillance dangereuse).

A partir de ces états, nous nous sommes intéressés à l'analyse des états possibles du système afin d'identifier les problèmes potentiels de sécurité dans le cas général. Pour cela, nous proposons un graphe d'état des systèmes considérés. Ces systèmes sont non réparables et embarquent des fonctions de sécurité permettant d'atteindre un état sécurisé lors de l'apparition de certaines défaillances.
Nous utilisons les notations suivantes : λ pour les taux de défaillances notés, γ pour les taux de détection des défaillances notés et les indices D (dangereuse), ND (non dangereuse) et SSS (sous système de sécurité) afin de caractériser les grandeurs précédentes.
Le sous système de sécurité représente l'ensemble des fonctions de sécurité intégrées au produit. Deux cas sont à

[26] Un cas correspond à un niveau de sévérité, un niveau d'exposition et un niveau de contrôlabilité soit $4^3 = 64$ cas. Nous avons donc calculé la fréquence à partir du nombre de cas ayant un ASIL donné par rapport au nombre de cas total.

considérer :

- soit le sous système de sécurité détecte l'ensemble des défaillances avec γ = 1 (Figure IV-5),
- soit le sous-système de sécurité ne détecte qu'une partie des défaillances avec γ < 1 (Figure IV-6).

Sur la Figure IV-5, le taux de détection du sous système de sécurité n'apparaît pas puisqu'il est égal à 1. Le graphe d'état du système comporte six états : nominal, dégradé, de sécurité, non sécurisé (2 états) et défaillant. L'état dégradé (2) apparaît lors de l'occurrence d'une défaillance non dangereuse dans le système depuis l'état nominal (1). Cet état correspond à un mode où le système continue à assurer sa fonction mais avec certaines fonctionnalités dégradées.

Les états non sécurisés (4 et 5) apparaissent lorsque le système est en mode nominal (1) ou dégradé (2) et que le sous système de sécurité devient défaillant. Dans ces états, le système continue d'assurer sa mission mais le sous système de sécurité est défaillant.

L'état de sécurité (3) est atteint lors de l'occurrence d'une défaillance dangereuse dans le système depuis les états nominal (1) ou dégradé (2).

Enfin, la défaillance du système (6) apparaît lors de l'occurrence d'une défaillance dangereuse dans le système dont le sous-système de sécurité est inactif (4 ou 5).

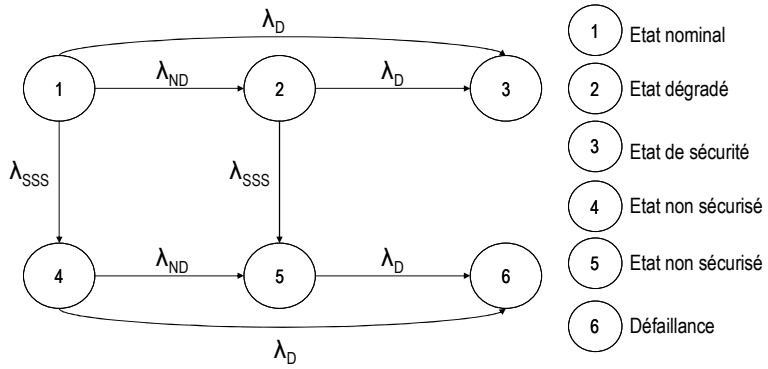


Figure IV-5 : Graphe d'état du système pour γ = 1

Soulignons que dans ce modèle, comme dans le suivant, nous n'avons pas considéré l'occurrence de défaillances non dangereuses ou du sous-système de sécurité consécutives qui entraineraient d'autres niveaux (d'autres états) de dégradation intermédiaires.

Nous présentons sur la Figure IV-6, le graphe d'état dans le cas où le taux de détection est inférieur à 1, i.e. le sous système de sécurité ne détecte pas toutes les défaillances.

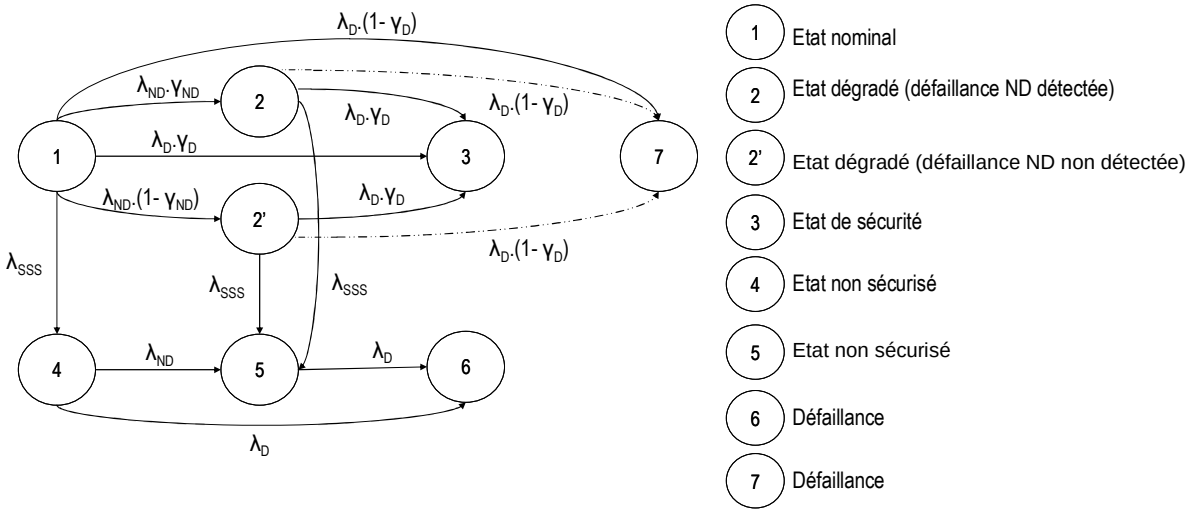


Figure IV-6 : Graphe d'état du système pour γ < 1

Sur ce graphe, les états 1, 2, 3, 4, 5 et 6 sont identiques à ceux de la Figure IV-5. L'état dégradé dans lequel une défaillance non dangereuse n'est pas détectée (2') correspond à un mode dans lequel le système continue à remplir sa mission mais avec la perte de certaines fonctionnalités. L'état de défaillance (7) est atteint lors de l'occurrence d'une défaillance dangereuse non détectée depuis le mode nominal (1) ou dégradé (2 ou 2').

Cette analyse des états possibles d'un système permet, dans un premier temps, la compréhension du problème de sécurité des systèmes considérés et, dans un second temps, permet d'identifier les différents taux de défaillances et de détection à considérer.

Nous nous intéressons maintenant aux grandeurs et aux formules définies dans les normes IEC 61508 et ISO 26262 afin de les comparer aux différents taux que nous avons identifiés sur les deux figures précédentes.

Notons, tout d'abord, la principale différence entre les deux normes qui réside dans les grandeurs considérées. Pour cette raison, nous proposons, dans un premier temps, la description des notations et des grandeurs utilisées dans les deux normes afin de pouvoir ensuite présenter les formules utilisant ces grandeurs.

Nous débutons par la présentation des grandeurs considérées dans la norme IEC 61508 :

- λ_{SD} correspond au taux de défaillances sûres détectées (i.e. les défaillances qui, en cas d'apparition, compromettent la fonction mais pas la sécurité),
- λ_{DD} correspond au taux de défaillances dangereuses détectées (par opposition aux précédentes, l'apparition de ce type de défaillances peut compromettre la sécurité si elles ne sont pas détectées),
- λ_{SU} correspond au taux de défaillances sûres non détectées (i.e. comme précédemment, ces défaillances, si elles apparaissent, compromettent les fonctionnalités du système mais pas sa sécurité),
- λ_{DU} correspond au taux de défaillances dangereuses non détectées qui entraînent le système dans un état de défaillances dangereuses,
- λ_D (parfois aussi noté $\lambda_{D\ total}$) correspond au taux de défaillances dangereuses total et est calculé par addition de λ_{DD} et $\lambda_{DU,}$
- λ_S correspond au taux de défaillances sûres total obtenu par addition de λ_{SD} et λ_{SU}.

La relation entre ces grandeurs est donnée, pour l'élément étudié, par l'équation :

$$\lambda_{élément} = \lambda_{SD} + \lambda_{DD} + \lambda_{SU} + \lambda_{DU} = \lambda_D + \lambda_s$$

Dans la norme ISO 26262, les grandeurs diffèrent des précédentes. Les notions définies sont :

- λ_{RF} : taux de défaillances résiduelles correspondant aux défaillances qui peuvent survenir et induire à la violation d'un objectif de sécurité dans un élément partiellement couvert par des mécanismes de sécurité (le taux correspond aux défaillances non couvertes),
- λ_{SPF} : taux de défaillances simples correspondant aux défaillances d'un élément qui, par leur apparition, mènent directement à la violation d'un objectif de sécurité,
- λ_{MPF} : taux de défaillances multiples correspondant aux combinaisons de plusieurs fautes indépendantes qui, par leur apparition simultanée, peuvent mener à la violation d'un objectif de sécurité,
- λ_S : taux de défaillances sûres.

La relation entre ces grandeurs est donnée, pour l'élément étudié, par l'équation :

$\lambda_{élément} = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_S$

Nous présentons une dernière grandeur définie dans les deux normes : les défaillances aléatoires (ou Random Hardware Failure) :

- selon la norme IEC 61508, elles correspondent aux défaillances survenant de manière aléatoire et résultant de divers mécanismes de dégradation au sein du matériel,
- selon l'ISO 26262, c'est la fin (apparaissant aléatoirement) de la capacité d'un composant ou d'une pièce à remplir sa fonction.

La correspondance entre les grandeurs définies dans la norme IEC61508 et les grandeurs employées dans les graphes d'états initiaux est facile à établir.

Taux considéré	→	fig. 5&6	→	IEC62508	→	ISO26262
Taux de défaillance non dangereuse	→	λ_{ND}	→	λ_S	→	λ_S
Taux de défaillance dangereuse	→	λ_D	→	λ_D	→	$\lambda_{SPF} + \lambda_{RF} + \lambda_{MPF}$
Taux de défaillance dangereuse détectée	→	$\lambda_D \gamma_D$	→	λ_{DD}	→	pas d'équivalent
Taux de défaillance dangereuse non détectée	→	$\lambda_D(1-\gamma_D)$	→	λ_{DU}	→	λ_{RF}

Cette comparaison permettra par la suite une meilleure compréhension des formules proposées dans la norme pour vérifier les niveaux d'intégrité de sécurité.

Il existe un grand nombre de tables proposées dans la norme qui présentent les niveaux à atteindre ou les plages de valeurs à respecter pour les différentes grandeurs en fonction du niveau d'intégrité de sécurité.
Ces différentes tables[27] permettent la vérification et la validation des SIL ou ASIL alloués à un système ou partie d'un système.
Nous avons présenté les grandeurs considérées, nous nous intéressons maintenant aux calculs utilisant ces grandeurs.

- Couverture de diagnostic (ou Diagnostic Coverage) :
  - selon la norme IEC 61508, cette grandeur correspond à "*la fraction exprimant la décroissance de la probabilité de défaillance dangereuse du matériel résultant du fonctionnement des tests de diagnostic automatique*". C'est la fraction de défaillances dangereuses détectées par rapport à l'ensemble des défaillances dangereuses.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \lambda_{DU}} \qquad (3)$$

  - selon la norme ISO 26262, cette grandeur correspond à "*la proportion de défaillance couverte en considérant les mécanismes de sécurité implémentés*". Comme nous l'avons précisé au début de cette partie, la norme ISO 26262 considère les grandeurs par rapport à d'autres grandeurs. On peut donc calculer la couverture de diagnostic par rapport aux fautes résiduelles

[27] Les règles d'utilisation de ces tables de correspondance sont données dans les normes IEC61508 et ISO 26262.

$$DC_{\text{par rapport aux fautes résiduelles}} = 1 - \frac{\lambda_{RF}}{\lambda_{\text{élément}}} \qquad (4)$$

- la fraction de défaillances sûres ou en sécurité (ou safe failure fraction : SFF) *:*
  - la norme IEC61508 la décrit comme la fraction de défaillances sûres i.e. n'ayant pas le potentiel de mettre le système dans un état dangereux.

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} \qquad (5)$$

- les fautes simples définies par rapport aux éléments relatifs à la sécurité du système *:*

$$\text{Taux de défaillance de faute simple} = 1 - \frac{(\lambda_{SPF} + \lambda_{RF})}{\lambda_{\text{élément}}} = \frac{\lambda_{MPF} + \lambda_S}{\lambda_{\text{élément}}} \qquad (6)$$

Nous avons intentionnellement utilisé les deux normes, l'IEC 61508 et l'ISO 26262, pour la définition des grandeurs de sécurité dans l'objectif de considérer les grandeurs les plus adaptées au niveau d'abstraction correspondant au PRAO, phase dans laquelle le produit n'existe pas.

Après avoir défini l'ensemble des grandeurs permettant de valider ou vérifier les exigences de sécurité, nous présentons les simplifications pouvant être acceptées dans le cadre de prévisions faites durant le PRAO. Nous cherchons en effet à caractériser les performances de la solution choisie. Il faudra ensuite au cours du développement, effectuer de façon plus fine le calcul des grandeurs afin de valider l'atteinte des objectifs.

Les clients souhaitent avoir un aperçu des niveaux atteignables. Leur objectif est de s'assurer que l'architecture matérielle de sécurité est suffisamment robuste pour réduire le taux de défaillances résiduelles ainsi que le taux de défaillances latentes [Dumas, 06]. Les grandeurs qui paraissent les plus accessibles au niveau de la définition du système dans le PRAO sont :

- la couverture de diagnostic qui peut être estimée de façon quantitative (en pourcentage) ou qualitative (bas, moyen, élevé) à l'aide des informations contenues dans la norme et que l'on a retranscrit dans les attributs sécurité de chaque bloc structurel,
- le taux de défaillances résiduelles,
- le taux de défaillances total du système calculé à partir des taux de défaillances de chaque module.

Pour conclure sur les taux de défaillances, rappelons que la norme [IEC 61508-6] autorise de considérer pour les composants complexes (un microcontrôleur par exemple) une répartition entre défaillances sûres et défaillances dangereuses à hauteur de 50% chacune. Pour les composants simples, cette répartition sera extraite du retour d'expérience, sinon, le plus souvent, on considère a priori 80% de défaillances sures et 20% de défaillances dangereuses.

3.3. Exigences sur la gestion et le traitement des objectifs SdF

Comme nous l'avons vu, une "démarche SdF" consiste généralement en l'emploi organisé d'une panoplie de méthodes susceptibles d'être associées pour atteindre un objectif final. A partir de méthodes usuelles en milieu industriel (présentées au chapitre 1), nous avons défini un processus standard (introduit au chapitre 2) sur lequel nous nous

appuyons pour la définition des méthodes à mettre en œuvre en fonction de l'objectif à atteindre et du contexte de travail. Le choix des méthodes pourra varier.

Il faut ici estimer les ressources nécessaires à chaque type d'étude figurant dans la démarche rappelée sur la Figure IV-1 et la durée de celles-ci dans le développement futur. Au niveau des ressources engagées pour une étude SdF, il est généralement recommandé de s'appuyer sur une équipe pluridisciplinaire intégrant l'ensemble des métiers nécessaires à la réalisation du projet.

Dans le contexte où nous nous plaçons et par rapport à l'ensemble des métiers impliqués dans la réalisation du produit, il faudra réunir au minimum :

- un représentant de la mécanique,
- un représentant de l'électronique,
- un représentant du logiciel,
- un représentant de la qualité,
- le chef de projet.

Par rapport à des besoins ponctuels, un représentant de la fabrication ou des experts pourront participer.

Le client peut imposer l'application de sa propre démarche SdF ou l'emploi d'un outil spécifique dans l'objectif de pouvoir vérifier plus facilement les analyses réalisées [Blancart, 07]. Un problème peut alors se poser au niveau de la maîtrise par l'entreprise des modes opératoires préconisés par le donneur d'ordre. Une solution alternative pour l'entreprise peut être de démontrer au client l'efficacité de sa propre démarche interne.

Dans l'industrie automobile, les constructeurs ont généralement l'initiative de la définition de processus standard ou d'utilisation de méthodes particulières et il est donc peu fréquent de rencontrer ce type de situation. Par contre, au niveau des outils supportant les analyses SdF, ces outils peuvent varier d'un client à l'autre.

Les principales informations à extraire du CdC concernant la démarche SdF et la panoplie de méthodes sont :

- le mode de réalisation de chaque analyse si le client l'impose (évènement déclencheur de l'étude ; c'est le cas pour les arbres de défaillances qui, selon les clients, seront réalisés si un risque est supérieur à un niveau fixé par le client ou en fonction du nombre d'ER (1 ER = 1 arbre),
- le plan SdF qui renseignera à quel moment dans le cycle de développement, le client souhaite disposer des différentes études, cela pouvant entraîner, par rapport à la démarche entreprise, des changements de priorité,
- le format de présentation des résultats.

4. Liens entre les exigences client et les modèles entreprise

Dans ce paragraphe, nous allons établir et expliciter les liens entre les exigences présentées dans le paragraphe précédent et les modèles du produit développés dans le chapitre 3 et qui ont été rappelés sur la Figure IV-1.

4.1. Relation entre les exigences de fiabilité et les modèles développés

L'évaluation de la fiabilité du produit utilise différents supports ; nous les rappelons sur la Figure IV-7 avant de montrer les liens entre ces deux types d'exigences et les supports correspondants. .

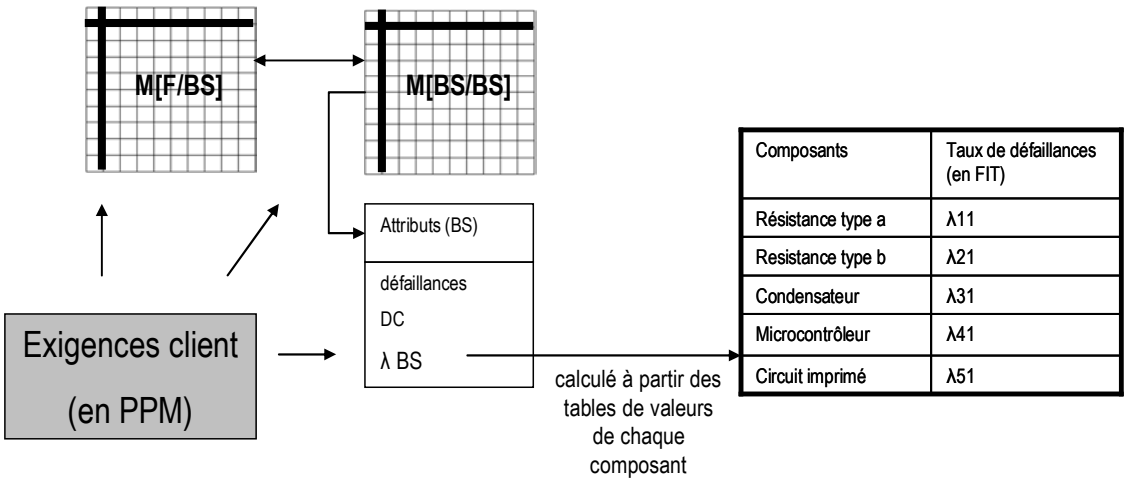


Figure IV-7 : Supports pour l'évaluation de la fiabilité

A l'aide des matrices M[F/BS] qui permet d'identifier les blocs structurels intervenant en support de chaque fonction et M[BS/BS] qui décrit l'organisation des blocs structurels entre eux, nous allons estimer les taux de fiabilité des différentes fonctions par rapport au taux de défaillance de chaque bloc. Nous souhaitons lier le taux de défaillances du système à l'exigence client en termes de PPM.

Le taux de défaillance correspond au nombre de défaillances par heure d'un système. En multipliant ce taux de défaillance par la durée de garantie du système puis par 10^6 nous obtenons le nombre de PPM prévisionnel.

$$PPM_p = (\text{défaillance/heure})_{\text{système}} \times \text{durée de garantie(en heure)} \times 10^6 \quad (7)$$

Cette expression permet une évaluation du niveau atteignable en termes de PPM par rapport aux taux de défaillances du système.

4.2. Relations entre les exigences de sécurité et les modèles développés

L'étude de la sécurité implique de considérer les principaux mécanismes de défaillances du système afin d'identifier les évènements redoutés (ER) du système ou analyser les évènements redoutés donnés par le client.

Un évènement redouté est, en effet, une conséquence d'une ou plusieurs défaillances affectant le système. Dans l'objectif d'identifier les éléments du système susceptibles d'être impliqués dans l'apparition d'un ER, il faut pouvoir relier cet ER aux fonctions ou aux blocs structurels du système considéré. Nous définissons pour cela une table de correspondance entre les évènements redoutés et les fonctions. Cette table de correspondance est assimilable à une analyse préliminaire des risques (présentée dans le chapitre 2) dans la mesure où elle consiste :

- à définir les fonctions impliquées pour un évènement redouté donné (si le client donne les ER à traiter),
- à définir les ER si le client ne les a pas fournis ou s'il stipule qu'il faut vérifier qu'il n'y ait pas d'ER supplémentaire.

En reprenant les principes de l'APR, il apparait que les informations dont nous avons besoin sont les liens entre les états du système et les fonctions. Ce constat justifie les idées présentées à la suite.

Nous considérons l'état du système par rapport à l'état de ses fonctions. Cette relation peut être représentée par une matrice de conditions. Ce type de matrice consiste en une matrice dont les lignes représentent les différents ER et les

colonnes l'ensemble des fonctions du système. Les termes figurant aux intersections ligne/colonne représentent pour ceux égaux à 1, les défaillances de fonctions minimales conduisant à l'ER de la ligne correspondante [Turinetti, 83].

Nous présentons ici un exemple de matrice de correspondance entre ER et F.

	F1	F2	F3	F4
ER1	1	1	0	0
ER2	1	0	0	0
ER3	0	1	0	1
ER4	0	0	1	0

En explicitant cette matrice, on obtient :

- ER 1 apparait si F1 et F2 défaillantes :

$$ER1 = \overline{F1} \wedge \overline{F2},$$

- ER 4 apparait si F3 défaillante :

$$ER4 = \overline{F3}.$$

Plusieurs conditions indépendantes peuvent cependant être à l'origine d'un évènement redouté. On peut faire apparaître sur ces matrices différentes conditions pour un même ER comme présenté sur la matrice suivante pour le premier ER :

	F1	F2	F3	F4
ER1	1	1	0	0
ER1	0	0	1	0
ER1	0	0	0	1
ER2	0	1	1	0

Dans la matrice précédente, l'équation relative à l'ER1 peut être écrite sous la forme :

$$ER1 = (\overline{F1} \wedge \overline{F2}) \vee \overline{F3} \vee \overline{F4}$$

4.3. Relation entre les exigences sur la démarche et les modèles développés

Afin d'intégrer au facteur d'impact SdF la part correspondant à l'engagement d'une méthodologie particulière (ou à des aménagements de la méthodologie en place), nous avons établi pour chaque méthode susceptible d'être utilisée une fiche permettant d'estimer la durée en fonction de divers paramètres. Ces paramètres sont choisis par rapport à la méthode de déroulement normal de l'étude : point à étudier, défaillances à analyser ou à prendre en compte, nombre de fonctions et modes de défaillance associés, nombre d'ER à traiter. Nous explicitons ces fiches et la manière avec laquelle elles ont été créées dans le paragraphe 5.4.

Nous rappelons la démarche analysée sur la Figure IV-8 et détaillons le principe retenu pour la définition des fiches d'estimation de la durée et de leurs paramètres.

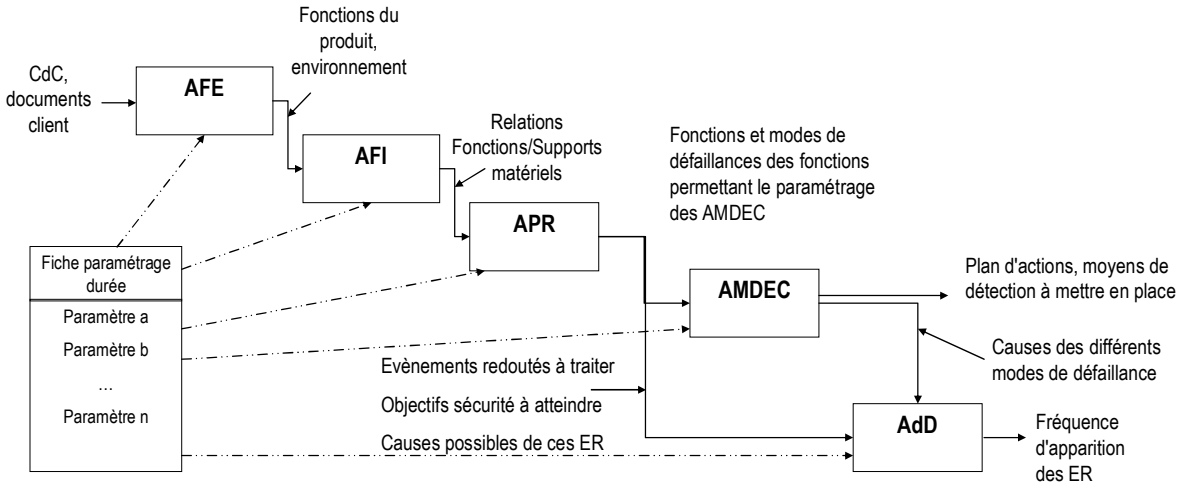


Figure IV-8 : Rappel de la démarche et fiches méthodes

Pour chaque méthode, nous avons défini les données d'entrée nécessaires ainsi que les données obtenues en sortie de la méthode. Ensuite, en nous basant sur le déroulement de l'analyse, nous avons défini l'ensemble des éléments à analyser dans l'objectif de définir un paramètre de base servant à estimer la durée. Pour l'AMDEC, ce paramètre consiste à évaluer le nombre de blocs structurels à étudier pour un mode de défaillance particulier ; pour l'arbre de défaillance, le paramètre est basé sur le nombre d'arbres à réaliser ainsi que sur le nombre de causes potentielles (au niveau du bloc structurel), ...

Nous avons analysé les méthodes les plus courantes dans un contexte industriel en considérant aussi les méthodes utilisées par l'entreprise partenaire. Cependant, dans le cas où le client requiert une étude particulière, deux situations sont à considérer :

- l'étude est déjà intégrée à la démarche entreprise et elle est dimensionnée sur la base des renseignements fournis par des fiches méthodes,
- l'étude ne figure pas dans la démarche entreprise et il faut soit estimer la charge qu'elle va représenter par une analyse complète soit rapprocher cette charge de celle d'une méthode déjà prise en compte en mettant en évidence une similarité d'objectifs et de déroulement d'étapes.

5. Méthodologie matricielle pour les étapes Projection et Evaluation

L'objectif de la projection est, rappelons le, d'obtenir la valeur d'impact de la prise en compte des exigences sûreté de fonctionnement sur le produit ainsi que sur la démarche à mettre en œuvre. Cette valeur d'impact est définie par le biais de l'application d'une méthodologie matricielle permettant d'assister l'acteur dans sa réflexion. Cette méthodologie a pour but de rendre possible et faciliter :

- l'étude des principaux mécanismes de défaillance du produit sous une forme intelligible par tout acteur quel que soit son métier,
- l'engagement d'études SdF ponctuelles en temps réel dans le PRAO pour traiter certains points particuliers
- l'utilisation de supports d'aide à la décision pour définir l'architecture du système ou l'organisation de certains blocs structurels,
- l'analyse des attributs de fiabilité et de sécurité,

- l'évaluation de la charge de travail correspondant aux analyses SdF qu'il faudra réaliser durant le développement futur du produit si le client accepte les conditions de la réponse à l'AO.

L'intégralité de la démarche a été proposée sur la Figure IV-2, nous rappelons ici les cinq étapes nécessaires à la projection et l'évaluation ainsi que les différentes activités intégrées à chaque étape.
La première étape de la méthodologie a pour objectif d'assister l'équipe acquisition dans le paramétrage des matrices et des attributs. Dans l'ordre, il faudra paramétrer M[F/F], M[F/BS], M[BS/BS] et enfin les attributs (i.e. les choix particuliers à effectuer sur un bloc structurel particulier : robustesse, sécurité,etc.).
La seconde étape concerne l'analyse prévisionnelle de la fiabilité du produit. Elle consiste à calculer le taux de défaillance du produit par rapport aux taux de défaillance des différents blocs structurels sélectionnés.
La troisième étape porte sur l'analyse de la sécurité du produit et est composée de plusieurs activités :

- le calcul du taux de défaillances résiduelles en regard des différentes sécurités mises en place dans le produit,
- l'analyse des fonctions du produit et de leur sécurité respective,
- l'analyse des ER du produit,
- des analyses en temps réel dans le PRAO afin de traiter certains points particuliers relatifs à la sécurité,
- l'analyse des défaillances de mode commun du produit.

La quatrième étape s'intéresse à l'évaluation de la charge de travail représentée par les analyses qu'il faudra engager dans le développement futur ainsi que celles effectuées durant le PRAO.
La dernière étape a pour objectif de définir l'impact financier de la prise en compte des exigences SdF sur le produit.
Les trois premières étapes ci-dessus constituent la projection, les deux dernières l'évaluation.

5.1. Etape 1 : Paramétrage des matrices

La prise en compte des activités du concepteur pendant le PRAO permet d'assister celui-ci pour le paramétrage des matrices. Nous présentons sur la Figure IV-9 le détail du paramétrage.

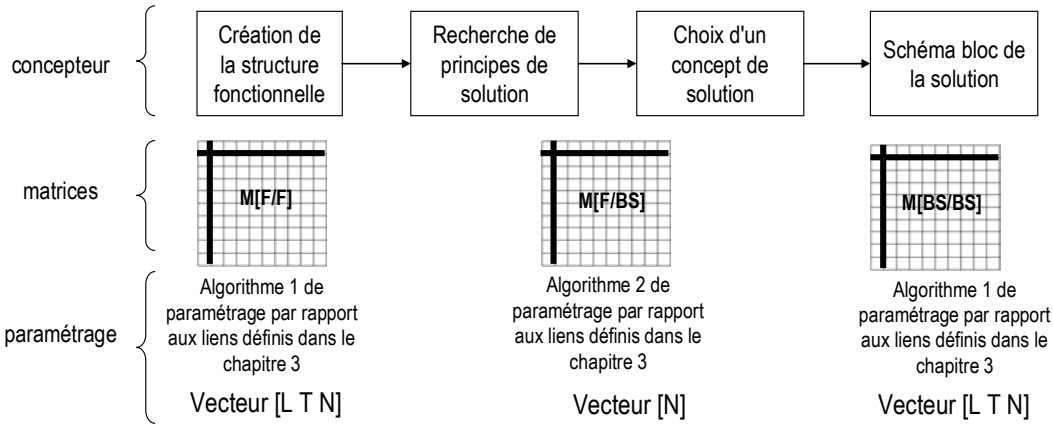


Figure IV-9 : Paramétrage des matrices

La première étape consiste à paramétrer les liens entre les différentes fonctions par le biais d'un premier algorithme basé sur les vecteurs de lien définis dans le chapitre 3. Cet algorithme est destiné au paramétrage des matrices intra-domaines M[F/F] et M[BS/BS] qui ont la particularité d'être des matrices carrés. Un autre algorithme nommé A2 sera présenté par la suite pour les matrices inter-domaines M[F/BS]. L'algorithme A1 est présenté sur la Figure IV-10 et la

matrice résultante M[F/F] sur la Figure IV-11.

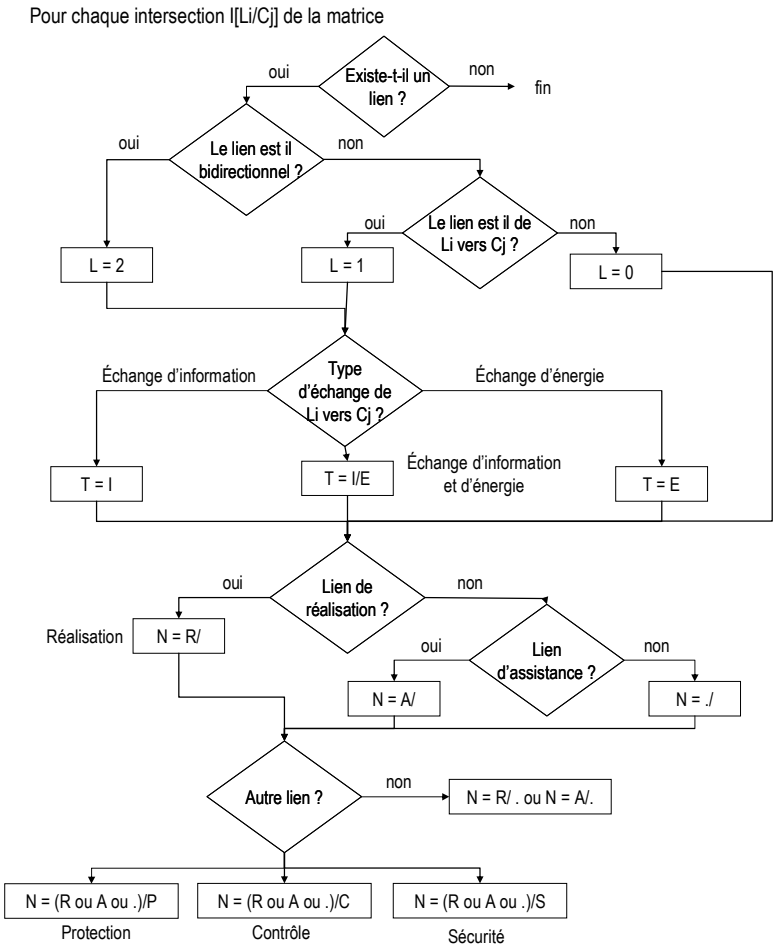


Figure IV-10 : Algorithme de paramétrage A1 M[F/F]

Dans l'algorithme de la Figure IV-10, la première information concerne l'existence ou non d'un lien. Dans le cas où il n'existe pas de lien, l'algorithme s'arrête et rien n'est indiqué dans l'intersection correspondante. Dans le cas où un lien existe, il faut caractériser celui-ci :

- si le lien est bidirectionnel (i.e. de l'élément de la ligne i à l'élément de la colonne j et inversement) alors L = 2,
- sinon deux cas sont à considérer :
  - le lien existe de l'élément de la ligne i vers l'élément de la colonne j alors L = 1,
  - le lien existe de l'élément de la colonne j vers l'élément de la ligne i alors L = 0.

Pour les cas (L=2) et (L=1), il faut caractériser le type d'échange existant :

- l'élément de la ligne i envoie des informations à l'élément de la colonne j alors T = I,
- l'élément de la ligne i envoie de l'énergie à l'élément de la colonne j alors T = E,
- l'élément de la ligne i envoie des informations et de l'énergie à l'élément de la colonne j alors T = E/I,

Ensuite, la dernière grandeur du vecteur concerne la nature du lien qui peut être double :

- si le lien existe pour la réalisation de la mission du produit, dans ce cas là la première composante sera égale à R : N = R/,
- dans le cas où le lien n'est pas un lien de réalisation, la première composante comportera un "." : N = ./.

Ensuite il faut définir la seconde composante de nature du lien :

- soit c'est un lien de réalisation uniquement alors N = R/.,
- soit ce n'est pas un lien de réalisation mais un lien autre alors N = ./(P ou C ou S),
- soit il existe un lien de réalisation ainsi qu'un lien de protection, de contrôle ou de sécurité alors N = R/(P ou C ou S).

L'algorithme A1 permet de définir le lien entre l'élément de la ligne i et celui de la colonne j mais renseigne aussi sur la nécessité de remplir l'intersection transposée (ligne j / colonne i) dans le cas où L = 0.

Nous illustrons l'application de l'algorithme A1 et le paramétrage dans le cas où le choix du concepteur s'est porté vers une solution à un microcontrôleur surveillé par un watchdog simple.

Cet exemple simple a été retenu pour deux raisons :

- la facilité de compréhension des matrices,
- le respect de confidentialité envers l'entreprise partenaire. En effet, la simple considération, par exemple, d'une situation à deux microcontrôleurs pourraient dévoiler via les informations contenues dans les matrices des stratégies de sécurité définies par l'entreprise partenaire.

Nous présentons sur la Figure IV-11 la matrice résultante.

Dans la matrice suivante, nous trouvons :

- entre les fonctions Acquérir et Traiter : un lien unidirectionnel d'Acquérir vers Traiter d'envoi d'informations pour la réalisation ; ce lien est représenté par :
  - à intersection ligne Acquérir et colonne traiter par un envoi (L+1) d'informations (T=I) pour la réalisation (N=R/.),
  - à intersection ligne Traiter et colonne Acquérir par une réception (L=0) d'informations dans le cadre de la réalisation (N=R/.),
- entre Stocker de l'information et Piloter, il existe un lien bidirectionnel (L=2) d'échange d'information (T=I) présent dans le cadre de la réalisation et du contrôle du fonctionnement de Piloter (N = R/C).

		Fournir les données extérieures à l'application client			Piloter	Envoyer la commande aux actionneurs et les informations vers l'extérieur			Assister		Sécuriser	
		Acquérir	Traiter	Transmettre	Piloter	Acquérir	Traiter	Transmettre	Alimenter	Stocker l'information	Contrôler le fonctionnement	Mettre en sécurité
Fournir les données extérieures à l'application client	Acquérir		[1 I R/.]						[0 . A/.]		[1 I ./C]	
	Traiter	[0 . R/.]		[1 I R/.]					[0 . A/.]		[1 I ./C]	
	Transmettre		[0 . R/.]		[1 I R/.]				[0 . A/.]		[1 I ./C]	
Piloter	Piloter			[0 . R/.]		[1 I R/.]			[0 . A/.]	[2 I R/C]	[1 I ./C]	[0 . ./S]
Envoyer la commande aux actionneurs et les informations vers l'extérieur	Acquérir				[0 . R/.]		[1 I R/.]		[0 . A/.]		[1 I ./C]	
	Traiter					[0 . R/.]		[1 I R/.]	[0 . A/.]		[1 I ./C]	
	Transmettre						[0 . R/.]		[0 . A/.]		[1 I ./C]	
Assister	Alimenter	[1 E A/.]	[1 E A/.]	[1 E A/.]	[1 E A/.]	[1 E A/.]	[1 E A/.]	[1 E A/.]		[1 E A/.]	[1 E A/.]	[1 E A/.]
	Stocker de l'information				[2 I R/C]				[0 . A/.]			
Sécuriser	Contrôler le fonctionnement	[0 . ./C]	[0 . ./C]	[0 . ./C]	[2 I ./C]	[0 . ./C]	[0 . ./C]	[0 . ./C]	[0 . A/.]			[1 I ./S]
	Mettre en sécurité				[1 I ./S]				[0 . A/.]		[0 . ./S]	

Figure IV-11 : Matrice M[F/F]

Après avoir établi la matrice M[F/F], le concepteur définit les blocs structurels supportant les différentes fonctions. Nous

assistons le concepteur dans le choix des blocs par le biais de l'affichage des différentes caractéristiques de chaque BS. La première étape consiste à identifier les blocs constitutifs du système. Le concepteur dispose d'une liste de blocs structurels définis dans le chapitre 3. Sur la base des degrés de liberté dont il dispose (paragraphe 3.2.3 du chapitre 3), le concepteur sélectionne la liste des blocs qu'il souhaite utiliser dans la solution (si plusieurs solutions sont envisageables, il sera établi autant de configurations afin de les comparer).

Il est possible de créer un utilitaire dédié au choix des blocs via un formulaire à l'aide de Microsoft Infopath qui permet de proposer un tableau comportant des cases à cocher. En fonction des choix effectués, une matrice vierge comportant les blocs structurels sélectionnés sera établie. Un aperçu de cette première étape est donné sur la Figure IV-12.

Choix des blocs structurels

Microcontrôleur	☑ Type 1	☐ Type 2	☐ Type 3	
Superviseur	☐ Watchdog	☐ Watchdog intelligent	☑ Microcontrôleur	☐ ASIC
Alimentation	☐ 1 alimentation	☑ 2 alimentations		
CAN	☑ 1 driver CAN	☐ 2 drivers CAN		

Figure IV-12 : Extrait du tableau de choix des blocs

L'algorithme de paramétrage et la matrice qui en résulte sont respectivement présentés sur la Figure IV-13 et la Figure IV-14. Cet algorithme A2 est basé sur les liens définis dans le chapitre 3 et est destiné aux matrices inter-domaines M[F/BS]. Ici, seule la composante nature du lien est renseignée.

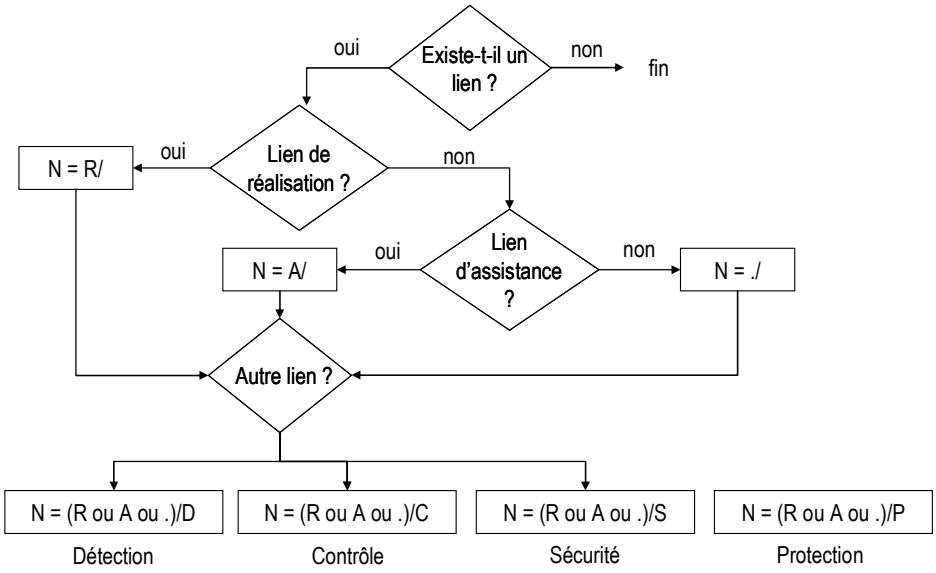


Figure IV-13 : Algorithme de paramétrage n°2 M[F/BS]

Dans l'algorithme A2 et par rapport aux liens définis dans le chapitre 3, les liens dans les matrices seront renseignés sous la forme [N]. La matrice résultante est représentée ci-dessous.

		Connecteur	Dispositif mise en forme des entrées analogiques	Dispositif mise en forme des entrées fréquentielles	Driver CAN	Micro contrôleur	Application client	Mémoire	Driver sortie 1	Alimentation 1	Watchdog	Dispositif de mise en sécurité
Fournir les données extérieures à l'application client	Acquérir	[R/.]								[A/.]		
	Traiter		[R/.]	[R/.]	[R/.]	[R/.]				[A/.]		
	Transmettre					[R/.]				[A/.]		
Piloter	Piloter					[R/.]	[R/.]			[A/.]		
Envoyer la commande aux actionneurs et les informations vers l'extérieur	Acquérir					[R/.]				[A/.]		
	Traiter					[R/.]			[R/.]	[A/.]		
	Transmettre	[R/.]				[R/.]				[A/.]		
Assister	Alimenter					[R/C]				[A/.]		
	Stocker de l'information					[R/.]		[R/.]		[A/.]		
Sécuriser	Contrôler le fonctionnement					[R/.]				[A/.]	[R/.]	
	Mettre en sécurité					[./S]				[A/.]	[R/S]	[R/.]

Figure IV-14 : Matrice M[F/BS]

Dans cette matrice, nous trouvons par exemple :

- entre la fonction Acquérir et le Connecteur : un lien de type réalisation (N=R/.),
- entre la fonction Alimenter et le Microcontrôleur : un lien de type réalisation et contrôle de la fonction (N=R/C].

Dans le paramétrage de la matrice M[F/BS], plusieurs liens apparaissent de manière récurrente car certaines fonctions sont toujours réalisées de la même manière quel que soit le produit. Une partie de la matrice peut être configurée automatiquement comme nous le montrons sur la Figure IV-15 dans laquelle les liens génériques apparaissent en grisé.

			Dispositif de mise en forme entrées analogiques	Dispositif de mise en forme entrées fréquentielles	Microcontrôleur	Superviseur	Driver CAN	Alimentation 1	Alimentation 2
Fournir les informations extérieures à l'application	Communiquer	Acquérir						[A/.]	
		Traiter	[R/.]	[R/.]	[.//C]	[./C]	[R/.]	[A/.]	
		Transmettre			[R/.]			[A/.]	
	Assister	Alimenter			[A/C]	[./C]		[R/.]	[R/.]
	Sécuriser	Contrôler le fonctionnement			[./C]	[R/.]			[A/.]
		Mettre en sécurité			[./S]	[R/.]			[A/.]

Figure IV-15 : Illustration du paramétrage semi-automatique de M[F/BS]

Dans cet exemple, il s'agit de la sous fonction Traiter de Communiquer qui sera toujours réalisée par les dispositifs de mise en forme des entrées et le Driver CAN ou des Alimentations qui assureront toujours la fonction Alimenter.

Il s'agit finalement de configurer la matrice M[BS/BS] ainsi que les paramètres des différents blocs qui permettront d'exploiter certains attributs. L'algorithme de paramétrage est similaire à celui utilisé pour la matrice M[F/F]. Nous ne le reprenons pas ici et donnons seulement la matrice résultante sur la Figure IV-16.

	Connecteur	Dispositif mise en forme des entrées analogiques	Dispositif mise en forme des entrées fréquentielles	Driver CAN	Microcontrôleur	Application client	Mémoire	Driver sortie 1	Alimentation 1	Watchdog	Dispositif de mise en sécurité
Connecteur		[1 I R/.]	[1 I R/.]	[1 I R/.]	[1 I R/.]			[0 . R/.]	[0 . A/.]		[1 -1 _ _]
Dispositif mise en forme des entrées analogiques	[0 . R/.]				[1 I R/.]				[0 . A/.]		
Dispositif mise en forme des entrées fréquentielles	[0 . R/.]				[1 I R/.]				[0 . A/.]		
Driver CAN	[0 . R/.]				[2 I R/.]				[0 . A/.]		
Microcontrôleur	[0 . R/.]	[0 . R/.]	[0 . R/.]	[2 I R/.]		[2 I R/.]	[2 I R/.]	[1 I R/.]	[0 . A/.]	[2 I ./C]	[0 . ./S]
Application client					[2 I R/.]				[0 . A/.]		
Mémoire					[2 I R/.]				[0 . A/.]		
Driver sortie 1	[1 I R/.]				[0 . R/.]				[0 . A/.]		
Alimentation 1	[1 E A/.]	[1 E A/.]	[1 E A/.]	[1 E A/.]	[1 E A/.]		[1 E A/.]	[1 E A/.]		[1 E A/.]	[1 E A/.]
Watchdog					[2 I ./C]				[0 . A/.]		[1 I R/S]
Dispositif de mise en sécurité	[1 I ./S]				[1 I ./S]				[0 . A/.]	[0 . ./S]	

Figure IV-16 : Matrice M[BS/BS]

Dans cette matrice, nous trouvons par exemple :

- entre le Connecteur et le Dispositif de mise en forme des entrées analogiques : un lien unidirectionnel du Connecteur vers le Dispositif (L=1) d'échange d'information (T=I) dans le cadre de la réalisation (N=R/.),
- entre le Watchdog et le Dispositif de mise en sécurité : un lien unidirectionnel du Watchdog vers le Dispositif de sécurité (L=1) d'échange d'information (T=I) dans le cadre de la réalisation et de la sécurité (N=R/S).

De la même façon que pour la matrice précédente, il est possible d'établir a priori des règles de liaisons dans l'architecture structurelle selon les blocs structurels présents. Nous donnons un exemple sur la Figure IV-17.

	Dispositif de mise en forme entrées analogiques	Dispositif de mise en forme entrées fréquentielles	Microcontrôleur	Superviseur	Driver CAN	Application client	Alimentation 1	Alimentation 2
Dispositif de mise en forme entrées analogiques			[1 I R/.]					
Dispositif de mise en forme entrées fréquentielles			[1 I R/.]					
Microcontrôleur	[0 . R/.]	[0 . R/.]		[2 I ./S]	[2 I R/.]	[2 I R/.]		
Superviseur			[2 I ./C]					
Driver CAN			[2 I R/.]					
Application client			[2 I R/.]					
Alimentation 1								
Alimentation 2								

Figure IV-17 : Illustration du paramétrage semi-automatique de M[BS/BS]

Cet exemple montre un cas impliquant un microcontrôleur et un watchdog. Dans cette configuration, l'ensemble des Dispositifs de mise en forme des entrées et des sorties est lié au Microcontrôleur (case grisée).

L'ensemble des matrices paramétrées a été défini. Il reste à établir certains paramètres de blocs qui permettront la définition des attributs liés à une solution particulière. Ces attributs sont :

1) le taux de défaillance du bloc, fonction du type de produit,

2) la couverture de diagnostic, fonction des mécanismes de sécurité que le concepteur souhaite implémenter dans chaque bloc.

Ces paramètres sont présentés sur la Figure IV-18 avec leur mode de paramétrage. L'illustration provient aussi du logiciel Microsoft Infopath dans lequel il est possible en fonction des paramètres cochés par le concepteur de définir des valeurs de variable (ici le taux de défaillance et la couverture de diagnostic).

Profil	Suspension	☐ Profil 1		
	ABS	☐ Profil 2		
	Direction	☐ Profil 3		
	Autres	1 ☐ 2 ☐ 3 ☐	Profil le plus proche	
Bloc	**Alimentation**			
λ	λ2	cas ABS		DC
Couverture de diagnostic	Basse	Voltage or current control (primary)	☐ DC < 60%	= 0 ☐ Bloc inconnu = 0,3 ☐ Bloc médian = 0,6 ☐ Bloc connu
	Moyenne		☐ 60%<DC<90%	= 0,6 ☐ Bloc inconnu = 0,75 ☐ Bloc médian = 0,9 ☐ Bloc connu
	Haute	Voltage or current control (secondary)	☐ DC>99%	= 0,99 ☐ Quel que soit le bloc
Taux de défaillances dangereuses résiduel approximatif	0,5 x (1-DC) x λ	λ_D		

Figure IV-18 : Exemple de paramétrage des attributs pour le bloc alimentation

Le but du paramétrage est d'intégrer le concepteur à la démarche de sélection des blocs mais aussi de capitaliser les choix effectués dans un certain contexte et, donc, de formaliser la connaissance du concepteur.

Dans la Figure IV-18, les taux de défaillances des composants utilisés dans le calcul de la fiabilité prévisionnelle des blocs structurels ou du produit seront configurés à partir du profil sélectionné (ici le profil de mission ABS). Dans le cas où le produit étudié appartient à la famille des produits "autres", deux solutions peuvent être envisagées : soit utiliser, par approximation, un profil de mission proche correspondant à l'un des trois profils prédéfinis ABS, Suspension ou Direction Assistée, soit recalculer, par le biais des outils existants, les taux de défaillance des différents composants pour le profil considéré.

Pour la couverture de diagnostic, les normes fixent trois niveaux en fonction du type de mécanisme de détection des défaillances mis en place pour les différents types de blocs structurels : bas, moyen et haut. Après avoir estimé le niveau par rapport à la norme, le concepteur pourra adapter ce niveau en fonction de sa connaissance sur le bloc structurel ou sur le mécanisme lui-même.

Enfin, par rapport au profil de mission sélectionné et à la couverture de diagnostic, un calcul du taux de défaillance dangereuse du bloc structurel pourra être automatiquement établi. Ce taux servira par la suite.

5.2. Etape 2 : Analyse de fiabilité

La fiabilité est calculée à partir des taux de défaillance des blocs structurels constituant le système. On dispose des taux de chaque BS ainsi que de l'expression du PPM à partir du taux de défaillances par heure (équation 7).

La première étape consiste à établir le taux de défaillance par heure du système par addition des taux de défaillance de

l'ensemble des blocs constituant la solution. On établit aussi la durée de fonctionnement sur la durée de garantie (environ 1000 heures) ce qui permet de calculer le PPM. Le taux est calculé ici sans considération de la couverture de diagnostic à l'aide des taux de défaillance des composants constituant le système.

Prenons l'exemple d'un ABS dont le calculateur a un taux de défaillance (hors considération de sécurité) de $57x10^{-8}$ défaillances par heure. En appliquant (7) sur une durée de garantie de 2 ans soit 1000 heures, on obtient un taux maximum de :

$$PPM_P = 57x10^{-8} \times 1000 \times 10^6 = 570$$

Ce résultat peut paraître élevé mais il est calculé à partir des taux de défaillance des composants primaires sans tenir compte des mécanismes de détection et de protection mis en place dans chaque bloc structurel ni des tests effectués en production dans l'objectif de détecter les problèmes avant livraison au client (contrôle visuel, test de mise en marche en sortie de chaîne). Le taux client sera, lui, égal au nombre de PPM en regard de toutes les implémentations de sécurité dans le produit, des tests et contrôles effectués durant la production.

5.3. Etape 3 : Analyse de sécurité

Cette étape correspond à la troisième étape de la démarche complète présentée sur la Figure IV-2. Plusieurs études peuvent être menées dans ce cadre. Nous proposons ici un aperçu des cinq activités ainsi que les notations utilisées dans l'exploitation des matrices (Figure IV-19).

Activité 3.1	Activité 3.2	Activité 3.3	Activité 3.4	Activité 3.5
Calcul du taux de défaillance résiduel	Analyse des fonctions hors et avec sécurité	Calcul de la fréquence d'apparition des ER	Analyse temps réel	Analyse des causes de modes communs

Figure IV-19 : Activités dans le cadre de l'étude de sécurité

La première activité (3.1) concerne le calcul du taux de défaillance résiduel par rapport aux mécanismes de sécurité implémentés (i.e. les défaillances susceptibles de survenir malgré les mécanismes de détection des défaillances implémentés sur les différents BS). Cette activité est réalisée à partir des informations contenues dans les attributs.

La seconde activité (3.2) concerne l'étude des dysfonctionnements des fonctions avec ou sans prise en compte de la sécurité.

La troisième activité (3.3) s'intéresse aux mécanismes de défaillance qui conduisent à l'apparition d'un ER et à l'analyse des fonctions et blocs structurels potentiellement impliqués dans l'apparition de celui-ci.

Les activités (3.4) et (3.5) ont pour objectif respectif la réalisation d'étude SdF en temps réel dans le PRAO pour l'éclaircissement de points particuliers et l'analyse des causes de modes communs.

Afin de faciliter la lecture des développements suivants, nous récapitulons les notations utilisées (Figure IV-20).

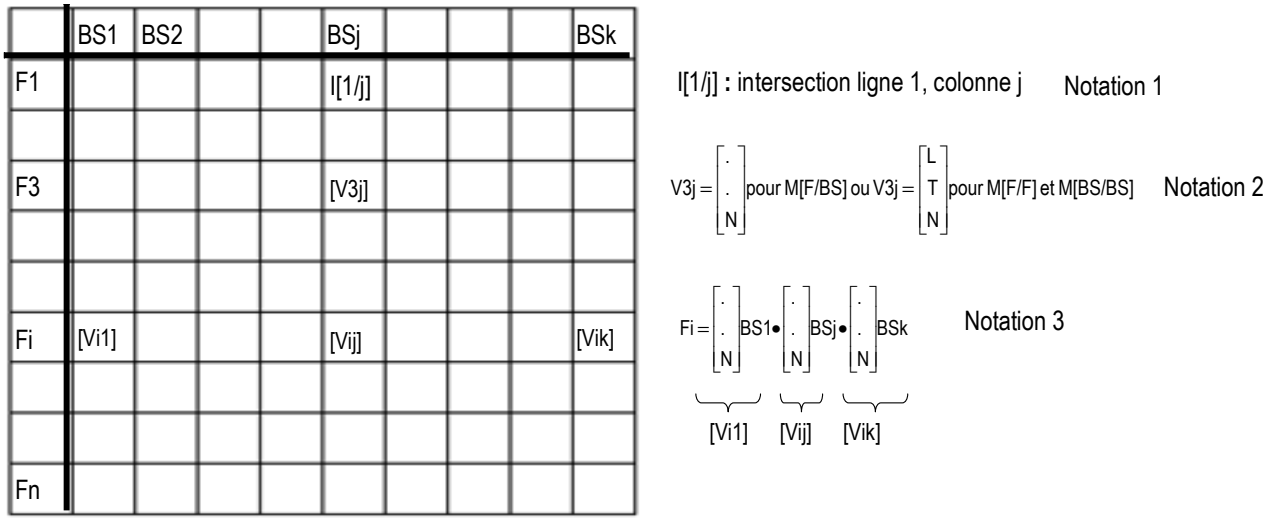


Figure IV-20 : Notations utilisées

La notation 1 sera utilisée pour l'identification des intersections non vides (existence d'un lien entre les éléments concernés par l'intersection) ou respectant certaines conditions.

La notation 2 présente les grandeurs des vecteurs présents dans les matrices intra-domaines et inter-domaines et explicite la nature des liens entre les éléments concernés.

La notation 3 sera utilisée dans le cadre de l'analyse des différentes fonctions. Elle permet la représentation d'une seule ligne de la matrice au lieu de la matrice entière. Dans cette notation, on ne représente que les intersections non vides.

5.3.1. Calcul du taux de défaillance résiduel (Activité 3.1)

Le taux de défaillance résiduel correspond au taux de défaillance d'un bloc structurel ou du système complet par rapport à l'ensemble des mécanismes de sécurité (protection/détection/…) implémentés. Les normes de sécurité fonctionnelle fournissent des plages de valeurs à respecter pour ce taux. L'activité 3.1 consiste à établir par le calcul du taux de défaillance résiduel de chaque BS (équation 1 dans le paragraphe 3.1 ou attribut du bloc structurel) puis du système complet (équation 2 dans le paragraphe 3.1 utilisé avec les taux résiduels de chaque bloc structurel. Le taux obtenu doit alors être comparé aux plages de valeur fixées par les normes afin de vérifier qu'il atteint bien le niveau requis (pour un ASIL B, par exemple, entre 10^{-6} et 10^{-7} défaillance par heure).

λ_{RF} est le premier indicateur de faisabilité SdF

5.3.2. Analyse des fonctions hors et avec sécurité (Activité 3.2)

Jusqu'ici, nous avons présenté les calculs basés uniquement sur les informations contenues dans les attributs de chaque bloc. Nous allons maintenant nous intéresser aux activités utilisant les matrices. Les calculs sur le système complet ne permettent pas d'observer les points faibles du système ce qui justifie l'utilisation des matrices qui permettent de procéder à des évaluations locales sur des fonctions ou des composants.

Différentes analyses peuvent être menées sur le fonctionnement du produit. Nous présentons par la suite :

- l'analyse du bon fonctionnement des fonctions ainsi que le taux de défaillance associé à ces fonctions en ne considérant pas les mécanismes de protection ou de détection implémentés,
- l'analyse du fonctionnement en sécurité des fonctions et le taux de défaillance associé,
- l'analyse simplifiée de la sécurité des différentes fonctions du produit.

La première étude concerne l'estimation des taux de défaillance des différentes fonctions du système. Nous utiliserons à ce niveau la matrice M[F/BS] pour la réalisation des calculs correspondants.

Nous considérons par exemple le cas de la fonction Stocker de l'information. La ligne de la matrice correspondante est représentée à l'aide de la notation 3 donnée sur la Figure IV-20.

$$\text{Stocker de l'information} = \begin{bmatrix} . \\ . \\ R/. \end{bmatrix} \text{Microcontroleur} \bullet \begin{bmatrix} . \\ . \\ R/. \end{bmatrix} \text{Mémoire} \bullet \begin{bmatrix} . \\ . \\ A/. \end{bmatrix} \text{Alimentation}$$

Comme nous l'avons précisé dans les notations, on ne considère ici que les intersections non vides.

Plusieurs calculs sont possibles.

Le premier concerne l'analyse du fonctionnement d'une fonction sans considération des mécanismes de détection ou de protection des défaillances implémentés. Pour une fonction Fi particulière, il faut rechercher dans la matrice M[F/BS] l'ensemble des intersections I[i/j] telles que N = R ou N = A qu'il y ait ou non une seconde composante et quelle que soit la nature de la seconde composante si elle existe comme ceci est illustré dans la notation précédente. Ensuite, on additionne les taux de défaillance des différents BS identifiés (en considérant que la perte d'un BS entraîne la perte de la fonction) pour obtenir le taux de défaillance de la fonction.

L'utilisation de la matrice M[F/BS] pour l'analyse de la perte de Fi est définie ci-dessous.

M[F/BS] ➡ Perte de Fi $\quad \sum\lambda[BSk]$ tel que dans I(i/j) la 1ère information de N est égale à R ou A

On peut aussi analyser le fonctionnement d'une fonction en tenant compte des mécanismes de détection et de protection implémentés. Il faut alors additionner les taux de défaillances calculés en considérant la couverture de diagnostic et le taux de défaillance des éléments de sécurité. Dans ce cas, il faut rechercher dans la matrice M[F/BS] l'ensemble des intersections non vides de Fi et additionner les taux de défaillances résiduelles des différents BS identifiés comme défini ci-dessous.

M[F/BS] ➡ Perte de Fi $\quad \sum\lambda_{RF}[BSk]$ tel que $[I(i/j) \neq 0]$

On peut réaliser ce calcul de façon plus précise en identifiant les blocs communiquant. Le calcul est effectué en plusieurs étapes. Si on souhaite analyser le fonctionnement d'une fonction en sécurité, on identifie dans la matrice M[F/BS] tous les blocs participant à la fonction par sa réalisation ou assistance (première information de N égale à R ou A). Dans la matrice M[BS/BS], il faut ensuite identifier les blocs dédiés à la surveillance, la protection ou la sécurisation (en recherchant les blocs liés tels que la seconde information de N est égale à P, C ou S) des blocs précédents. L'extraction des informations des matrices est illustrée ci-dessous pour Fi ainsi que pour le bloc BSk.

$$Fi = [\ R/.]BS1 \bullet [\ A/.]BS3 \bullet [\ R/.]BSk \bullet [\ R/.]BSn \qquad BSk = \begin{bmatrix} 0 \\ . \\ ./S \end{bmatrix} BS1 \bullet \begin{bmatrix} 0 \\ . \\ ./S \end{bmatrix} BSj$$

Pour avoir une fonction sécurisée, il faut analyser l'ensemble des cas pour lesquels la sécurité de la fonction ne sera pas assurée. Par rapport à l'extraction précédente, pour que Fi fonctionne en sécurité, il faudra que BS1 et BSj soient disponibles.

Considérons, par exemple, la sous-fonction Traiter de la fonction Envoyer les données à l'application client. La matrice M[F/BS] permet d'obtenir, en considérant les liens tels que la première information de la composante N soit égale à R ou A) :

$$\text{Traiter} = [\text{R/.}]\text{Dispositif E1} \bullet [\text{R/.}]\text{Dispositif E2} \bullet [\text{R/.}]\text{Driver CAN} \bullet [\text{R/.}]\text{Microcontrôleur} \bullet [\text{A/.}]\text{Alimentation}$$

Pour chaque bloc identifié dans l'équation précédente, on identifie dans M[BS/BS], les blocs en relation de protection, sécurité, contrôle ; seul le microcontrôleur est sécurisé par le watchdog.

$$\begin{bmatrix} 1 \\ \text{I} \\ \text{R/.} \end{bmatrix}\text{Microcontrôleur} \bullet \begin{bmatrix} 2 \\ \text{I} \\ \text{./C} \end{bmatrix}\text{watchdog}$$

L'analyse du fonctionnement sera simplifiée : puisque c'est le Watchdog qui assure la sécurité, l'étude de ses défaillances suffira à celle de la sécurité si la fonction a été analysée précédemment.

De la même manière, on peut schématiser cette recherche par :

M[F/BS]	➡	F_J	Recherche des BS_K tels que I[j/i] ait la 1ère information de N égale à R ou A
M[BS/BS]	➡	BS_K	Recherche des BS_i tels que I[k/i] ait la 2nde information de N égale à S, C ou P

Lorsque cette recherche dans les matrices a été effectuée, il suffit d'étudier les BSi correspondant à la sécurité de la fonction.

5.3.3. Calcul de la fréquence d'apparition des évènements redoutés (Activité 3.3)

Si des exigences SdF sont exprimées sous forme de niveau SIL ou ASIL requis pour le système, le client peut souhaiter être assuré, dès le PRAO, que les performances du futur produit sont proches de celles attendues.

Comme nous l'avons vu dans le paragraphe 4.2, un ER est caractérisé par une matrice de conditions le reliant aux fonctions du produit. L'ER apparaît généralement lorsqu'une défaillance affecte une fonction sans avoir été détectée d'où l'importance dans cette partie des mécanismes de protection, détection et sécurité.

Nous présentons la méthode permettant d'obtenir les équations relatives à l'apparition des ER.

A partir de la matrice M[F/F] et des liens établis, l'équipe acquisition doit identifier les fonctions ou combinaisons de fonctions dont la perte impliquerait un évènement redouté donné. Dans le cas considéré, on obtient la matrice de condition M[ER/F]. La matrice de condition M[ER/F] permet l'identification des différentes fonctions impliquées dans l'apparition d'un ER comme indiqué ci-dessous (matrice et équation ER1).

	F1	F2	F3	F4
ER1	1	1	0	0
ER1	0	0	1	0
ER2	0	0	0	1
ER2	1	0	0	0

$$ER1 = (\overline{F1} \wedge \overline{F2}) \vee \overline{F3}$$

Dans cet exemple, F1 est une fonction qui récupère les données des capteurs extérieurs au produit, F2 une fonction qui envoie la commande aux actionneurs, F3 est la fonction Alimenter et F4 contrôle le fonctionnement et assure la sécurité.

La matrice M[F/BS] permet d'identifier les blocs structurels nécessaires à la réalisation des fonctions. Dans l'exemple, BS1 est le Dispositif de mise en forme des entrées, BS2 le Microcontrôleur, BS3, le Driver de sortie, BS4 l'alimentation, BS5 le Watchdog et BS6 le dispositif de mise en sécurité.

	BS1	BS2	BS3	BS4	BS5	BS6
F1	[R/.]	[R/.]		[A/.]	[./C]	[./S]
F2		[R/.]	[R/.]	[A/.]	[./C]	[./S]
F3				[R/.]		
F4				[A/.]	[R/.]	[R/.]

Dans la matrice inter-domaines précédente, on identifie les dépendances :

- F1 réalisée par BS1 et BS2, assistée par BS4, contrôlée par BS5 et sécurisée par BS6,
- F2 réalisée par BS2 et BS3, assistée par BS4, contrôlée par BS5 et sécurisée par BS6,
- F3 réalisée par BS4, contrôlée par BS5 et sécurisée par BS6,
- F4 réalisée par BS5 et BS6 et assistée par BS4.

L'occurrence de l'ER correspond également la perte de la fonction sécuritaire associée au bloc ; on utilisera la matrice intra-domaine M[BS/BS] pour identifier les sécurités mises en place.

	BS1	BS2	BS3	BS4	BS5	BS6
BS1		[1 I R/.]		[0 . A/.]	[1 I ./C]	[0 . ./S]
BS2	[0 . R/.]		[1 I R/.]	[0 . A/.]	[1 I ./C]	[0 . ./S]
BS3		[0 . R/.]		[0 . A/.]	[1 I ./C]	[0 . ./S]
BS4	[1 E A/.]	[1 E A/.]	[1 E A/.]		[1 E A/.]	[1 E A/.]
BS5	[0 . ./C]	[0 . ./C]	[0 . ./C]	[0 . A/.]		[1 I ./S]
BS6	[1 I ./S]	[1 I ./S]	[1 I ./S]		[1 I ./C]	

La matrice précédente met en évidence que BS5 assure le contrôle du fonctionnement des blocs structurels BS1, BS2, et BS3 alors que BS6 permet d'assurer la sécurité en cas de détection de défaillance pour les blocs précédents.

Suite à l'analyse des matrices, deux solutions sont envisageables pour représenter les mécanismes d'apparition de l'ER soit sous forme d'arbre de défaillances soit sous forme d'équation logique.

En reprenant la matrice M[F/BS] et les liens définis dans celle-ci, l'expression de l'ER1 devient :

$$ER1 = (\overline{F1} \wedge \overline{F2}) \vee \overline{F3} \vee \overline{F4} = [((\overline{BS1} \vee \overline{BS2}) \wedge (\overline{BS5} \vee \overline{BS6})) \vee \overline{BS4}] \wedge [((\overline{BS2} \vee \overline{BS3}) \wedge (\overline{BS5} \vee \overline{BS6})) \vee \overline{BS4}] \vee \overline{BS4}$$
$$= [((\overline{BS1} \wedge \overline{BS5}) \vee (\overline{BS1} \wedge \overline{BS6}) \vee (\overline{BS2} \wedge \overline{BS5}) \vee (\overline{BS2} \wedge \overline{BS6})) \vee \overline{BS4}] \wedge [((\overline{BS2} \wedge \overline{BS5}) \vee (\overline{BS2} \wedge \overline{BS6}) \vee (\overline{BS3} \wedge \overline{BS5}) \vee (\overline{BS3} \wedge \overline{BS6})) \vee \overline{BS4}]$$
$$\vee \overline{BS4}$$

$= (\overline{BS1} \wedge \overline{BS2} \wedge \overline{BS5^2}) \vee (\overline{BS1} \wedge \overline{BS2} \wedge \overline{BS5} \wedge \overline{BS6}) \vee (\overline{BS1} \wedge \overline{BS3} \wedge \overline{BS5^2}) \vee (\overline{BS1} \wedge \overline{BS3} \wedge \overline{BS5} \wedge \overline{BS6}) \vee (\overline{BS1} \wedge \overline{BS4} \wedge \overline{BS5})$
$\vee (\overline{BS1} \wedge \overline{BS2} \wedge \overline{BS5} \wedge \overline{BS6}) \vee (\overline{BS1} \wedge \overline{BS2} \wedge \overline{BS6^2}) \vee (\overline{BS1} \wedge \overline{BS3} \wedge \overline{BS5} \wedge \overline{BS6}) \vee (\overline{BS1} \wedge \overline{BS3} \wedge \overline{BS6^2}) \vee (\overline{BS1} \wedge \overline{BS4} \wedge \overline{BS6})$
$\vee (\overline{BS2^2} \wedge \overline{BS5^2}) \vee (\overline{BS2^2} \wedge \overline{BS5} \wedge \overline{BS6}) \vee (\overline{BS2} \wedge \overline{BS3} \wedge \overline{BS5^2}) \vee (\overline{BS2} \wedge \overline{BS3} \wedge \overline{BS5} \wedge \overline{BS6}) \vee (\overline{BS2} \wedge \overline{BS4} \wedge \overline{BS5})$
$\vee (\overline{BS2^2} \wedge \overline{BS5} \wedge \overline{BS6}) \vee (\overline{BS2^2} \wedge \overline{BS6^2}) \vee (\overline{BS2} \wedge \overline{BS3} \wedge \overline{BS5} \wedge \overline{BS6}) \vee (\overline{BS2} \wedge \overline{BS3} \wedge \overline{BS6^2}) \vee (\overline{BS2} \wedge \overline{BS4} \wedge \overline{BS6})$
$\vee (\overline{BS2} \wedge \overline{BS4} \wedge \overline{BS5}) \vee (\overline{BS2} \wedge \overline{BS4} \wedge \overline{BS6}) \vee (\overline{BS3} \wedge \overline{BS4} \wedge \overline{BS5}) \vee (\overline{BS2} \wedge \overline{BS4} \wedge \overline{BS6}) \vee \overline{BS4^2})$
$\vee \overline{BS4}$

En factorisant les termes communs et par l'utilisation des lois de Morgan :

$ER1 = (\overline{BS5} \vee \overline{BS6} \vee \overline{BS5} \wedge \overline{BS6}) \wedge ((\overline{BS1} \wedge \overline{BS2}) \vee (\overline{BS2} \wedge \overline{BS3}) \vee (\overline{BS3} \wedge \overline{BS1}))$
$\vee (\overline{BS5} \vee \overline{BS6}) \wedge \overline{BS4} \wedge (\overline{BS1} \vee \overline{BS2} \vee \overline{BS3})$
$\vee (\overline{BS2}) \wedge (\overline{BS5} \vee \overline{BS6})$
$\vee \overline{BS4}$

Ce qui devient par simplification :

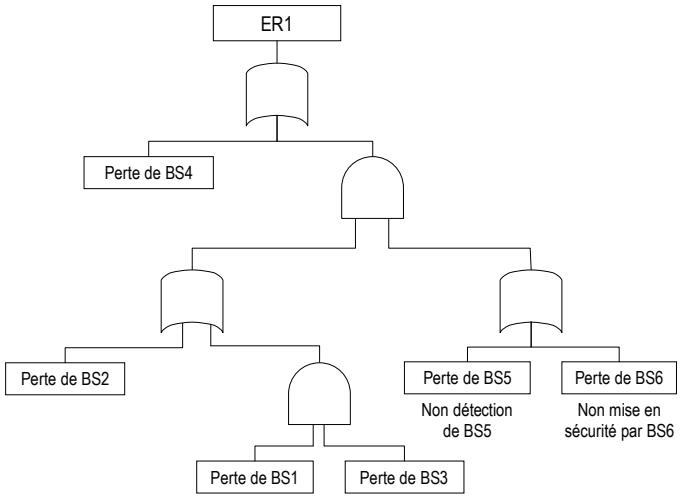
$ER1 = (\overline{BS5} \vee \overline{BS6}) \wedge [(\overline{BS1} \wedge \overline{BS2}) \vee (\overline{BS2} \wedge \overline{BS3}) \vee (\overline{BS1} \wedge \overline{BS3}) \vee (\overline{BS4} \wedge (\overline{BS1} \vee \overline{BS2} \vee \overline{BS3}) \vee \overline{BS2}]] \vee \overline{BS4}$

$ER1 = (\overline{BS5} \vee \overline{BS6}) \wedge [(\overline{BS1} \wedge \overline{BS2}) \vee (\overline{BS2} \wedge \overline{BS3}) \vee (\overline{BS1} \wedge \overline{BS3}) \vee \overline{BS2}]] \vee \overline{BS4} \vee [\overline{BS4} \wedge (\overline{BS5} \vee \overline{BS6}) \wedge (\overline{BS1} \vee \overline{BS2} \vee \overline{BS3})]$
$= (\overline{BS5} \vee \overline{BS6}) \wedge [(\overline{BS1} \wedge \overline{BS2}) \vee (\overline{BS2} \wedge \overline{BS3}) \vee (\overline{BS1} \wedge \overline{BS3}) \vee \overline{BS2}]] \vee \overline{BS4} \wedge [1 + ((\overline{BS5} \vee \overline{BS6}) \wedge (\overline{BS1} \vee \overline{BS2} \vee \overline{BS3}))]$
$= (\overline{BS5} \vee \overline{BS6}) \wedge [(\overline{BS1} \wedge \overline{BS2}) \vee (\overline{BS2} \wedge \overline{BS3}) \vee (\overline{BS1} \wedge \overline{BS3}) \vee \overline{BS2}]] \vee \overline{BS4}$

Enfin dans la première partie de l'équation, on peut faire les simplifications relatives à BS2 :

$ER1 = [(\overline{BS5} \vee \overline{BS6}) \wedge [(\overline{BS1} \wedge \overline{BS3}) \vee \overline{BS2}]] \vee \overline{BS4}$

L'arbre correspondant peut être établi pour les blocs structurels à partir des analyses précédentes :



Sur l'arbre précédent, la spécificité de stratégie de sécurité des produits considérés apparaît sous la forme de l'opérateur ET reliant les BS réalisant les fonctions (BS1, BS2 et BS3) à la stratégie de sécurité. L'ER apparaît dans le cas de l'occurrence d'une défaillance non détectée sur un BS ou pour laquelle BS6 ne serait pas en état de mettre en sécurité le produit.

Dans une forme pratique, il est possible, par l'analyse de la matrice M[F/BS], d'établir des relations logiques d'association des BS. Les BS réalisant la fonction sont liés entre eux par un opérateur OU ; ils sont liés aux blocs réalisant leur contrôle ou leur sécurité par un opérateur ET. Les BS assistant une fonction par apport d'énergie

(informations issues de M[F/BS] et M[BS/BS]) induisent dès l'occurrence d'une défaillance les affectant la perte de la fonction assistée.

5.3.4. Analyse en temps réel (Activité 3.4)

Nous avons présenté jusqu'ici les études réalisables en utilisant les matrices et les calculs associés. Nous allons montrer maintenant que les matrices peuvent aussi être utiles à la réalisation d'études en temps réel durant le PRAO (analyse accélérée) pour traiter des points particuliers. Ces analyses peuvent varier en fonction du problème considéré.
Nous proposons l'exemple du dédoublement d'une fonction sur deux blocs structurels de même nature avec une répartition de la "charge" entre les deux blocs. Cet exemple est illustré sur la Figure IV-21 par les blocs BS1 et BS2.

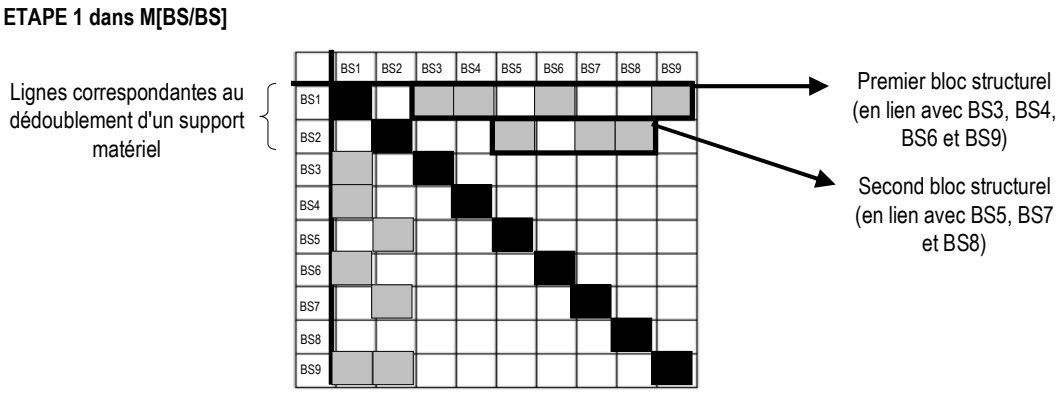


Figure IV-21 : Analyse temps réel dans le PRAO

Sur la figure précédente, chaque bloc dédoublé est lié à différents blocs ; la défaillance de BS1 implique la perte de BS3, BS4, BS6 et BS9 ; celle de BS2 implique la perte de BS5, BS7 et BS9. Après l'identification de l'impact au niveau structurel de la défaillance des blocs dédoublés, l'étape suivante consistera à identifier dans M[F/BS] l'impact de ces défaillances au niveau fonctionnel.
L'étape n°2 est illustrée sur la Figure IV-22.

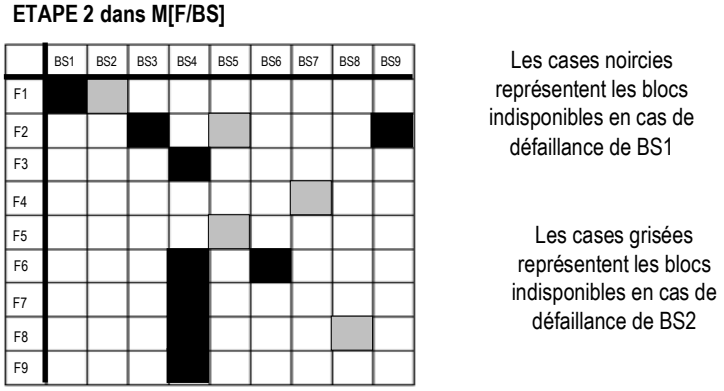


Figure IV-22 : Illustration de l'étape n°2

L'analyse de la matrice montre qu'en cas de défaillance de BS1, les fonctions F1, F2 et F8 sont dégradées et que les fonctions F3, F6, F7 et F9 sont indisponibles. De façon identique, la défaillance de BS2 implique que F1, F2 et F9 sont dégradées et F4 et F5 indisponibles.
L'indisponibilité des différentes fonctions pour chaque cas permet d'identifier la conséquence sur le système et, si les

conséquences sont trop importantes, d'adapter la répartition des fonctionnalités différemment sur les deux blocs structurels dédoublés.

L'analyse précédente peut être appliquée au niveau plus détaillé d'un bloc particulier auquel on s'intéresse plus particulièrement comme, par exemple, celui qui commande les sorties.

Le BS de Commande des sorties peut être composé de plusieurs canaux de commande des sorties. Pour identifier les cas de défaillance dans lequel le système sera sécurisé, le bloc peut être modélisé sous la forme de quatre sous-blocs pour identifier les situations qui ne respectent pas le nombre de sorties nécessaires pour avoir un état correct vis à vis de la sécurité. Par exemple, pour l'ABS, on considère que le système est encore en sécurité si deux ou trois sorties parmi les quatre sont bien commandées. Cette analyse à un niveau de détail plus fin que précédemment permet de caractériser les situations correspondant à un mode normal, un mode dégradé ou un mode dans lequel le système peut être une source de danger.

Finalement, le dernier type d'analyse en temps réel réalisable à partir des matrices concerne l'identification des chaînes d'informations à l'intérieur du calculateur via les interactions définies. A partir de la modélisation des relations de type échange d'information, on peut visualiser aisément les différents flux d'informations dans la matrice.

		Fournir les données extérieures à l'application client			Piloter	Envoyer la commande aux actionneurs et les informations vers l'extérieur		
		Acquérir	Traiter	Transmettre	Piloter	Acquérir	Traiter	Transmettre
Fournir les données extérieures à l'application client	Acquérir		[1 I R/.]					
	Traiter	[0 . R/.]		[1 I R/.]				
	Transmettre		[0 . R/.]		[1 I R/.]			
Piloter	Piloter			[0 . R/.]		[1 I R/.]		
Envoyer la commande aux actionneurs et les informations vers l'extérieur	Acquérir				[0 . R/.]		[1 I R/.]	
	Traiter					[0 . R/.]		[1 I R/.]
	Transmettre						[0 . R/.]	

Figure IV-23 : Visualisation des flux d'informations

Cette notion est visualisée sur l'extrait de matrice de la Figure IV-23 par l'exemple d'un regroupement illustré sur la diagonale. En réorganisant les colonnes des matrices M[F/BS] et M[BS/BS], on peut restituer sous une forme visuelle l'impact de la défaillance (ou perte) d'un bloc sur ces chaînes d'informations. Dans l'extrait de matrice précédent, les vecteurs [1 I R/.] représentent un transfert d'information de l'élément de la ligne vers l'élément de la colonne correspondant dans le cadre de l'information. La chaîne d'information représentée par le regroupement sur la diagonale part d'Acquérir les données extérieures et arrive à Transmettre les données vers l'extérieur, elle représente l'ensemble de la chaîne de traitement des données dans le produit.

5.3.5. Analyse des défaillances de mode commun (Activité 3.5)

Les défaillances de mode commun sont directement visualisables sur les matrices M[F/F], M[F/BS] et M[BS/BS] par les colonnes ou lignes pleines dans les matrices mettant en évidence les BS ou les fonctions nécessaires aux autres BS ou fonctions selon la matrice considérée. Une illustration est donnée sur la matrice de la Figure IV-24 dans laquelle apparaissent de manière évidente les situations particulières du Microcontrôleur et de l'Alimentation dont les défaillances

impactent l'ensemble des autres blocs structurels.

	Connecteur	Dispositif mise en forme des entrées analogiques	Dispositif mise en forme des entrées fréquentielles	Driver CAN	Microcontrôleur	Application client	Mémoire	Driver sortie 1	Alimentation 1	Watchdog	Dispositif de mise en sécurité
Connecteur		[1 I R/.]	[1 I R/.]	[1 I R/.]	[1 I R/.]			[0 . R/.]	[0 . A/.]		[1 -1 _ _]
Dispositif mise en forme des entrées analogiques	[0 . R/.]				[1 I R/.]				[0 . A/.]		
Dispositif mise en forme des entrées fréquentielles	[0 . R/.]				[1 I R/.]				[0 . A/.]		
Driver CAN	[0 . R/.]				[2 I R/.]				[0 . A/.]		
Microcontrôleur	[0 . R/.]	[0 . R/.]	[0 . R/.]	[2 I R/.]		[2 I R/.]	[2 I R/.]	[1 I R/.]	[0 . A/.]	[2 I ./C]	[0 . ./S]
Application client					[2 I R/.]				[0 . A/.]		
Mémoire					[2 I R/.]				[0 . A/.]		
Driver sortie 1	[1 I R/.]				[0 . R/.]				[0 . A/.]		
Alimentation 1	[1 E A/.]	[1 E A/.]	[1 E A/.]	[1 E A/.]	[1 E A/.]		[1 E A/.]	[1 E A/.]		[1 E A/.]	[1 E A/.]
Watchdog					[2 I ./C]				[0 . A/.]		[1 I R/S]
Dispositif de mise en sécurité	[1 I ./S]				[1 I ./S]				[0 . A/.]	[0 . ./S]	

Figure IV-24 : Visualisation défaillances de mode commun

Nous avons présenté l'ensemble des analyses SdF directement réalisables à partir des matrices ; les étapes suivantes portent sur l'évaluation de la charge de travail et de l'impact sur le produit.

5.4. Etape 4 : Evaluation de l'impact du traitement des exigences SdF sur la démarche durant le développement

Nous avons jusqu'ici défini les activités relatives à l'analyse SdF du produit à partir des attributs et des matrices. Nous nous intéressons maintenant aux coûts relatifs à la SdF et, plus particulièrement ici, au coût relatif à l'engagement d'une démarche SdF dans le développement futur (dans le cas de l'acceptation de l'offre par le client).

Pour évaluer ce coût, trois étapes sont nécessaires :

- le dimensionnement des durées de réalisation des différentes études par la définition de paramètres d'estimation et la notion de durée moyenne d'étude,
- le dimensionnement des ressources engagées par la définition d'équipe minimale, moyenne et maximale,
- le dimensionnement des coûts basé sur un coût horaire moyen et calculé à partir des deux dimensionnements précédents.

5.4.1. Estimation des durées

La démarche générale a été rappelée dans le paragraphe 4.3 et est composée de cinq méthodes chaînées :

- l'analyse fonctionnelle externe (AFE),
- l'analyse fonctionnelle interne (AFI),
- l'analyse préliminaire des risques (APR),
- l'analyse des modes de défaillances, de leurs effets et de leur criticité (AMDEC),
- la méthode des arbres de défaillances (AdD).

Nous décrivons comment définir le dimensionnement de la durée des études puis nous développons pour, chaque

étude, les paramètres à considérer pour cette estimation.

Pour chaque méthode, nous nous sommes intéressés à ses principes de réalisation en analysant les descriptifs d'emploi des outils qu'elle utilise, des procédures liées et les résultats d'études déjà menées dans l'entreprise partenaire ou renseignés dans différents articles.

A partir de cette analyse, nous avons établi des fiches d'estimation pour chaque méthode reprenant les étapes de réalisation et la connaissance relative au produit pour l'estimation de la durée.

L'estimation de la durée globale d'une étude n'est pas aisée pour un certain nombre de méthodes. Pour cette raison, nous avons préféré décomposer les étapes de réalisation de l'étude afin d'identifier des paramètres d'estimation à un niveau de détail plus important.

Nous commençons par le dimensionnement de la durée de l'analyse fonctionnelle externe.

L'analyse fonctionnelle externe peut être définie à un haut niveau d'abstraction pour chaque type de produit. En effet, quel que soit le produit, les environnants à un niveau d'abstraction élevé sont ceux présentés sur la Figure IV-25. Les actionneurs et les capteurs diffèrent pour les différentes familles ; l'environnement (le produit pouvant être placé à différents endroits du véhicule) et les autres ECU en relation peuvent varier. C'est aussi le cas de l'application client qui peut être réalisée en interne dans certains projets. Ces éléments (encadrés sur la Figure IV-25) doivent être définis préalablement pour chaque type de produit.

L'AFE revêt un caractère générique pour chacune des trois premières familles de produits (ABS, Suspension, Direction). Par contre, elle doit être réalisée pour les produits de la quatrième famille.

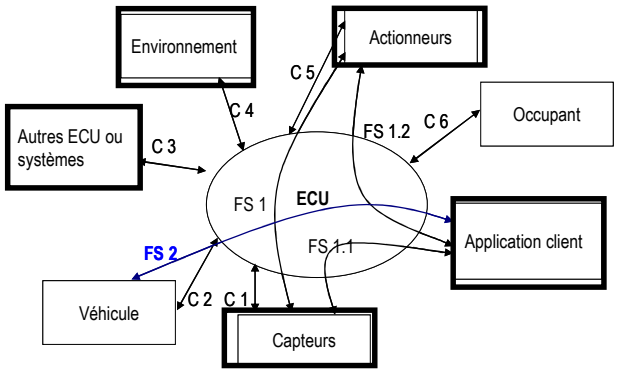


Figure IV-25 : Eléments à définir pour chaque famille

Le dimensionnement de la durée de l'AFE dépend directement du type de produit puisque, même dans le cadre générique des trois familles de produits usuels, l'équipe acquisition devra tout de même valider l'analyse générique et en préciser les détails (capteurs, actionneurs, environnement et autres ECU).

La durée moyenne de l'AFE, notée $d_{M\_AFE,}$ est estimée à partir du retour d'expérience. L'ordre de grandeur de d_{M_AFE} est d'environ trois heures. Afin d'estimer la durée de l'AFE, notée d_{AFE}, nous introduisons des facteurs de pondération :

- P_{connu} pour les trois premières familles avec $P_{connu} < 1$,
- $P_{inconnu}$ pour la quatrième famille de produit avec $P_{inconnu} > 1$.

Globalement, pour un produit "connu", l'AFE dure environ deux heures et quatre heures et plus pour un produit "inconnu" (cf. retour d'expérience sur les cas passés).

La seconde étude de la démarche SdF est l'analyse fonctionnelle interne (AFI). Elle consiste en la décomposition successive des fonctions en sous-fonctions jusqu'à l'obtention de fonctions techniques supportées par des blocs structurels représentatifs des principes de solution retenus. La première étape est assimilable au paramétrage de la matrice M[F/F] qui permet de créer les liens entre les sous-fonctions. La deuxième étape, débouchant sur l'identification des blocs structurels, s'apparente au paramétrage de la matrice M[F/BS] qui conduit à affecter à chaque fonction son support de réalisation. Finalement, le schéma bloc de principe de la solution est obtenu sous une forme matricielle par le biais du paramétrage de la matrice M[BS/BS].

La durée de l'AFI, notée d_{AFI}, est donc assimilée à la durée de paramétrage des matrices que nous estimons évoluer entre une et trois heures (cf. retour d'expérience sur les cas passés). La durée varie peu puisque, en règle générale, les matrices ont des dimensions comparables, il existe peu de variation du nombre de fonctions ou de blocs structurels.

La troisième étude est une analyse préliminaire des risques (APR) dont l'objectif est :

- soit de définir les ER par rapport aux modes de défaillance des différentes fonctions,
- soit d'identifier les causes des ER au niveau de détail du bloc structurel.

Cette activité est assimilable à l'identification des conditions de défaillance des fonctions induisant l'apparition des évènements redoutés comme cela est indiqué dans les matrices de conditions.

La durée de l'APR, notée d_{APR}, est donc assimilée au temps passé à définir les conditions d'apparition des ER. Nous estimons cette durée à quelques heures en fonction de la complexité du produit (entre deux et quatre heures) (cf. retour d'expérience sur les cas passés). De la même manière que pour les études précédentes, la durée de l'APR pourrait être paramétrée en fonction du nombre d'ER ou de la complexité du produit cependant le niveau d'identification des causes étant fixé au niveau du BS, la durée estimée est raisonnable.

La quatrième étude est l'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC). Cette étude a pour objectif d'analyser l'ensemble des modes de défaillance des fonctions, leurs effets et leurs causes au niveau matériel.

Le dimensionnement de la durée de cette étude sera effectué par la définition de différents paramètres dont la méthode de définition est donnée ci-dessous.

Considérons un cadre AMDEC générique (i.e. tableau support à la réalisation de l'AMDEC) tel celui donné sur la Figure IV-26.

Fonction	Modes de défaillances	Effets	Causes	Gravité G	Fréquence F	Sévérité S	Criticité C	Plan/Actions
Fonction considérée F	Perte de F Dégradation de F F intermittente Absence de F F intempestive	Impact sur le système de la défaillances	Causes de la défaillances	À coter en fonction des grilles utilisées	À coter en fonction des grilles utilisées	À coter en fonction des grilles utilisées	= GxFxS	Actions recommandées pour éviter la défaillance

Figure IV-26 : Grille AMDEC

L'analyse d'une fonction comporte l'étude de ses modes de défaillances et, pour chaque mode, l'étude des causes possibles. Pour le PRAO, le niveau de détail considéré est celui du BS. Nous avons décomposé l'étude AMDEC en un ensemble de cas à étudier. Un cas représente l'analyse d'un BS impliqué dans le mode de défaillance d'une fonction. Un

extrait de la fiche d'estimation est présenté sur la Figure IV-27

Formalisme	☐ client	☐ interne			
Nombre de fonctions		issu de M[F/F]			
Modes de défaillances considérés	☐ Perte de F	☐ Dégradation de F	☐ Absence de F à la sollicitation	☐ F intempestive	
Liste des blocs potentiellement impliqués dans la défaillance de Fi	F1 : ☐ BS1 ☐ ... ☐ BSn	.....	Fn : ☐ BS1 ☐ ... ☐ BSn	liste des blocs extrait du fichier de sélection des blocs	

Figure IV-27 : Extrait fiche estimation AMDEC

Le format de réalisation ou l'outil support à l'étude peut être imposé par le client ; ceci est représenté par le premier choix "format de réalisation client ou interne" sur la fiche d'estimation.

Le second choix à effectuer est celui du nombre de fonctions du produit à étudier.

Le troisième choix concerne la définition des modes de défaillance à étudier ou ceux pertinents pour le produit considéré.

Enfin, pour chaque fonction, il faut définir à l'aide de la matrice M[F/BS] les blocs structurels qui peuvent être impliqués dans la défaillance de la fonction (BS supportant la fonction).

A partir de cette étape, le nombre de cas à étudier est connu. On observe que ce nombre de cas est directement corrélé au nombre de BS à étudier par fonction.

Nous avons également défini pour cette étude une durée moyenne de réalisation basée sur le nombre de cas à traiter. Cette durée moyenne par analyse d'un BS, notée $d_{M\_AMDEC/BS}$, est obtenue à partir du retour d'expérience.

Nous exploitons ensuite la connaissance disponible sur les différents BS afin d'affiner l'estimation de cette durée. Les attributs renseignant le type de BS que le concepteur a sélectionné sont :

- "connu" pour un BS déjà utilisé,
- "adapté" pour un BS adapté d'une solution connue,
- "inconnu" pour un BS non déjà utilisé.

Comme présenté sur la Figure IV-28, on peut affiner l'estimation de la durée en configurant le type de bloc pour chaque fonction.

Type de blocs sélectionnés (issu des attributs)	Nombre de blocs connus Nombre de blocs inconnus Nombre de blocs adaptés	.....	Nombre de blocs connus Nombre de blocs inconnus Nombre de blocs adaptés
Nombre de cas connus (pour chaque F)	$\sum_{Fi}(\text{nombre Modes défaillances de } Fi)\times(\text{nombre de blocs connus en lien avec } Fi)$		
Nombre de cas inconnu (pour chaque F)	$\sum_{Fi}(\text{nombre Modes défaillances de } Fi)\times(\text{nombre de blocs inconnus en lien avec } Fi)$		
Nombre de cas adaptés (pour chaque F)	$\sum_{Fi}(\text{nombre Modes de défaillances de } Fi)\times(\text{nombre de blocs adaptes en lien avec } Fi)$		

Figure IV-28 : Estimation par rapport à la connaissance disponible

Pour différencier les différents cas, nous définissons des facteurs de pondération fonction du type de bloc :

- P_{connu} pour les blocs déjà utilisés avec $P_{connu} < 1$,

- $P_{adapté}$ pour les blocs adaptés avec $P_{adapté} \approx 1$,
- $P_{inconnu}$ pour les autres avec $P_{inconnu} > 1$.

Par rapport à la durée moyenne définie, la durée d'étude d'un cas sur un bloc inconnu sera donnée par la formule : $d_{AMDEC/BS} = P_{inconnu} \times d_{M\_AMDEC/BS}$.

Il faut enfin rajouter l'étude des fonctions contraintes qui permettront de vérifier que le produit supporte les contraintes de son environnement. Le mode de paramétrage est présenté sur la Figure IV-29 dans laquelle apparaît le nombre de fonctions contraintes ainsi que le nombre de blocs mécaniques (boîtier, couvercle, joint, vis) et la carte électronique (circuits imprimés) sur laquelle seront placés les composants.

Nombre de fonctions contraintes du type respect EMC, Humidité	issu de l'étude des produits	**Nombre de blocs Mécanique + 1 pour le calculateur (PCB + composant)**	issu de l'étude des produits	**Nombre de cas fonctions contraintes**	= nombre de fonctions x nombre de blocs

Figure IV-29 : Fonctions contraintes

Les éléments présents dans les figures précédentes peuvent être facilement extraits du paramétrage des matrices. En effet, on obtient via :

- la matrice M[F/F] : le nombre de fonctions du produit,
- la matrice M[F/BS] : le nombre de blocs pouvant avoir un impact sur chaque fonction,
- le paramétrage des blocs : le type de blocs structurels (connu, adapté, inédit),
- l'AFE : le nombre de fonctions contraintes du produit.

La durée totale de l'AMDEC, notée $d_{AMDEC,}$ est obtenue en ajoutant les durées d'étude de tous les blocs structurels.

$$d_{AMDEC} = \sum_{\text{ensemble des fonctions des modes de défaillance et des BS associés}} d_{AMDEC/BS}$$

Par retour d'expérience, l'ordre de grandeur de la durée moyenne pour l'étude d'un cas particulier est estimé à quelques heures (trois à cinq heures). En effet, certaines estimations donnent une cadence de réalisation d'une AMDEC de 10 lignes par heure. Pour un produit composé de 500 composants supposés équi-répartis dans les BS, on obtient 50 composants par BS. L'étude d'un cas pouvant être assimilé à l'étude des défaillances des composants d'un BS, il faudra étudier 50 composants par cas soit cinq heures au plus (en considérant une ligne d'AMDEC par composant défaillant dans l'analyse d'un mode de défaillance d'une fonction).

La cinquième méthode est celle des arbres de défaillances (AdD). L'objectif est d'identifier, pour chaque évènement redouté, les causes de cet évènement et sa fréquence d'apparition afin de vérifier si la fréquence d'apparition de cet évènement respecte bien les spécifications client.

De la même manière que pour l'AMDEC, l'analyse a débutée par l'étude du mode de réalisation d'un ER. Nous proposons sur la Figure IV-30 un exemple d'AdD pour un ER.

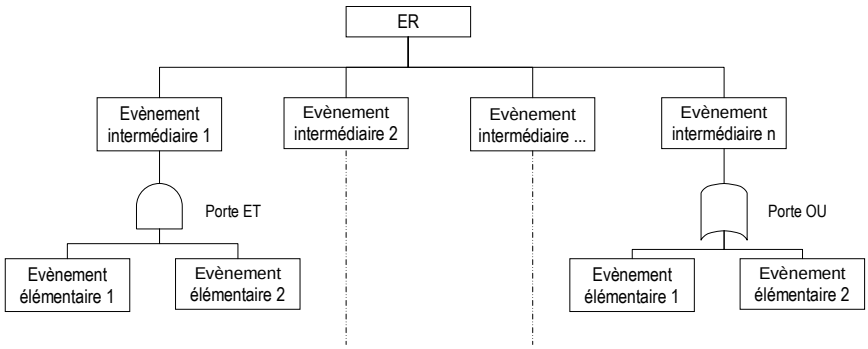


Figure IV-30 : Exemple arbre de défaillances

La racine de l'AdD est l'occurrence de l'ER, il faut donc un arbre par ER. Intéressons nous à la connaissance disponible afin d'estimer la durée nécessaire à l'élaboration de l'arbre.

La matrice de condition définit l'ensemble des défaillances des fonctions conduisant à un ER ; ceci permet d'obtenir pour chaque évènement redouté le nombre de causes à étudier i.e. le nombre de BS susceptibles d'être à l'origine de la défaillance (ceci est illustré par les cinq premières lignes de la Figure IV-31).

Formalisme	☐ client	☐ interne	
Nombre d'ER			
Nombre de conditions par ER	Nombre de conditions ER1 =	.....	Nombre de conditions ERn =
Liste des fonctions pour chaque condition	C1(ER1) : ☐ F1 ☐ ..... ☐ Fn C2(ER1) : ☐ F1 ☐ ..... ☐ Fn		C1(ERn) : ☐ F1 ☐ ..... ☐ Fn
Nombre de BS pour chaque fonction issu de M[F/BS]	Liste des blocs pour chaque fonction pour lesquels la première information de N est égale à R ou A		Liste des blocs pour chaque fonction pour lesquels la première information de N est égale à R ou A
Liste des BS liés aux précédents pour la réalisation ou l'assistance	Liste des BS pour chaque BS précédent pour lesquels la première information de N est égale à R ou A	.....	Liste des BS pour chaque BS précédent pour lesquels la première information de N est égale à R ou A
Liste des BS liés aux précédents pour la sécurité, le contrôle ou la protection	Liste des BS pour chaque BS précédent pour lesquels la seconde information de N est égale à S, C ou P		Liste des BS pour chaque BS précédent pour lesquels la seconde information de N est égale à S, C ou P
Nombre de causes estimé par fonction et par arbre	Pour chaque condition et pour chaque fonction : Nombre de causes par fonction = (nombre de BS liés à F + Nombre de BS liés au précédent pour R ou A) Nombre de causes par arbre = ∑(sur l'ensemble des conditions et sur l'ensemble des fonctions du [(nombre de BS liés à F + Nombre de BS liés au précédent pour R ou A)]		

Figure IV-31 : Fiche d'estimation de la durée d'un arbre de défaillances

Les trois dernières lignes sont destinées :

- pour la quatrième ligne, à analyser les BS pouvant être impliqués dans la défaillance d'un autre BS (liste des BS ayant un lien de réalisation ou d'assistance avec ceux réalisant les fonctions),
- pour la cinquième ligne, à aider l'équipe projet dans le développement futur, en indiquant les BS ayant un lien de contrôle C, sécurité S ou protection P avec ceux réalisant les fonctions dans le but de mettre en évidence les barrières de sécurité (qui devront figurer dans l'arbre de défaillances),
- pour la dernière, la définition de la manière avec laquelle le nombre de causes de chaque arbre est calculé.

Comme pour les études précédentes, le retour d'expérience permet de fixer une durée moyenne par cause notée $d_{M\_AdD/cause}$.

La durée estimée d'établissement de l'AdD associé à un ER sera établie par :

d_{AdD} (ERi) = nombre de causes de l'ERi x $d_{M\_AdD/cause}$

et la durée totale de l'étude des ER, notée D_{AdD}, par :

$$D_{AdD} = \sum_{\text{ensemble des ERi}} d_{AdD}(ERi)$$

5.4.2. Estimation de la charge de travail en fonction des ressources

Après avoir déterminé la durée totale de réalisation des analyses de SdF et avant de nous intéresser au coût de réalisation des études SdF, nous estimons les ressources engagées et la charge de travail afférente pour la réalisation des analyses SdF dans le PRAO pour l'AFE, l'AFI et l'APR et dans le développement futur pour l'AMDEC et les AdD.

Nous considérons essentiellement ici des ressources humaines i.e. des acteurs nécessaires à la réalisation des études. Nous ne tenons pas compte des ressources matérielles (support ou outil de réalisation,…,) qui sont négligeables vis-à-vis des précédentes.

La charge de travail est généralement fonction de la durée totale des études et du nombre de ressources disponibles. Le calcul prend comme hypothèse que les activités peuvent être réparties entre les acteurs. Dans le cadre d'étude SdF, la durée n'est pas fonction du nombre de ressources puisque les études sont réalisées dans le cadre de réunions réunissant l'ensemble des acteurs. Dans notre cas, la charge de travail sera estimée par le produit de la durée totale des études et du nombre de personnes nécessaires à l'étude.

Comme nous l'avons rappelé au paragraphe 3.3, les analyses SdF sont généralement réalisées par une équipe pluridisciplinaire représentant les principaux métiers impliqués dans la réalisation du produit. Généralement, sont définis les rôles et responsabilités suivants [Qualite_online, WEB] :

- le pilote technique : il a la responsabilité de l'étude jusqu'à l'aboutissement des actions,
- l'animateur : il est garant de la méthode,
- le représentant qualité : il apporte son expérience sur les objectifs de qualité et fiabilité, l'historique des problèmes rencontrés,…,
- les représentants études : leurs métiers sont fonction du produit considéré,
- un représentant fabrication : il apporte son expérience sur les problèmes rencontrés durant la production de produits précédents,
- des spécialistes ou experts : ils apportent leur savoir sur un sujet donné en fonction des besoins.

Dans les cas étudiés dans notre étude, les rôles de pilote technique, animateur et représentant qualité sont assurés par une même personne issue de la qualité et les représentants études sont ceux de l'électronique, du logiciel et de la mécanique. Il est fréquent qu'un représentant de la fabrication participe à la réalisation des études et, enfin, les experts interviennent occasionnellement en fonction des besoins.

Par le retour d'expérience et en fonction du type de produit considéré, il est possible de fixer une équipe moyenne dont le nombre de personnes est noté N_{M_P}. A partir de la définition de ce dernier, il est possible de calculer la charge de travail totale notée CT à partir de la formule :

$CT = D_{SdF\_étude} \times N_{M\_P}$

Les études SdF durant le développement sont généralement réalisées durant des réunions permettant la rencontre de tous les participants. Les réunions sont organisées généralement sur un créneau de deux heures et sont hebdomadaires, voire bihebdomadaires, en fonction de la disponibilité des acteurs projets et de la réactivité requise. Il paraît alors intéressant de définir, une durée en nombre de semaine qui permette d'anticiper la date de début de l'étude en fonction de la date limite à laquelle le client souhaite recevoir les résultats.

5.4.3. Estimation du coût

Le coût estimé ici est limité au coût relatif à l'engagement de la démarche SdF standard définie précédemment. Nous avons estimé la durée de chaque étude, les ressources nécessaires et, par association de ces deux éléments, la charge de travail afférente qui représente l'ensemble des heures qu'il faudra prévoir pour l'application de la démarche SdF complète.

Pour obtenir le coût, il faut établir un coût horaire moyen, noté C_{M_H}, pour la réalisation des études. Ce type d'estimation est classique dans les entreprises qui, pour chaque projet, calculent les coûts en fonction des hommes/mois nécessaires à sa réalisation. Il est aussi possible de différencier le coût horaire de chaque type de ressources : techniciens, ingénieurs, chef de projet,…, en caractérisant le type des ressources dans l'étape précédente. Dans cette configuration, pour chaque type de ressource, il faut estimer la charge de travail afférente et par le coût horaire moyen adapté, le coût de l'engagement de la démarche SdF.

Dans le cas où l'hypothèse est faite que le coût horaire moyen peut être utilisé pour l'ensemble des ressources, le coût de l'engagement de la démarche SdF, noté $C_{SdF\_démarche}$, est obtenu par :

$$C_{SdF\_démarche} = D_{SdF\_étude} \times N_{M\_P} \times C_{M\_H}$$

5.4.4. Bilan de l'impact démarche SdF

Dans cette quatrième étape, nous avons montré comment estimer :

- la durée de chaque type d'étude,
- les ressources nécessaires à leur réalisation et la charge de travail correspondant,
- le coût de l'engagement de la démarche SdF.

Nous obtenons l'estimation du coût $C_{SdF\_démarche}$ via la relation complète suivante :

$$C_{SdF\_démarche} = (d_{AFE} + d_{AFI} + d_{APR} + d_{AMDEC} + D_{AdD}) \times N_{M\_P} \times C_{M\_H}$$

Les hypothèses posées ici peuvent être modifiées dans différents cas comme nous explicitons ci-dessous :

- les ressources nécessaires diffèrent d'une étude à l'autre, la charge de travail doit être estimée séparément pour chaque étude,
- des études spécifiques "métier" doivent être réalisées ; deux situations sont possibles :

- soit l'étude métier utilise une méthode déjà paramétrée précédemment (une AMDEC électronique, par exemple), il faut alors reprendre le même principe d'estimation : renseignement des paramètres d'estimation pour obtenir la durée, identification des ressources nécessaires, estimation du coût,
- soit l'étude métier utilise une méthode différente et il faudra en plus des activités précédentes définir les paramètres d'estimation de durée pour celle-ci,

- le coût horaire moyen diffère selon la ressource engagée ; il faudra estimer pour chaque type de ressources le nombre, la charge de travail et le coût correspondant.

Enfin, les premières estimations réelles proposées dans notre démonstration sont extraites de l'expertise des cas passés ; par une consignation des durées réelles observées dans le traitement des prochains AO, ces estimations pourront être affinées.

Nous avons considéré dans cette partie uniquement les coûts relatifs à l'engagement des méthodes d'analyse SdF ; il est possible de prendre en compte le coût d'autres activités SdF tels que la mise en œuvre de tests de résistance, d'essais accélérés,…, qui pourra être obtenu par la même méthode : estimation des paramètres, des ressources et du coût.

5.5. Etape 5 : Evaluation de l'impact du traitement des exigences SdF sur le produit

Le cout SdF est fortement dépendant des solutions retenues afin de respecter les objectifs SdF imposés dans le cahier des charges. Le calcul de ce coût peut s'appuyer sur l'expertise de l'entreprise et, en particulier, sur les supports d'expérience relatifs au coût d'un produit. Nous avons présenté, dans le paragraphe 3.2.4 du chapitre 2, les différentes méthodes d'estimation des coûts (analogiques, paramétriques et analytiques) et défini brièvement les coûts relatifs aux différentes composantes (liées aux métiers) formant le produit.

Nous présentons ci-après, pour chacun des postes de coût relatifs aux métiers de l'entreprise partenaire (électronique, logiciel et mécanique), la méthode employé et dégageons les caractéristiques économiques en lien direct avec la SdF.

Remarque : l'apport méthodologique est limité car la détermination de ces coûts est très étroitement corrélée aux méthodes d'estimation des coûts qui sont propres à chaque entreprise.

5.5.1. Coût SdF électronique

Au niveau électronique, les coûts correspondent à ceux des composants électroniques utilisés dans la solution. La méthode d'estimation utilisée par l'entreprise partenaire est une méthode analogique basée sur le retour d'expérience. Un logiciel a été créé par l'entreprise pour le calcul de ces coûts. Il comprend l'ensemble des solutions déjà implémentées sur le produit pour chaque BS. Un BS existant est décrit par son nom, les composants constitutifs, leur quantité, leur référence dans les bases de données de coût de l'entreprise, leur coût unitaire et permet le calcul du coût total du BS. L'écran d'accueil du logiciel permet au concepteur de sélectionner les BS pertinents pour le cas considéré, le BS choisi est alors affiché sous la forme donnée sur la Figure IV-32, cet extrait est simplifié pour ne pas dévoiler le savoir-faire de l'entreprise.

BS	Composants	Quantité	Référence BD	Coût Composant	Coût BS
Alimentation	Régulateur	1	Reg1	Ca	
	Résistance type a	3	Rra	Cb	
	Condensateur type a	1	Rca	Cc	
	....	....	....	....	
					∑Ci

Figure IV-32 : Utilitaire d'estimation des coûts électroniques

Les BS déjà développés pour des projets précédents ont la particularité d'intégrer une part relative à la SdF puisque les contraintes SdF s'exerçaient déjà sur ces solutions. Pour cette raison, il faut définir, pour chaque BS ou pour la solution électronique complète, quel est le coût engendré par le respect des exigences SdF.

Deux approches sont possibles.

Une première approche, globale, consiste à considérer que certains BS sont directement liés à la SdF. En effet, comme nous l'avons défini dans le paragraphe 3.2.3 du chapitre 3, les degrés de liberté de conception sont fortement corrélés à la SdF. La configuration minimale définie permet d'assurer la réalisation de la mission du produit, elle comporte : les Dispositifs de mise en forme des entrées analogiques et fréquentielles, le Driver CAN, le Microcontrôleur, le Driver de sorties, l'Alimentation, l'Horloge. Les BS complétant cette configuration minimale : Watchdog ou Microcontrôleur secondaire, seconde Alimentation,…, sont directement liés à la SdF. La solution consiste donc à considérer que le coût SdF est établi en considérant la différence entre le coût total électronique et celui de la configuration minimale. Le coût SdF électronique noté C_{E_SdF} est alors obtenu par :

C_{E_SdF} = Coût total électronique – Coût des BS appartenant à la configuration minimale

Cette solution est facile à implémenter par rapport à l'existant dans l'entreprise partenaire.

La deuxième approche, qui conduit à une estimation plus détaillée du coût SdF, consiste à se placer au niveau du composant dans un BS particulier. Le coût SdF électronique peut être considéré comme le surcoût lié à la réalisation d'une augmentation de la fiabilité ou de la sécurité du BS. Pour implémenter cette solution, il faut pouvoir, pour chaque BS, définir une solution fonctionnelle qui satisfait aux seules exigences techniques sans tenir compte des exigences SdF. La première difficulté inhérente à cette solution réside dans la nécessité de définir, pour chaque BS, une solution fonctionnelle suffisamment générique pour être utilisable dans l'ensemble des projets afin de ne pas redéfinir celle-ci à chaque appel d'offre.

La seconde difficulté, lorsque la solution fonctionnelle est établie, concerne l'identification de la part relative à la SdF dans les solutions existantes i.e. le composants intervenant dans le BS à des fins uniques de SdF.

Suite à l'étude des produits et aux particularités de chaque méthode d'estimation des coûts, nous préconisons pour l'entreprise partenaire le choix de première solution qui consiste à chiffrer le coût SdF électronique comme le coût relatif aux éléments rajoutés à la configuration minimale.

5.5.2. Coût SdF logiciel

Au niveau logiciel, les coûts correspondent aux ressources nécessaires pour la réalisation des modules logiciels. Ces coûts sont estimés par rapport au type de module, au nombre de lignes relatives aux modules et à une cadence de développement du logiciel par rapport au nombre de lignes estimées. Pour ces coûts logiciels, l'entreprise partenaire a également développé un utilitaire basé sur une méthode analytique permettant l'estimation. Cet utilitaire prend en compte les différents modules logiciels à développer ; la définition du coût SdF peut s'appuyer sur une estimation séparée du coût des modules SdF et des autres. Les modules SdF sont les modules nécessaires au test du logiciel applicatif, les modules de test des différents blocs structurels (test de cohérence, test de vérification,...,) et le(s) module(s) relatif(s) à la stratégie de sécurité implémentée. Nous obtenons alors le coût SdF noté C_{L_SdF} par :

C_{L_SdF} = Coût du développement des modules SdF

5.5.3. Coût SdF mécanique

Au niveau mécanique, les coûts correspondent au coût matière nécessaire à la réalisation des pièces et au coût de fabrication de ces pièces. La méthode d'estimation du coût matière est paramétrique (i.e. fonction de la quantité de matière par rapport à la taille des pièces), celle de la fabrication est analytique et basée sur les technologies d'usinage envisagées. Le coût matière est estimé, par pièce, en fonction d'une approximation de la taille de la carte électronique qui sera insérée dans le boitier. La taille de cette carte permet d'estimer, en fonction des contraintes de l'environnement (EMC, échauffement des composants,...), la surface du boîtier et du couvercle associés ainsi que le type de joint nécessaire à l'isolation du produit. Le dimensionnement de cette surface conduit à l'évaluation du coût de la matière première. Le coût matière mécanique est donc lié à l'environnement dans lequel le produit évolue et à la taille de la carte électronique.

La définition d'un coût SdF mécanique suppose qu'il existe une solution non SdF. Les exigences à respecter sont étroitement liées aux contraintes du produit (résister à l'environnement, permettre la dissipation thermique,...) et il est difficilement envisageable de définir une solution standard non SdF qui ne répondrait pas aux contraintes précédentes. Dans cette application, il n'y a donc pas de coût mécanique lié à la SdF. Cependant, dans d'autres contextes, une pièce mécanique peut être utilisée pour réaliser des fonctions de sécurité ; dans ce cas là, un coût SdF mécanique pourra être défini.

5.5.4. Bilan de l'impact produit

Dans cette cinquième étape, nous avons présenté des pistes possibles pour l'estimation du coût SdF produit. Nous avons mis en évidence que cette estimation est très fortement liée aux méthodes d'estimation des coûts propres à chaque entreprise aussi seuls les principes de notre présentation sont génériques ; leurs modes d'application seront particularisés à chaque entreprise.

Nous avons cependant proposé ici l'analyse des coûts relatifs à l'électronique, au logiciel et à la partie mécanique pour obtenir l'estimation du coût SdF produit, noté $C_{SdF\_produit}$. Dans le cadre des produits considérés dans l'application, seuls les aspects électroniques et logiciels interviennent directement dans le coût SdF par la relation :

$C_{SdF\_produit} = C_{E\_SdF} + C_{L\_SdF}$

Après la réalisation des étapes 4 et 5, on obtient le coût SdF total, noté C_{SdF} par la relation :

$C_{SdF} = C_{SdF\_démarche} + C_{SdF\_produit}$

6. Conclusion

Les développements que nous avons proposés dans ce chapitre avaient pour objectif de montrer la méthodologie permettant d'estimer une valeur d'impact de la prise en compte des exigences SdF sur le produit et sur la démarche associée.

Nous avons tout d'abord défini la notion de valeur d'impact SdF, nous avons ensuite défini les exigences client que nous avons liées aux modèles présentés dans le chapitre 3. Nous nous sommes ensuite focalisés sur les étapes Projection et Evaluation et avons développé la méthodologie matricielle destinée à ces étapes. Enfin, tout au long du chapitre, nous avons illustré par des exemples les principes définis par rapport aux supports de connaissances de l'entreprise partenaire.

Les matrices définies forment un support efficace pour les analyses SdF en conservant une représentation facilement utilisable par les acteurs des phases d'acquisition ou de développement.

Les principaux résultats concernent l'utilisation de ces matrices pour l'analyse SdF du produit dans le PRAO et l'évaluation du coût de la démarche SdF. L'estimation du coût produit est si étroitement couplée à l'entreprise considérée, à ses méthodes d'estimation de coût et aux produits que la définition de coût SdF générique n'est pas envisageable.

L'organisation proposée et les supports utilisés sont aussi un outil efficace de capitalisation d'expérience puisque :

- d'une part, ils permettent de capitaliser la connaissance sur les blocs structurels via les attributs,
- d'autre part, jusque là réalisé implicitement les analyses ou les décisions relatives à la SdF sont détaillées et capitalisables pour chaque produit.

La méthode définie possède une propriété d'amélioration continue. En effet, pour chaque appel d'offre, les différentes étapes de la démarche d'évaluation de l'impact seront tracés via les matrices, les attributs, les fiches d'estimation de durée des études ainsi que les analyses SdF qui seront réalisées (et réutilisables puisque le modèle sur lequel s'appuie la connaissance sur le produit est générique) ce qui permettra pour les AO suivants de s'appuyer sur les cas passés pour optimiser l'évaluation. De plus, dans chaque projet acquis par l'entreprise suite à un AO, un effort devra être fourni sur la consignation des différentes durées des études pour pouvoir, à la fin du projet, comparer la durée prévue et la durée réelle afin d'ajuster les différents paramètres. Le dernier point concerne l'amélioration du traitement de la SdF dans les projets, par le biais de la méthodologie proposée, on traite la SdF au plus tôt ce qui permet :

- de prévoir les ressources nécessaires à son étude et donc d'anticiper,
- d'afficher pour tout acteur projet la charge de travail que cela représente,
- d'avoir une vision complète de la démarche.

Nous obtenons en sortie le coût total de la SdF dans un projet qui va permettre de mieux anticiper les problèmes SdF sur le produit et les besoins en termes de ressources pour les éléments relatifs à la SdF.

Cette méthodologie dont nous avons défini les principes mais aussi le mode de mise en œuvre est applicable à de nombreux contextes dès lors que le produit décomposable en fonctions et en blocs structurels.

CONCLUSION GENERALE

La sûreté de fonctionnement (SDF) est une préoccupation majeure pour les industriels. C'est le cas du secteur automobile et en particulier des équipementiers qui se voient imposer par les constructeurs des exigences de plus en plus fortes relativement au niveau de sûreté des systèmes qu'ils développent. La tendance inflationniste du nombre de spécifications SDF est induite par un double phénomène. Il s'agit tout d'abord de justifier de l'atteinte du niveau de sûreté requis par la démonstration préliminaire d'une démarche rigoureuse adaptée au contexte. Il s'agit ensuite de réaliser cette démonstration dès le stade de l'appel d'offre (AO).

Le travail de recherche présenté dans ce mémoire à donc abordé la problématique d'identification de la "dimension SdF" du produit au stade de l'AO et à l'évaluation de l'impact sur le développement futur de l'intégration des exigences correspondantes. Le chiffrage économique attendu devait intégrer à la fois les conséquences sur le produit en termes de robustesse mais aussi l'influence de la démarche d'analyse permettant de dimensionner les solutions appropriées.

Les produits concernés sont des équipements mécatroniques embarqués.

La démarche de recherche a conduit à une structuration du mémoire en quatre chapitres

Nous avons présenté dans le premier chapitre le contexte général des travaux, la problématique de recherche, sa formalisation et son positionnement par rapport aux travaux scientifiques du domaine. Nous avons successivement décrit le contexte de l'industrie automobile et la nature des produits fournis par les équipementiers (systèmes embarqués pluridisciplinaires). La problématique étant centrée sur la phase d'acquisition, nous avons alors proposé une représentation du processus de réponse à appel d'offre (PRAO) et son positionnement par rapport au processus de conception. L'analyse des contraintes du problème confrontée au contexte étudié nous a permis de conclure sur la nécessité de proposer une approche d'intégration de la Sûreté de Fonctionnement ciblée sur le PRAO et prenant en compte les routines de conception de l'entreprise. Les études conduites à ce stade du projet devaient en outre pouvoir être exploitées et amplifiées en phase de développement.

Dans le second chapitre, nous avons développé l'organisation du PRAO préconisée pour la prise en compte de la dimension SdF. La solution d'organisation comporte cinq étapes : Filtrage, Traduction, Projection, Evaluation et Restitution. L'approche proposée met de plus en jeu quatre plans d'abstraction et apporte des informations sur le caractère méthodologique et structurant de la solution d'organisation à mettre en place pour atteindre l'objectif fixé. L'organisation du PRAO à partir des documents "client" fournis dans le dossier de réponse à l'AO, conduit à l'évaluation économique de la prise en compte des exigences SdF dans le projet. La fin du chapitre est consacrée à un bilan des

supports de connaissance utiles au développement de l'organisation. Ces supports revêtent un grand intérêt puisque, durant le PRAO, les informations ne sont pas stabilisées (le produit n'existant pas) et il est donc important de s'appuyer sur le retour d'expérience des projets précédents.

Dans le chapitre 3, nous avons proposé un modèle produit multimétier intégrant la dimension SdF. L'analyse des produits considérés et les besoins identifiés dans les deux premiers chapitres nous ont permis de conclure à la pertinence de choix d'une représentation matricielle. Ce type de représentation possède de nombreux avantages tels que la facilité de paramétrage et d'utilisation. Les matrices apportent aussi un support commun pour l'ensemble des métiers constitutifs du produit. Deux types de matrices dites "intra-domaines" permettent de représenter les liens respectifs entre fonctions ou entre composants. Le troisième type de matrice dite "inter-domaine" caractérise les relations entre composants et fonctions. Nous avons associé à ces matrices des attributs destinés à formaliser et capitaliser les connaissances SdF ainsi que les choix de conception effectués durant le PRAO.

Le dernier chapitre est consacré au couplage entre l'organisation proposée et les modèles développés dans l'objectif de définir l'impact de la prise en compte des exigences SdF dans un projet et d'évaluer son coût. L'impact économique de la SdF est induit à la fois par les solutions intégrées au produit pour assurer la robustesse désirée mais aussi par la démarche méthodologique ayant conduit à la définition de ces solutions. Les étapes Projection et Evaluation et les activités qui permettent par analyse successive d'obtenir les conséquences du traitement de la SdF dans un projet ont été détaillées. Nous avons finalement présenté dans ce chapitre une méthode d'analyse SdF d'un produit depuis la création de son modèle par le paramétrage des matrices jusqu'à la définition du coût de prise en compte de la SdF. La simplicité des exemples illustratifs est justifiée, d'une part, par la nécessité de proposer des exemples compréhensibles par un lecteur non spécialisé dans les systèmes embarqués et, d'autre part, par le respect du savoir-faire de l'entreprise partenaire.

Dans le détail, les principaux résultats pratiques qui accompagnent la méthodologie mise en place dans ce travail concernent :

1. la création d'une **organisation du PRAO** permettant la prise en compte de la dimension SdF et l'évaluation économique de son impact dans un projet. Cette organisation repose :
    - sur une instrumentation des différentes étapes conduisant à l'établissement d'une réponse rapide et appropriée au cahier des charges d'un client
    - sur l'intégration des connaissances métiers déjà présentes au sein de l'entreprise.
2. la **formulation d'une connaissance** extraite de la structure industrielle et formalisée sous forme :
    - brute par l'utilisation de supports nécessaires à l'instanciation des différentes étapes. Sur ce plan nous avons vu qu'on pouvait distinguer quatre types de supports selon qu'ils soient issus de l'expertise métier, du retour d'expérience ou bien qu'ils soient tirés des normes ou des procédures en vigueur dans l'entreprise.

- analytique par une représentation matricielle mettant en jeu des vues fonctionnelles et structurelles complétées par des informations, localisées aux intersections et révélant, à partir de certains attributs, la nature des connexions considérées. Cette représentation matricielle facilite le design rapide de solutions préliminaires et conduit à une rapide estimation de l'impact SdF correspondant.

3. la **caractérisation d'une démarche d'implémentation** d'une méthodologie de ce type via :
   - un état des lieux et la définition d'un questionnaire permettant, à l'instar d'un audit interne, d'évaluer le niveau de maturité de l'entreprise sur le plan de la connaissance des outils et méthodes de sûreté de fonctionnement.
   - l'identification de plans d'abstraction autorisant une structuration de la réflexion à conduire pour la définition de l'organisation.
   - la recherche de généricité des modèles développés pour une instanciation dans des contextes différents de celui considéré dans le cadre de ce travail relatif à l'électronique embarquée dans l'automobile.

A un niveau plus général, la méthodologie proposée permet, en plus d'un renforcement de l'efficacité du PRAO pour le traitement de la SdF, l'affichage envers le client du savoir-faire SdF de l'entreprise dès les premières prises de contact. Elle offre également une vue du processus SdF complet (et de la charge de travail afférente) pour l'ensemble des acteurs. La méthodologie facilite la capitalisation d'expérience pouvant être ultérieurement réengagée dans les nouveaux projets. Les résultats finaux de cette étude permettront d'assister les acteurs concernés par la phase d'acquisition dans leur tâche de définition des architectures préliminaires en intégrant la dimension fiabiliste et sécuritaire attendue par le client à partir de la caractérisation de la démarche nécessaire pour y arriver

Notons enfin que la solution envisagée s'appuie sur des modèles possédant de fortes qualités de généricité notamment via les matrices dont les fonctions ou les blocs structurels peuvent être modifiés, complétés ou réduits en fonction du contexte et du type de produit. Les informations véhiculées par les liens mis en évidence au sein d'une matrice peuvent en outre être affinés par des attributs dont la définition dépend du problème à traiter et de la connaissance à formaliser.

Les résultats obtenus et les solutions proposées permettent d'entrevoir, d'une part, des prolongements de l'action engagée et, d'autre part, l'extension des investigations vers des pistes de développement supplémentaires.

La première action de prolongement concerne le déploiement de la solution et sa mise en place dans un contexte donné. Ce déploiement nécessite, pour une optimisation de la solution proposée, le développement d'utilitaires logiciels permettant une meilleure application de la solution. Nous avons développé les principes de chaque étape de l'organisation et proposé, par endroit, des voies pour l'instrumentation logicielle qu'il faudrait formaliser dans l'objectif de fournir un outil clé en main. Les démonstrateurs ponctuels que nous avons créés valident la faisabilité de celle-ci et en fixent les principes directeurs. Cette première action est liée à la nécessité, pour l'amélioration continue et l'optimisation de la solution, de faciliter la capitalisation d'expérience pour des phases telles que celles contenues dans le PRAO pour

lesquelles les informations ne sont pas stabilisées étant donné que le produit n'existe pas encore.

La deuxième action de prolongement est liée à la formalisation plus détaillée des calculs matriciels permettant de configurer les liens intra ou inter domaines (fonctions/fonctions, composants/composants ou fonctions/composants). Des logiques de combinaisons entre les indicateurs descriptifs du comportement Sûreté de Fonctionnement des entités élémentaires sont à approfondir pour procéder à l'évaluation des mêmes indicateurs (taux de défaillance, coût, couverture de diagnostic, niveau d'intégrité de sécurité, …) ou d'autres mesures d'évaluations situés à des niveaux supérieurs dans la décomposition du produit étudié.

Dans une logique quelque peu similaire, on pourrait imaginer proposer également une amplification du jeu de matrices pour considérer, dans un même tableau, des éléments de niveaux différents. On se trouverait ainsi en présence de matrices mettant en relation des fonctions avec des sous fonctions ou des sous-ensembles structurels avec des composants plus élémentaires. Cet élargissement de la panoplie des matrices faciliterait de façon biunivoque le passage des niveaux de description détaillés (proches du composant ou de la fonction élémentaire) vers des niveaux offrant une vue plus panoramique pour l'appréhension de sous-ensembles (structurels ou fonctionnels) plus complets.

Concernant les pistes d'extension nous pensons en premier lieu qu'il serait intéressant de conduire des travaux sur l'insertion de la méthodologie en phase d'exploitation. Il s'agirait de travailler dans un cadre rendu progressivement plus confortable par la mise à disposition d'une information, issue du retour d'expérience et alimentant de façon continue les réservoirs d'informations exploités pour la mise en place de la démarche. La capitalisation des informations de chaque AO pourrait permettre la définition et le développement d'un système de raisonnement à partir de cas (RàPC). Dans cet objectif, les caractéristiques d'un Appel d'Offre devront être définies : client concerné, type de produit, criticité SdF, type d'exigences client, problèmes rencontrés, remarques client,… L'ensemble de ces caractéristiques fixe le type de cas et en fonction du type d'AO auquel l'entreprise est confrontée à un moment donné, la sélection du cas le plus approprié sera plus immédiate. Comme à chaque fois, lorsque la méthode de RàPC est utilisée, les problématiques à solutionner concerneront l'identification des cas similaires et la définition de l'adaptabilité au cas présent des solutions retenues par le passé.

Une autre piste d'extension est relative à la mise en œuvre d'une logique de bibliothèque constituée de primitives descriptives du produit ou de modèles de comportements situés au niveau le plus bas de généricité. L'utilisation de ces primitives est importante dans le cadre de cette étude puisqu'elle favorisera la réactivité du processus de réponse à appel d'offre. Si nous avons parlé dans le cadre de ce mémoire de modèles produits génériques (sur le plan fonctionnel ou structurel) ou pourrait imaginer ,dans une même logique, des méthodologies préétablies par rapport à un produit donné comme par exemple des AMDEC paramétrables ou préfabriquées qu'il suffirait d'instancier au cahier des charges du client pour qu'elle délivre les résultats attendus.

Ce travail de thèse a été réalisé dans un cadre industriel. Nous avons eu en permanence au cours de nos développements le souci de conserver ce cadre d'application afin de proposer une méthodologie facile à déployer dans

un contexte d'entreprise. Nous avons, pour cela, considéré tout au long de ce travail les routines de conception et pris en compte le concepteur en tant que partie prenante de l'analyse de la Sûreté de Fonctionnement. Nous avons essayé également de garder un caractère générique au développement. Lorsque les développements étaient trop corrélés à l'entreprise partenaire, des propositions d'adaptation à d'autres contextes ont été formulées.

A l'issue de ce travail de 3 ans, il apparaît aujourd'hui que la problématique de départ est plus que jamais d'actualité. La méthodologie que nous proposons est opérationnelle. L'exploration des champs d'investigation que nous venons de mentionner plus haut permettra d'en faire un vrai levier de performance pour la prise en compte rapide et efficace de la dimension Sûreté de Fonctionnement en phase de réponse à appel d'offre.

ANNEXES

Annexe I-A : Questionnaire développé pour l'interview des acteurs projet

Cette annexe présente le questionnaire que nous avons développé dans le cadre de l'analyse de l'état des lieux de l'entreprise partenaire.

1- Service et poste au sein de la société

SV C SC C T2 Sélectionner...

Poste Sélectionner...

Pilote métier ☐ OUI ☐ NON

Si autres, précisez :

2- Nombre d'années d'expérience dans l'industrie automobile : ___ans
dont Siemens VDO/Continental Automotive France SAS :
Autres :

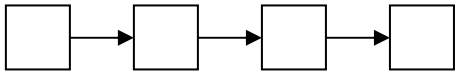
3- Maîtrise des méthodes de la sûreté de fonctionnement (cochez les cases correspondantes) :

	Nom de la méthode	Abréviation	Connue	Déjà utilisée	lecture	réalisation	nécessité de réalisation
1	Analyse préliminaire des risques / *Hazard Preliminary Analysis*	APR / *HPA*	☐	☐	☐	☐	☐
2	Analyse des modes de défaillances de leurs effets et de leur criticité / *Failure Mode, Effects and Criticity Analysis*	AMDEC / *FMECA*	☐	☐	☐	☐	☐
		AMDEC Design	☐	☐	☐	☐	☐
		AMDEC Produit/ Système	☐	☐	☐	☐	☐
		AMDEC Process	☐	☐	☐	☐	☐
3	Méthodes des arbres de défaillances / Fault Tree Analysis	AdD / FTA	☐	☐	☐	☐	☐
4	Analyse Fonctionnelle / Functional Analysis	AF / *FA*	☐	☐	☐	☐	☐

Autres méthodes utilisées : _____

4- Maîtrise du processus de Management des risques

Noter les numéros des méthodes dans leur ordre d'utilisation dans les projets



5- Culture sûreté de fonctionnement

Qu'est-ce que la sûreté de fonctionnement pour vous ?

A quoi sert-elle ?

Pourquoi vouloir développer cette discipline ?

6- Domaine d'expertise particulier

Avez-vous un domaine d'expertise particulier ?

Si oui, lequel ?

Avez-vous la fonction d'expert ?

7- Connaissances des bases de données

Connaissez-vous des bases de données de l'entreprise :

Si oui, citez-les :

Les utilisez-vous ? ☐ OUI ☐ NON

Si oui, à quelle fréquence ?

8- Connaissances des outils de capitalisation d'expérience

Connaissez-vous des outils de capitalisation d'expérience ?

Si oui, citez-les :

9- Formations

Avez-vous suivi les formations suivantes ?

Code formation	Nom de la formation	Formation réalisée	
		OUI	NON
ATT1.04	Méthodes, Outils et Processus de la Sûreté de Fonctionnement	☐	☐
ATT1.05	Maitrise des exigences réglementaires dans le développement des produits	☐	☐
ATT5.07	Méthodes et outils Qualité (FMEA-FTA-caractéristiques spéciales-fiabilité-DOE-capabilités SPC-MSA) PART 1	☐	☐
ATT5.08	Méthodes et outils Qualité (Analyse fonctionnelle-8D-RMM-Traçabilité-Dérogations) PART 2	☐	☐
Q01A	Sûreté de Fonctionnement : formation	☐	☐
Q01B	Sûreté de Fonctionnement des Systèmes Electroniques de l'Automobile	☐	☐
Q10	Analyse fonctionnelle - formation	☐	☐
Q13	RMM : Risk Management Method	☐	☐
Q15A	FMEA : Méthode : sensibilisation	☐	☐
Q15B	FMEA : Outil - IQRM : sensibilisation	☐	☐
Q15C	FMEA : Méthode + Outil : formation	☐	☐
Q16A	FTA/Méthodes des Arbres de Défaillances : sensibilisation	☐	☐
Q16B	FTA/Méthodes des Arbres de Défaillances : formation	☐	☐
Q21	Maitrise des démarches de Fiabilité	☐	☐

Ces formations vous ont-elles servies ? ☐ OUI ☐ NON

Remarques diverses

10- Sur quel(s) projet(s) travaillez-vous ?

Projet 1 : Sélectionner... Précisez :
Projet 2 : Sélectionner... Précisez :
Projet 3 : Sélectionner... Précisez :
Projet 4 : Sélectionner... Précisez :

Si nombre de projets supérieur à 4, nommez les autres ci-dessous :

11- Problèmes sûreté de fonctionnement rencontrés
Avez-vous rencontré des problèmes sûreté de fonctionnement dans vos projets ?

☐ OUI ☐ NON

Si oui, sur quel(s) projet(s) ?
Comment ont-ils été résolus ?
Quel a été votre rôle dans la résolution ?

12- Remarques diverses concernant la sûreté de fonctionnement, le questionnaire… :

Annexe I-B : Détail des travaux de Scaravetti

Cette comparaison des processus de conception a été proposée par Scaravetti dans [Scaravetti, 04] dans le cadre de l'identification des jalons communs de conception. Cette présentation des processus de conception est réalisée dans le but de positionner le problème et non dans l'objectif de définir un nouveau processus. Les travaux présentés ont pour objectif de formaliser un problème de conception pour proposer un système d'aide à la décision en conception préliminaire. Cela nous intéresse particulièrement dans le sens où on cherche, dans notre problème, à identifier de façon générique les activités de conception correspondant au processus de réponse à appel d'offre. Nous présentons brièvement les différents processus de conception présent dans la Figure I-16.

[Cav 95] : Cavailles J.. Méthodes de management de programme, 2nde édition, DGA-Teknea, 1995.
Cet ouvrage présente les principes de conception ainsi que le processus correspondant aux normes RG Aero en vigueur dans le secteur aéronautique.

[Nad 02] : Nadeau J-P.. De l'analyse fonctionnelle à la créativité technique et à l'innovation, cours ENSAM, 2002.
Ce cours propose un processus de conception en trois phases principales.

[Fan 94] : Fanchon J-L.. Guide des sciences et technologies industrielles, AFNOR-Nathan, 1994.
Ce guide, réédité régulièrement (dernière édition en date du 19 mai 2008) est destiné à ceux qui suivant des études en sciences et technologies industrielles (STI). Ce guide contient une synthèse des savoirs et connaissances sur les sciences industrielles et les systèmes correspondants, à la fois pour comprendre, analyser, et représenter, mais aussi pour concevoir et expérimenter.

[Aou 90] : Aoussat A.. La pertinence en innovation : nécessité d'une approche plurielle, Thèse de doctorat, ENSAM, 1990.
Le processus proposé dans ces travaux a un caractère très orienté vers l'innovation : i.e. qui se place dans le cas où c'est l'entreprise qui définit le produit à concevoir.

[AFA 94] : AFAV. Management et démarches de projet – Projet de guide d'intégration des démarches qualité dans la conception de produit, Association Française pour l'Analyse de la valeur, 1994.
Ces travaux concernent un projet à l'initiative de l'AFAV pour une meilleure intégration de la qualité en conception.

[BNA 99] : BNAE (Bureau de Normalisation de l'Aéronautique et de l'Espace) : Recommandation générale pour la spécification de management de programme, RG. Aero 000 40, 1999.
Cet ouvrage contient l'ensemble des recommandations relatives à la spécification du management de programme dans les secteurs aéronautique et spatial. Le BNAE est un comité spécialisé pour l'aéronautique et l'espace, subdivisé en une douzaine de sous-comités. Ce comité participe à la définition des normes de ces secteurs et propose des

recommandations dont celle définie ci-dessus.

[Pah 96] : Pahl G., Beitz W.. Engineering design – A systematic approach, Springer-Verlag, London, 2nde édition, ISBN 3540199179, 1996.
Le processus de conception proposé par les auteurs dans cet ouvrage fait référence dans le domaine de la conception. Le modèle proposé est adapté des directives VDI (Société des ingénieurs allemands) et traduit en anglais par les auteurs. Le vocabulaire défini, en anglais, est aujourd'hui intégré dans des normes et fait référence.

[Die 00] : Dieter G.E.. Engineering design – A materials and processing approach, 3ème édition, Mc Graw-Hill International editions, 2000.
Le modèle de processus proposé ici est une adaptation de celui de Pahl et Beitz.

[Ull 03] : Ullman D.G.. The mechanical design process, 3ème édition, Mc Graw-Hill Higher Education, New-York, 2003.
L'auteur considère le processus de conception comme une succession d'état dans lequel chaque décision enrichit la description du produit.

[Hub 01] : Hubka V., Eder E.. Design science, édité pour le web par Filipo A. Salustri, 2001.
Selon les auteurs, la conception est une transformation d'information (besoins exigences, etc.) en description d'une structure permettant de remplir ces demandes. Ils considèrent aussi que la conception est largement influencée par l'expertise et le savoir-faire du concepteur.

Annexe II-A : Présentation du logiciel POWERGREP et des tests pour le filtrage d'information

Le logiciel POWERGREP© en version de démonstration ou en version payante est téléchargeable à l'adresse : http://www.powergrep.com/.

Les fonctionnalités de cette outil sont multiples, nous présentons les principales caractéristiques puis détaillons l'utilisation des "expressions régulières" qui permettent de rechercher de façon plus générique certains termes ou formes du texte (titre, paragraphe).

Le détail des fonctionnalités est extrait, traduit et adapté du manuel d'utilisation disponible sur le site.

Les activités de recherche d'informations que l'on peut réaliser avec ce logiciel sont :

- la recherche de fichier dans l'ensemble d'un disque dur ou dans des dossiers particuliers ou de format de fichiers par rapport à des termes figurant, dans le nom du fichier ou dans le fichier lui même,
- la recherche dans un ou plusieurs documents de liste de mots clés, d'expression régulières, d'un mot clé que l'on peut afficher de différentes manières (terme seul, terme dans son contexte, affichage du nombre d'occurrence du terme dans chaque fichier, affichage par fichier ou par terme, etc.),
- la recherche et le remplacement d'un ou plusieurs termes dans les fichiers,
- l'extraction des données résultantes et la collecte des statistiques sur l'apparition des termes,
- la création de bibliothèques de recherche prédéfinies,
- etc.

Afin d'utiliser le logiciel, certaines étapes sont à respecter. Tout d'abord, il faut sélectionner le fichier ou l'emplacement dans lequel on souhaite effectuer la recherche. L'outil propose le marquage de ces fichiers afin de cibler la recherche. De manière générale, le marquage ou l'exclusion peut être réalisé sur :

- un disque complet,
- un dossier,
- un fichier.

L'étape suivante consiste à définir le type d'action de recherche. Il existe plusieurs sortes de recherche :

- recherche de fichier : pour identifier les fichiers contenant un ou plusieurs termes ou, à l'inverse, ceux qui ne les contiennent pas,
- affichage des termes recherchés pour obtenir la liste de tous les termes présents dans les fichiers marqués,
- recherche et remplacement de termes de façon automatique ou manuelle en fonction de l'affichage du contexte dans lequel le terme apparaît,
- collecte de données pour l'extraction des termes recherchés et l'écriture de ces termes dans un nouveau fichier.

Il faut ensuite définir le type de recherche souhaité :

- texte littéral : un mot, une phrase, une expression,
- expression régulière : un motif décrivant la forme du texte recherché (exemple : les mots écrits en majuscule, une adresse mail caractérisée par du texte, le signe @ suivi d'un texte, etc.),
- expression régulière sans considération des espaces et des commentaires dans le motif nommé "free-spacing regular expression",
- données binaires : recherche de données entrées dans un mode hexadécimal pour les recherches dans les fichiers binaires,
- motif unique : un mot, une expression régulière, une phrase, etc,
- liste de motifs : l'ensemble des termes de la liste doivent être définis soit en temps réel soit par le biais des bibliothèques prédéfinies,…

Pour finir, nous proposons la présentation de quelques expressions régulières qui permettent la recherche générique dans un document de motif prédéfini.

Le premier exemple est celui de la recherche de titre. L'expression correspondante en langage naturel couplé au formalisme des expressions régulières est :

"Recherche en début de ligne (^) un numéro de 0 à 9 ([0-9]) suivi d'un point ou non (\.?) suivi ou non d'un autre numéro ([0-9]?) et éventuellement d'un point (\.)?".

Le second exemple concerne la recherche d'un motif texte particulier pouvant être mal orthographié, l'absence d'une lettre est considérée ici :

"recherche du terme microcontroller ou microcontroler (microcontroll?er)".

Le dernier exemple est celui de la recherche de plusieurs termes :

"sûreté de fonctionnement"|"fiabilité"|"sécurité".

De nombreuses recherches génériques sont envisageables à l'aide des expressions régulières. Dans le manuel d'utilisation du logiciel, disponible sur le site, de nombreuses autres possibilités sont offertes par l'utilisation de l'ensemble des méta-caractères définis pour les expressions régulières.

Annexe III-A : Détail de la méthode d'analyse fonctionnelle RESEAU proposée par Tassinari dans [Tassinari, 06]

La méthode RESEAU est utilisée pour la réalisation de l'analyse fonctionnelle externe. La méthode RESEAU est caractérisée par l'auteur comme "*une méthode permettant d'identifier, d'une façon exhaustive et dans un temps minimum, les fonctions à satisfaire par un produit*".

La méthode est définie par des étapes successives :

- R, Recherche intuitive,
- E, Etude du cycle de vie et de l'environnement,
- S, Sequential Analysis of functional Elements (SAFE),
- E, Examen des mouvements et des efforts,
- A, Analyse d'un produit de référence,
- U, Utilisation des normes et des règlements.

La première étape de recherche inductive est elle-même organisée en différentes activités :

- l'analyse des informations sur le produit considéré,
- la recherche d'information sur le produit considéré : produit similaire précédent, informations issues du retour d'expérience, ...,
- la recherche des fonctions que le produit devra réaliser sous la forme d'un brainstorming où chaque participant propose spontanément les fonctions qu'il imagine pour le produit,
- la phase de critique et d'analyse des fonctions proposées précédemment,
- la formulation des fonctions sélectionnées de façon claire et précise,
- la définition des caractéristiques des différentes fonctions : critère, niveau flexibilité,
- la rédaction du CdC fonctionnel.

Dans l'application considérée, cette phase est généralement du ressort du client qui fournit le CdC fonctionnel dans le dossier de réponse à appel d'offre.

La seconde étape d'étude du cycle de vie contient aussi plusieurs activités successives :

- la définition du cycle de vie (par exemple : production, utilisation, maintenance, fin de vie,...),
- l'identification des éléments de l'environnement,
- la recherche des fonctions d'adaptation par rapport à cet environnement,
- la recherche des fonctions d'interaction du produit avec l'environnement,
- la formulation de ces fonctions,
- la caractérisation des fonctions,
- l'enrichissement du CdC fonctionnel.

La troisième étape, par le biais de la méthode SAFE, a pour objectif l'analyse des fonctions du produit dans les différentes phases de son cycle de vie. Elle peut être décomposée en différentes activités :

- la sélection des phases du cycle de vie qui nécessitent d'être décomposées en séquences,
- la recherche des séquences de chaque phase,

- l'établissement du graphe de séquence,
- la recherche des fonctions à partir des différentes séquences,
- la formulation des fonctions,
- la caractérisation des fonctions,
- l'enrichissement du cahier des charges.

La cinquième étape d'analyse d'un produit de référence permet de comparer l'étude théorique composée des étapes précédentes et un produit similaire existant dans l'objectif d'identifier si des fonctions sont manquantes. Dans le cas où certaines fonctions n'ont pas été identifiées, il faut les définir, les caractériser et enrichir le CdC.
La dernière étape de la méthode RESEAU consiste à utiliser les normes et réglementations afin d'identifier les fonctions résultantes : par exemple, respecter la norme, être conforme à la règlementation. Comme précédemment, il faut alors définir les fonctions supplémentaires, les caractériser et les intégrer au CdC.

Annexe III-B : Présentation des projets AUTOSAR et EASIS

Nous proposons la présentation des projets AUTOSAR et EASIS.

AUTOSAR

AUTOSAR pour **AUT**omotive **O**pen **S**ystem **AR**chitecture est un projet dont l'objectif est d'élaborer et de normaliser, par le développement d'un standard, une architecture logicielle ouverte destinée aux calculateurs électroniques automobiles. Le projet est réalisé par un partenariat de différents acteurs du secteur automobiles : constructeurs, équipementiers et outilleurs. L'origine du besoin émane de la multiplication, depuis quelques années, du nombre de calculateurs dans un véhicule. AUTOSAR a pour objectif final la mise au point de spécifications décrivant les composants de l'architecture logicielle et définissant leurs interfaces (entre eux et avec la partie électronique du calculateur).

Le projet AUTOSAR a été initié en 2003 et les principaux partenaires ("core") sont : BMW, Bosch, Continental, DaimlerChrysler, Ford, Opel, PSA Peugeot Citroën, Siemens VDO Automotive, Toyota et Volkswagen. En plus de ces partenaires principaux qui dirigent le projet et en assument la responsabilité et la maîtrise, le projet regroupe 100 membres "premium" qui ont des rôles de développeurs, d'associés ou de participants.

Nous présentons l'organisation du projet suivi des différentes couches logicielles définies, l'objectif étant de rendre indépendant l'application de l'électronique.
Le projet est découpé en différents "Work-Packages" (WP) dont les principaux sont décrits ci-dessous :

- WP1 pour la définition de l'architecture logicielle et de la méthodologie de développement,
- WP2 pour la génération et la description du système,
- WP3 pour la prise en compte de la sûreté de fonctionnement,
- WP4 pour la configuration et le logiciel de base,
- WP5 pour la définition des processus de test et d'intégration,
- WP10 pour la définition des interfaces avec les fonctions applicatives,
- WP20 pour la gestion des tests de conformité, la gestion des différentes gestions du logiciel et la définition des processus de maintenance,
- ...

Le projet a permis de définir une architecture logicielle générique dont nous présentons les différentes couches après avoir rappelé la vue d'ensemble d'un logiciel.

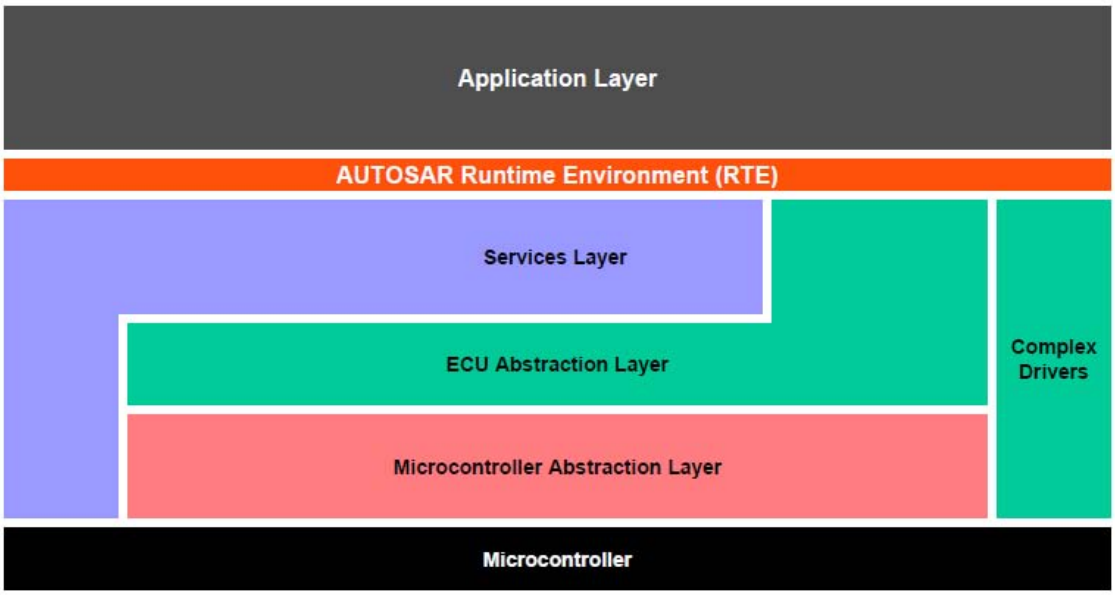


Figure IIIB 1: Couches logicielles définies dans le projet AUTOSAR

Au deux extrémités, on trouve la couche "microcontroller" qui correspond au microcontrôleur principal d'un calculateur dans lequel le logiciel est implanté et la couche "Application layer" qui correspond au logiciel applicatif contenant les lois de commande du système.

On trouve dans le logiciel quatre couches qui ont pour objectif de rendre indépendant le microcontrôleur de l'application.

La première couche "Microcontroller Abstraction Layer" est la couche la plus basse du logiciel basique. Il contient les drivers qui sont des modules ayant un accès direct aux périphériques internes du microcontrôleur ainsi qu'aux mémoires internes et externes. L'objectif de cette couche est de rendre les couches supérieures indépendantes du microcontrôleur. L'implémentation de cette couche est dépendante du microcontrôleur utilisé. Elle contient des modules de quatre natures : les modules propres aux drivers du microcontrôleur (horloge interne, périphérique interne du microcontrôleur), les modules relatifs aux mémoires internes et externes du microcontrôleur (RAM, Flash, EEPROM, etc.), les modules relatifs à la communication (communication avec le véhicule via le bus CAN, communication inter-microcontrôleurs via le bus SPI, etc.) et enfin les modules relatifs aux entrées/sorties (signaux digitaux, analogiques, convertisseur analogique/digital et inversement).

La seconde couche "ECU Abstraction Layer" crée l'interface pour la couche d'abstraction du microcontrôleur. Elle permet notamment aux couches supérieures d'accéder aux drivers en faisant abstraction de leur emplacement (interne ou externe au microcontrôleur) et de leur connexion au microcontrôleur. Elle rend donc indépendant les modules des couches supérieures du microcontrôleur.

La troisième couche "Services Layer" contient l'ensemble des services nécessaires au fonctionnement de la couche applicative, c'est la couche la plus haute du logiciel basique. Les services fournis sont :

- les fonctionnalités de l'OS (operating system),
- le management et la gestion des communications avec le réseau du véhicule,
- les services d'accès aux mémoires,
- les services de diagnostic et de mémorisation des erreurs,
- la gestion des états du calculateur.

Ces services sont accessibles par les couches inférieures et le logiciel applicatif.

La quatrième couche "Complex drivers" est destinée à l'implémentation de drivers complexes pour les capteurs et les actionneurs permettant un accès direct aux fonctionnalités internes du microcontrôleur.

Enfin entre ces quatre couches du logiciel basique et le logiciel applicatif, on trouve la couche "Autosar runtime environment (RTE)" qui a pour vocation de rendre indépendant les modules AUTOSAR de l'implémentation sur une application particulière. Cette couche est caractérisée comme "middleware" et fournit les services de communication pour les modules AUTOSAR présent dans le logiciel applicatif comme présenté dans la figure suivante.

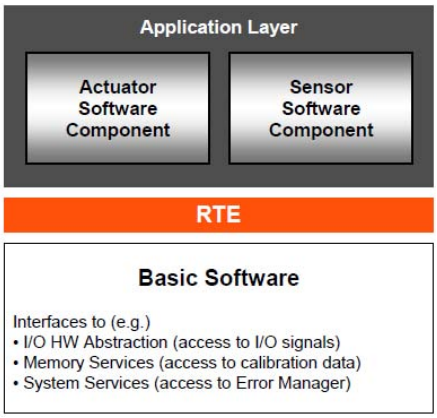


Figure IIIB 2 : Illustration des modules AUTOSAR du logiciel applicatif

Enfin le dernier point que nous présentons concerne les possibilités de communication entre les différentes couches.

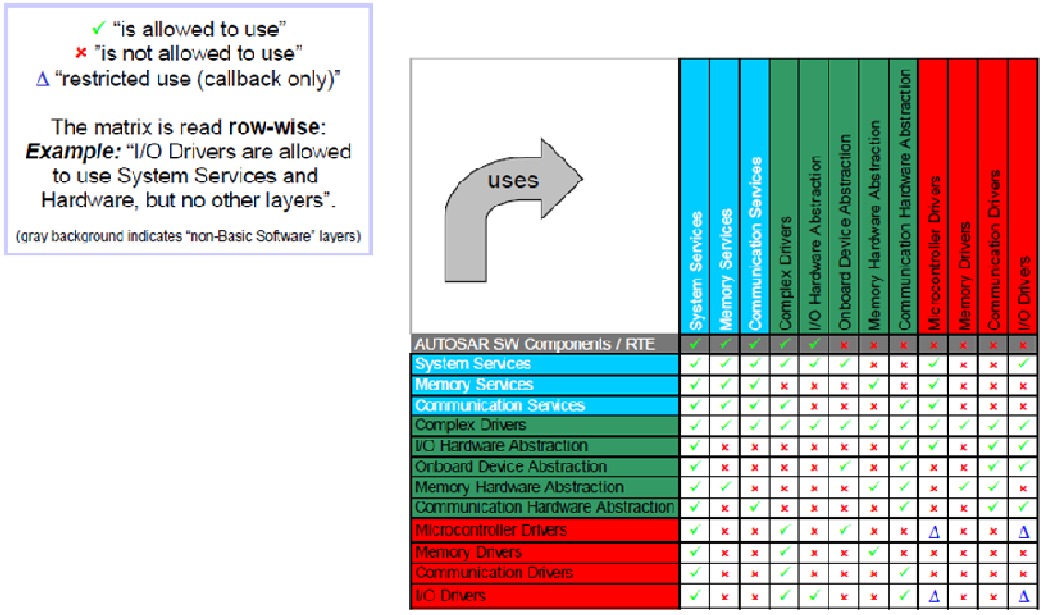


Figure IIIB 3 : Interaction entre modules dans AUTOSAR

Ce tableau donne l'ensemble des interactions autorisées entre les différents modules. Il permet notamment de montrer que les différents modules peuvent être utilisés ceux des couches voisines excepté pour la couche services qui elle fournit ces fonctionnalités à l'ensemble des modules.

Pour plus de détails, le site web [AUTOSAR, WEB] du projet propose le téléchargement des différents documents

relatifs aux "Work-Packages".

EASIS

EASIS pour **E**lectronic **A**rchitecture and **S**ystem Engineering for **I**ntegrated **Safety** Systems est un projet dont l'objectif est le développement d'une architecture électronique du véhicule standardisée ainsi qu'une approche système standard pour les systèmes intégrés de sécurité. Ce projet émane des nouveaux challenges induits par les systèmes intégrés de sécurité tels que l'intégration des différents domaines automobile (contrôle moteur, châssis, habitacle,..) entraînant un recouvrement des fonctions de sécurité, la manipulation de produits de plus en plus complexes ou l'intégration de services télématiques pour les systèmes de sécurité.

La complexité de ces nouveaux challenges est illustrée dans la figure suivante qui met en évidence, notamment, les systèmes impliquant différents partenaires (OEM pour constructeurs, supplier 1 et 2 pour les équipementiers) ou les interactions des systèmes intégrés de sécurité avec leur environnement.

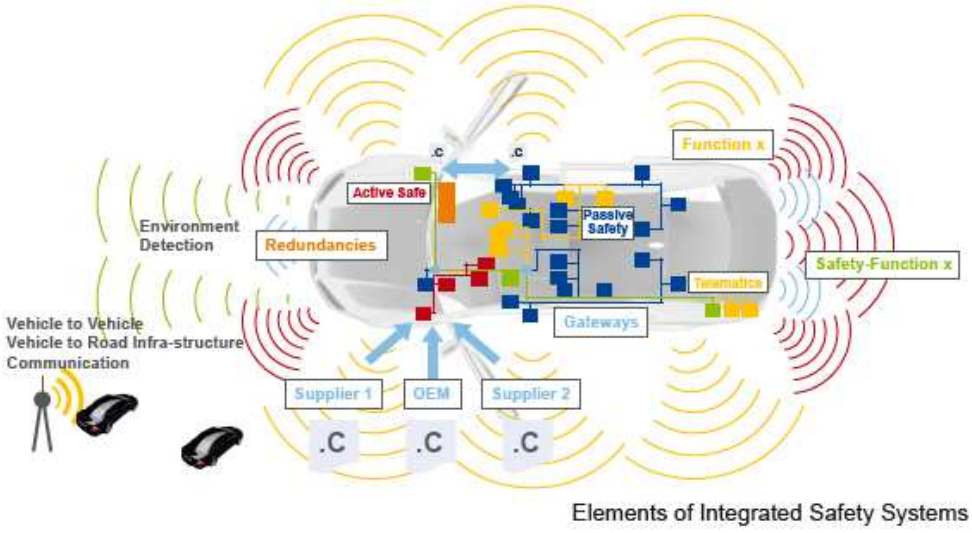


Figure IIIB 4 : Illustration des futurs challenges issue de [AUTOSAR_PRESENTATION]

Le projet EASIS a été initié en janvier 2004 par un consortium composé :

- de constructeurs : Daimler Chrisler, DAF, Centre de recherche FIAT, Opel, PSA Peugeot Citroen, Volvo,
- d'équipementiers : Bosc, Continental Teves, Lear Corporation, Motorola, Philips, Valeo, ZF,
- de membres associés : TRW,
- de fournisseurs d'outils et de middleware : Decomys, dSpace, ETAS, VECTOR,
- d'établissements de recherche : OFFIS, MIRA, Institut d'informatique ICB.

Le projet est découpé en différents " Work-Packages" dont les principaux sont :

- WP0 pour la définition des spécifications des systèmes intégrés de sécurité,
- WP1 pour la définition de l'architecture logicielle,
- WP2 pour la définition de l'architecture électronique,
- WP3 pour la prise en compte de la sûreté de fonctionnement,

- WP4 pour la définition des outils et des processus,
- WP5 pour la validation et l'exploitation des résultats,
- WP6 pour la coordination et la gestion du projet,
- un dernier Work-Package ayant pour objectif la définition d'une architecture véhicule sécurisée obtenue par les résultats des différents Work-Package précédent.

Chacun de ces Work-Packages est décomposé en tâches dont le détail est présenté dans [EASIS_Presentation].

Nous présentons ici les différents Work-Packages ainsi que leur objectif après avoir donné les résultats du projet EASIS :

- une plateforme pour les fonctionnalités basées sur le logiciel, cette plateforme fournit des services communs à partir desquels les futures applications pourront être développées,
- une infrastructure électronique du véhicule supportant les spécifications des systèmes intégrés de sécurité définies et minimisant les coûts d'intégration ainsi que des blocs génériques organisables en différentes configurations pour un système intégré de sécurité,
- la proposition de méthodes et techniques pour la prise en compte de la sûreté de fonctionnement à partir de l'analyse des méthodes existantes, leur adaptation aux systèmes considérés et leur définition pour le projet,
- la définition d'une démarche de développement et des outils associés pour la conception de ces systèmes.

L'architecture logicielle définie adopte une décomposition en différents couches généralement employé pour la définition des architectures logicielles. On observe une couche haute (application) et une couche basse (microcontrôleur) dont les couches médianes vont isolés ces deux premières. L'architecture logicielle est présentée sur la figure suivante :

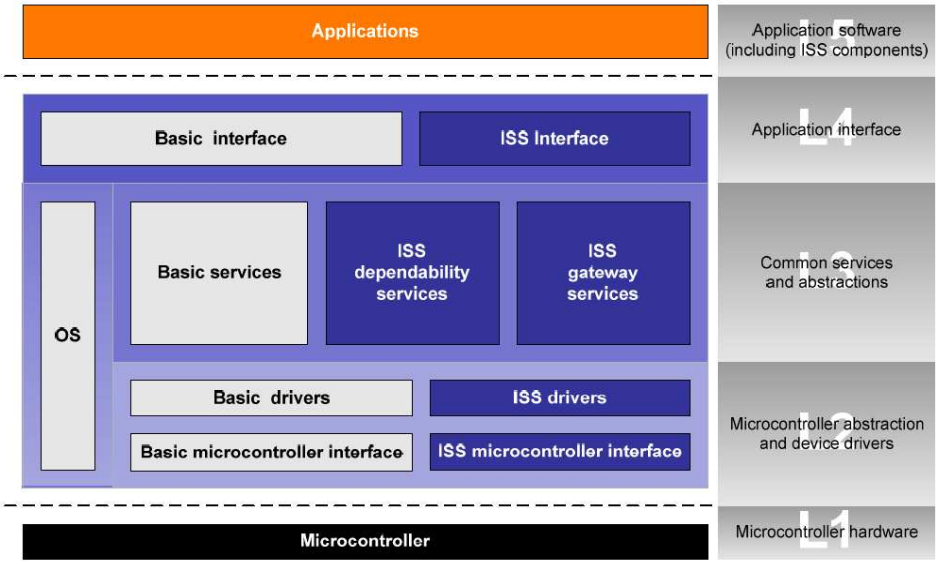


Figure IIIB 5 : Architecture logicielle issue de [EASIS D1.2]

Dans cette architecture les services basiques (Basic service) émanent d'AUTOSAR dans l'objectif d'être compatible. Les éléments définis concernent l'ensemble des modules dont le nom commence par ISS (pour Integrated safety system) qui sont en fait des modules gérant uniquement les aspects sûreté de fonctionnement des modules de base correspondant.

Concernant l'architecture électronique, le projet propose différentes organisations entre les systèmes embarqués des différents domaines au niveau véhicule. Le projet a aussi permis de définir pour chaque système des blocs génériques :

- Power Supply : l'alimentation,
- Main MCU : le processeur,
- Supervisor : superviseur, il assure la surveillance du système,
- Input filter : l'interface avec les capteurs,
- Output Driver : l'interface avec les actionneurs.

La démarche définie dans le projet EASIS pour la prise en compte de la SdF est classique et propose différentes étapes :

- l'identification et la hiérarchisation des risques,
- la définition des spécifications se SdF en regard de ces risques,
- la vérification et la validation des spécifications SdF.

La démarche complète est présentée sur la figure suivante.

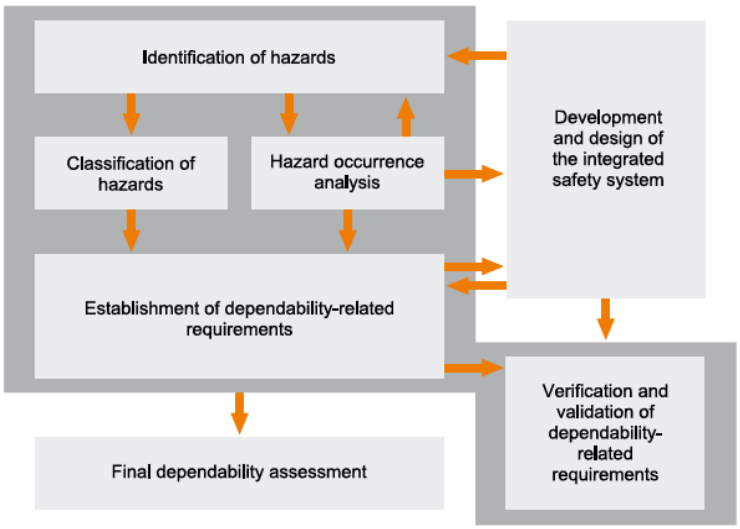


Figure IIIB 6 : Démarche SdF issue de [EASIS D3.2]

Nous finissons par la présentation de l'approche système proposée dans le projet. La proposition d'un standard de développement pour les systèmes intégrés de sécurité émane de la spécificité de ces systèmes d'utiliser des informations du véhicule ou de son environnement pour influencer des systèmes temps réels du domaine châssis, par exemple, créant ainsi la nécessité d'une boucle de sécurité pour le système impacté. La démarche proposée intègre le développement, la gestion des risques ainsi que de nombreux concepts de l'ingénierie système, cela en prenant en compte et en adaptant les étapes en fonction des caractéristiques des systèmes intégrés de sécurité. L'objectif de cette proposition est présenté sur la figure suivante.

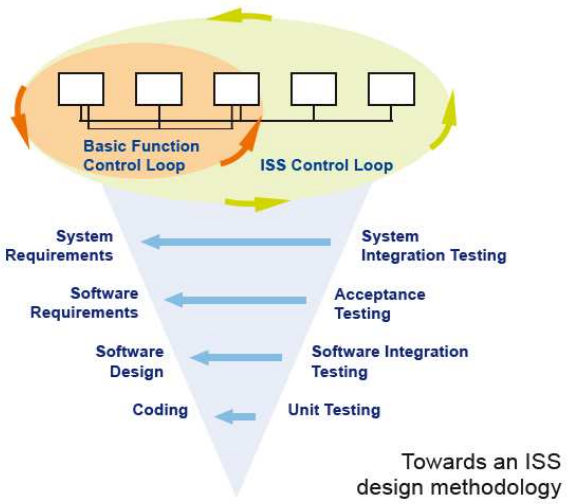


Figure IIIB 7 : Démarche proposée issue de [EASIS D4.1]

Pour plus de détails, le site web [EASIS, WEB] du projet propose le téléchargement des différents documents relatifs aux "Work-Packages".

Annexe III-C : Détail de l'étude des produits

Nous proposons certains détails de l'analyse des produits existants qui ne nous ont pas semblés nécessaires à la compréhension du travail effectué mais qui fournissent des informations plus détaillées. Nous nous focalisons ici sur le détail de la composition électronique des produits considérés. Pour cela, nous utilisons les produits existants dans l'entreprise partenaire ainsi que les projets du domaine tels que EASIS et AUTOSAR pour arriver à la définition de blocs structurels génériques sur l'ensemble des produits.

Tout d'abord, au niveau électronique, les ECU sont des calculateurs composés d'une à quelques centaines de composants [Ziegler, 05] organisés en modules[28]. Nous proposons un bilan des blocs constitutifs d'un calculateur. Chen dans [Chen, 08] propose une décomposition en cinq parties (Figure IIIC 1).

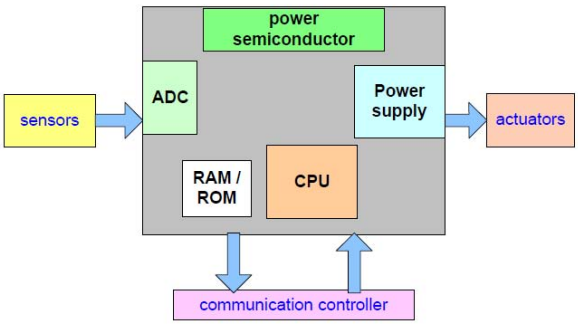


Figure IIIC 1 : Composition électronique ECU d'après Chen dans [Chen, 08]

Cinq blocs principaux sont considérés dans ses travaux :

- CPU (Core Processor Unit) : le processeur du système,
- RAM/ROM : les mémoires,
- Power-Supply : l'alimentation,
- Communication Controller : l'interface de communication entre le système et le véhicule,
- Sensors/Actuators : les capteurs actionneurs qui eux sont à l'extérieur de l'ECU.

Cependant, on distingue dans ce modèle une partie ADC (Convertisseur Analogique / Digital) pour permettre l'interfaçage des capteurs et une partie Power-Semiconductor destinée à commander les actionneurs.

Ce modèle nous paraît trop abstrait pour définir la constitution électronique d'une ECU. Nous présentons donc ensuite les travaux générés par le projet EASIS au niveau électronique. Pour cela, nous nous appuierons, d'une part, sur un schéma simplifié d'un calculateur et, d'autre part, sur un exemple proposé dans le cadre d'une application du projet. Le premier modèle est donné sur la Figure IIIC 2.

[28] Nous nommons module un ensemble de composants organisé de façon à remplir une fonction électronique (exemple : alimentation)

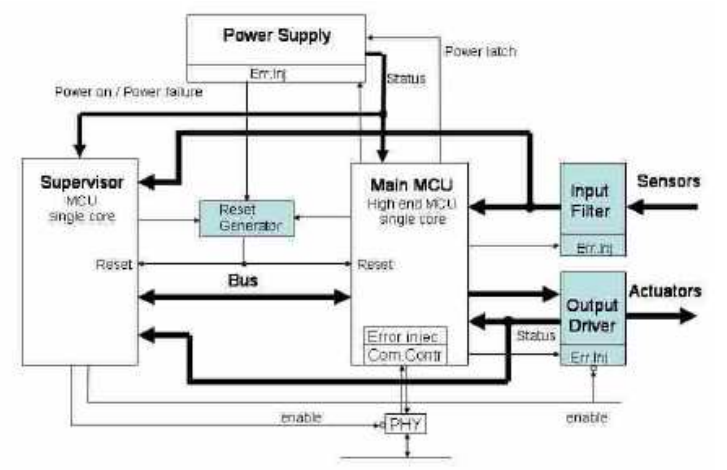


Figure IIIC 2 : Schéma bloc d'une ECU issu de [EASIS D2.2]

On distingue dans le modèle proposé, les blocs :

- Power Supply : l'alimentation,
- Main MCU : le processeur,
- Supervisor : superviseur, il assure la surveillance du système,
- Input filter : l'interface avec les capteurs,
- Output Driver : l'interface avec les actionneurs.

L'exemple donné dans [EASIS D2.2], exemple de prototype :

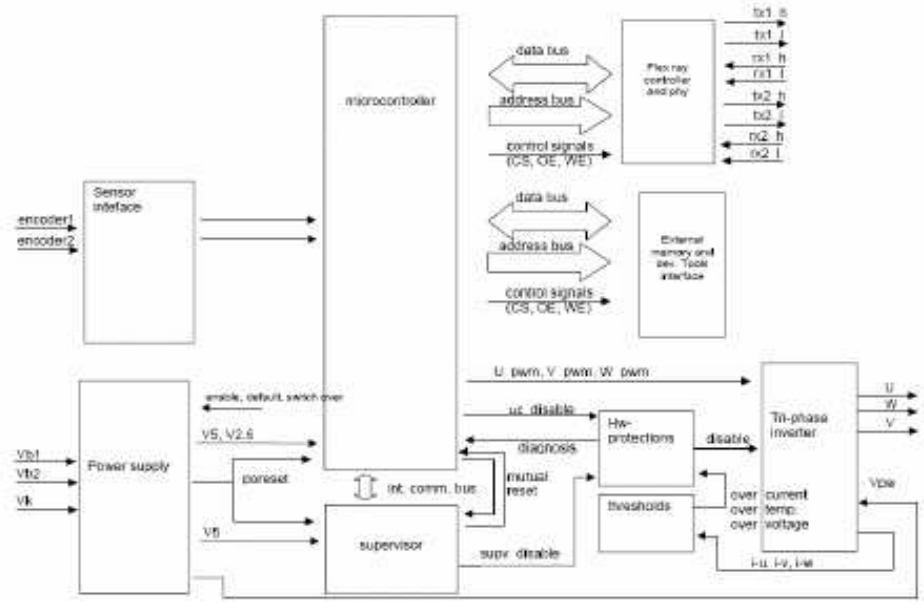


Figure IIIC 3 : Exemple d'ECU issu de [EASIS D2.2]

On retrouve les blocs identifiés dans des travaux réalisées par des constructeurs ou équipementiers comme illustré sur la figure suivante : un microcontrôleur, un watchdog, des driver de sorties, des alimentations, etc.

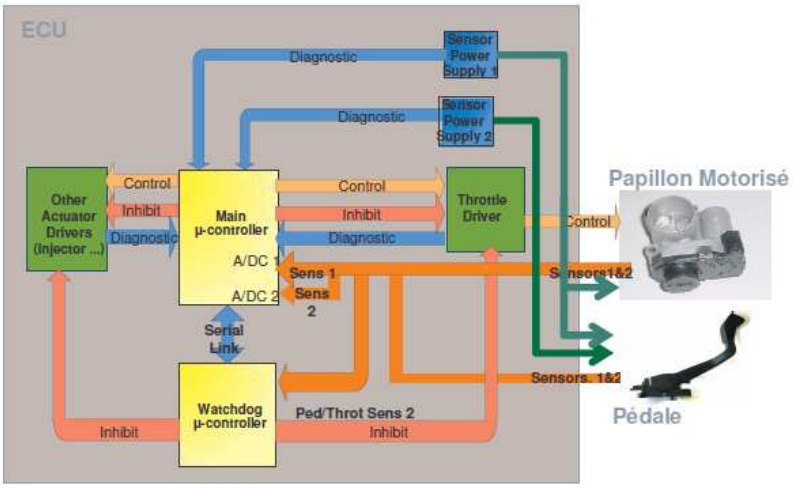


Figure IIIC 4 : ECU issu de [VEMS, 05]

Nous avons ensuite repris des descriptions existantes afin de faire un bilan des modules électroniques généralement définis.

VEMS 05	**EASIS**	**Xi-Chen**	**Etude interne**
	Input interface	ADC	Dispositif de mise en forme des entrées
Main microcontrôleur	MCU	CPU	Processeur
	Memory	RAM/ROM	Mémoire
	Output Interface or Driver	Power semi-conductor	Drivers de sorties
Power supply	Power Supply	Power Supply	Alimentation
	Communication controller	Communication controller	Interface de communication
Sensors	Sensors	Sensors	Capteurs
Actuators	Actuators	Actuators	Actionneurs
Watchdog/microcontroller	Supervisor	Supervisor	Superviseur

Tableau IIIC 1 : Comparaison des différents blocs

Enfin, nous avons comparé les différents types de blocs et les différents modèles, identifié leurs atouts et leurs faiblesses pour enfin proposer une liste, que nous pensons exhaustive, des modules électroniques qui peuvent être rencontrés dans un calculateur.

	EASIS	Xi-Chen	Modèle proposé
Atouts	Projet réalisé sur l'ensemble des domaines (Châssis, Powertrain...) d'où généricité des	Projet spécifique au domaine Châssis donc problématique correspondante	Intégration des projets généraux dans le modèle mais en conservant les habitudes de l'entreprise

	concepts		
Limites	Description des modules pas assez précise par rapport à nos besoins Projet orienté architecture ECU et non composition des différents blocs	Modèle proposé pas assez détaillé et trop abstrait pour fixer les connaissances métiers électronique et plutôt orienté architecture ECU et non description des différents blocs	Nécessité d'adapter le modèle dans le cas d'une application différente

Tableau IIIC 2 : Atouts et limites des modèles étudiés

Ces détails permettent surtout d'illustrer la manière avec laquelle nous avons procédé pour l'analyse de la partie électronique ainsi que d'avoir un aperçu des modèles étudiés.

Références bibliographiques

[AFIS, 04] Association Française d'Ingénierie Système. Glossaire de base de l'ingénierie système, Version expérimentale 1.2, 5 octobre 2004.

[AFNOR NF X50-150] NF X50-150 : Analyse de la valeur – Analyse fonctionnelle – Vocabulaire, 1990.

[AFNOR X 60-010] NF X 60-010: MAINTENANCE CONCEPTS ET DEFINITIONS DES ACTIVITES DE MAINTENANCE, décembre 1994, ISBN 978212X600100.

[AFNOR X 60-500] NF X 60-500 : Terminologie relative à la fiabilité - Maintenabilité – Disponibilité, octobre 1988.

[Alhajj, 08] Alhajj T.. TCSIM: A Top-Down approach to Mixed-Signal Circuits and Systems design, Rapport de master, Department of Electrical and Computer Engineering McGill University, Montreal (Quebec/Canada), 2008.

[Angueniol&al, 05] Angéniol S., Gardoni M., Yannou B., Chamerois R.. Vers une intégration du design to cost pour l'optimisation de la conception - Cas d'étude : analyse des besoins métiers chez Eurocopter. 2ème Colloque du groupe de travail C2EI : Modélisation et pilotage de systèmes de Connaissances et de Compétences dans les Entreprises Industrielles, 1-2 Décembre 2005, Nancy (France).

[Assali&al, 08] Assali A.A., Lenne D., Debray B.. Ontology development for industrial risk analysis, 3ème conférence internationale des technologies de l'information et de la communication : de la théorie à l'application ICCTTA 2008, 7-11 avril 2008, Damascus (Syrie).

[AUTOSAR, 06] Projet AUTOSAR, Communiqué de presse : AUTOSAR, une technologie au service de l'électronique automobile de pointe, octobre 2006, disponible sur http://www.autosar.org

[AUTOSAR, WEB] www.autosar.org

[AUTOSAR_PRESENTATION] Projet AUTOSAR : layered software architecture V2.0, disponible sur http:\\www.autosar.org, 2006.

[Baziz, 05] Baziz M.. Indexation conceptuelle guidée par ontologie pour la recherche d'information, Thèse de doctorat, Université Paul Sabatier, Toulouse (France), 2005.

[Ben-Ahmed, 05] Ben-Ahmed W.. SAFE-NEXT : une approche systémique pour l'extraction de connaissances de données – Application à la construction et à l'interprétation de scénarios d'accidents de la route, Thèse de doctorat, Ecole centrale des arts et manufactures « Ecole centrale Paris », Paris (France), 2005.

[Berger, WEB] http://philippe.berger2.free.fr/automatique/cours/sadt/sadt.htm#Définition

[Beugin, 06] Beugin J.. Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé, Thèse de doctorat, Université de Valenciennes et du Hainaut-Cambresis, Valenciennes (France), 2006.

[Beugin, 06] Beugin J.. Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé, Thèse de doctorat, Université de Valenciennes et du Hainaut-Cambresis, Valenciennes (France), 2006.

[Bieber&al, 04] Bieber P., Castel C., Kehren C., Seguin C.. Safety Architecture patterns : une introduction, journées FAC'04 : Formalisation des activités concurentes, 9-10 mars 2004, Toulouse (France).

[Blancart, 07] Blancart P.. Maitrise des risques sécurité et pannes : points délicats à l'interface constructeur / fournisseurs, Atelier SIA Management de la fiabilité, 14 mars 2007, Suresnes(France).

[Bonhomme, 98] Bonhomme S.. Transformation de documents structurés, une combinaison des approches explicite et automatique, Thèse de doctorat, Université Joseph Fourier, Grenoble (France), 1998.

[Bonivento, 07] Bonivento A.. Platform Based Design for Wireless Sensor Networks, Technical Report No. UCB/EECS-2007-85 disponible sur http://www.eecs.berkeley.edu/Pubs/TechRpts/2007/EECS-2007-85.html, 20 juin 2007.

[Boumane&al, 06] Boumane A., Talbi A., Tahon C., Bouami D.. Contribution à la modélisation de la compétence, Congrès international de Modélisation et de Simulation MOSIM'06, 3-5 avril 2006, Rabat (Maroc).

[Bracquemond, 07] Bracquemond A.. Sécurité générale du produit, Atelier SIA (Société des ingénieurs de l'automobile) : La sécurité générale du produit, 10 juillet 2007, Suresnes (France).

[Cagno&al, 00] Cagno E., Caron F., Mancini M.. Cost Estimation of Industrial Risk in the Bidding Process, SENET review, 1st South East Europe Regional Conference on Project Management, 9-11 novembre 2000, Ljubljana (Slovénie).

[Cagno&al, 01] Cagno E., Caron F., Perego A.. Multi-criteria assessment of the probability of winning in the competitive bidding process, Journal international de management de projet n°19, p313-324, 2001.

[Chakrabarti, 01] Chakrabarti A.. Sharing in design - categories, importance, and issues, International Conference on Engineering Design ICED 01, 21-23 aout 2001, Glasgow (U.K.).

[Chalal&al, 05] Chalal R., Alquier A.M.. Un système d'information pour le management des connaissances sur les risques projet, 4ème Conférence Internationale en Conception et Production Intégrées CPI 2005, 9-11 novembre 2005, Casablanca (Maroc).

[Chalal&al, 06] Chalal R., Ghomari A. R.. An Approach for a Bidding Process Knowledge Capitalization, Proceedings of world academy of science, Engineering and technology Volume 13, Mai 2006, ISSN 1307-6884.

[Chaussis, 06] Chaussis P.. Sécurité Fonctionnelle des systèmes EE embarqués dans les véhicules routiers : Vision d'un donneur d'ordre : projet de norme ISO 26262, PUCE Sécurité Fonctionnelle des systèmes, 3èmeJournée thématique : Sûreté de Fonctionnement en Ingénierie Système, AFIS, 4 octobre 2006, Toulouse (France).

[Chen, 08] Chen X.. Requirement and concepts for future automotive electronic architectures from the view of integrated safety, Thèse de doctorat, Universitatsverlag Karlsruhe (Allemagne), 2008.

[Cortes-Robles, 06] Cortes-Robles G.. Management de l'innovation technologique et des connaissances : synergie entre la théorie TRIZ et le Raisonnement à Partir de Cas - Application en génie des procédés et systèmes industriels, Thèse de doctorat, Institut national polytechnique de Toulouse, Toulouse (France), 2006.

[Cours UTC, 08] TECRIS Consultants et associés. Management de la sûreté de fonctionnement, cours de l'ingénieur UTC, Université de technologie de Compiègne, disponible sur http://tice.utc.fr/moodle/course/category.php?id=1 catégorie FQ05 : Fiabilité industrielle, 2008.

[Couto, 06] Couto J.. Une plate-forme informatique de Navigation Textuelle : modélisation, architecture, réalisation et applications de NaviTexte, Thèse de doctorat, Université de Paris IV - Sorbonne, Paris (France), 2006.

[Couto&al, 02] Couto J., Ferret O., Grau B., Hernandez N., Jackiewicz A., Minel J-L., Porhiel S.. RÉGAL, un système pour la visualisation sélective de documents, Revue d'Intelligence Artificielle. Volume X – n° X/2002, pages 1 à 35, 2002.

[Couto&al, 04] Couto J., Minel J-L.. Interfaces dynamiques de fouilles textuelles : vers une plate-forme de navigation textuelle, 7ème conférence internationale de Recherche d'information assistée par ordinateur RIAO 2004, 26-28 avril 2004, Avignon (France).

[Couto&al, 06a] Couto J., Minel J-L.. SEXTANT, un langage de modélisation des connaissances pour la navigation textuelle, Colloque international : Discours et Document ISDD'06, 15-16 juin 2006, Caen (France).

[Couto&al, 06b] Couto J., Minel J-L.. Navigation textuelle : représentation des textes et des connaissances, revue internationale Traitement Automatique des Langues (TAL), Volume 47 – n° 2/2006, pages 225 à 254. Disponible sur http://www.atala.org/-Volume-47-.

[Dekeyser, 05] Dekeyser J-L.. System on Chip Co-Design, cours de master recherché, année 2005/06, Université des Sciences et Technologies de Lille, Lille (France).

[Demri&al, 07a] Demri A., Charki A., Guérin F., Kahn P., Christofol H.. Analyse Qualitative et Quantitative d'un Système Mécatronique, 5ème conférence internationale en Conception et Production intégrées CPI 2007, 22-24 octobre 2007, Rabat (Maroc).

[Demri&al, 07b] Demri A., Charki A., Guerin F., Barreau M., Christofol H.. Fiabilisation d'un système mécatronique dès la phase de conception, 18ème congrès français de mécanique, 27-31 Aout 2007, Grenoble (France).

[Dieng, 00] Dieng R.. Méthodes et Outils pour la Gestion des Connaissances, Présentation du projet ACACIA (INRIA), 2000.

[Dumas, 06] Dumas P.. Vision d'un donneur d'ordre : projet de norme ISO 26262, Atelier SIA Recueil de données du REX, 29 Novembre 2006, Suresnes (France).

[Dumas&al, 08] Dumas X., Pagetti C., Sagaspe L., Bieber P., Dhaussy P.. Vers la génération de modèles de sûreté de fonctionnement, 2ème Conférence Francophone sur les Architectures Logicielles (CAL 2008), 3-7 Mars 2008, Montréal (Québec, Canada).

[Dupouy, 05] Dupouy F.. Exigences de fiabilité et leurs validations pour un système électronique, Atelier SIA Exigences de fiabilité et leurs validations pour un système électronique, 15 décembre 2005, Suresnes (France).

[EASIS D0.1.2] Projet EASIS Deliverable D0.1.2 : State of the art, V1.0, 5 août 2004, disponible sur http:\\www.easis-online.org.

[EASIS D1.2] Projet EASIS Deliverable D1.2 : Overall description of the software platform V1.0, 28 novembre 2006, disponible sur http:\\www.easis-online.org.

[EASIS D2.2] Projet EASIS Deliverable D2.2 : Conceptual Hardware Architecture Specification, V1.0, 6 décembre 2006, disponible sur http:\\www.easis-online.org.

[EASIS D3.2] Projet EASIS Deliverable D3.2 Part 1 : Guidelines for establishing dependability requirements and performing hazard analysis V2.0, 14 novembre 2006, disponible sur http:\\www.easis-online.org.

[EASIS D4.1] Projet EASIS Deliverable D4.1 : EASIS engineering process framework V1.0, 25 novembre 2006, disponible sur http:\\www.easis-online.org.

[EASIS, WEB] http://www.easis.org/

[EASIS_Presentation] Projet EASIS : the enabling technology for the introduction of integrated safety systems, disponible sur http://www.easis-online.org/wEnglish/img/pdf-files/EASIS_Presentation_040813.pdf.

[Eppinger&al, 94] Eppinger, S. D, Pimmler, T. U.. Integration Analysis of Product Decompositions, ASME Design Theory and Method Conference DTM'94, Vol 68, pp. 343-351, Septembre 1994, Minneapolis (USA).

[Faure, 07] Faure C.. Introduction au text-mining. Disponible sur http://www.christian-faure.net/2007/05/30/introduction-au-text-mining/ (dernière consultation le 26/02/2009).

[FIDES, 04] FIDES Group : FIDES Guide issue A : Reliability Methodlogy for Electronic System, DGA – DM/STTC/CO/477-A, 2004.

[Frigant&al, 01] Frigant F., Talbot D.. Proximités et logique modulaire dans l'automobile et l'aéronautique : vers une convergence des modèles d'approvisionnement, 3èmes journées de la proximité : "Nouvelles croissances et territoires", 13-14 décembre 2001, Paris (France).

[FUTURA_SCIENCE_WEB] Disponible sur http://www.futura-sciences.com/fr/definition/t/high-tech-1/d/filtre_1724/ (dernière consultation le 11/03/2009).

[Gautier&al, 00] Gautier F., Giard V.. Vers une meilleure maîtrise des coûts engagés sur le cycle de vie, lors de la conception de produits nouveaux, 11ème congrès de l'association française de comptabilité, 18-20 mai 2000, Angers (France).

[Gendreau&al, 07] Gendreau D., Gauthier M., Hériban D., Lutz P.. Contribution à la mise en place d'une architecture modulaire pour la conception des microsystèmes de production, 7ème congrès international de génie industriel CIGI 2007, 5-8 juin 2007, Trois rivières (Quebec/Canada).

[Geneste&al, 06] Béler C., Desforges X., Geneste L.. Architecture de retour d'expérience : application à la prévention des risques en montagne, Congrès international de Modélisation et de Simulation MOSIM'06, 3-5 avril 2006, Rabat (Maroc).

[Gouriveau, 03] Gouriveau R.. Management des risques : proposition d'une base d'outils pour le processus de réponse à appel d'offre, Rapport de DEA, Laboratoire Génie de production de Tarbes, Tarbes (France), 2003.

[Guide PMBOK, 00] Project Management Institute. Guide du référentiel des connaissances en gestion de projet, American national standard : ANSI/PMI 99-001 2000, 2000.

[Gutierrez-Estrada, 07] Gutierrez-Estrada C.Y.A.. Méthodes et Outils de la conception Système couplée à la Conduite de Projet, Thèse de doctorat, Institut national des sciences appliquées de Toulouse, Toulouse (France), 2007.

[Hadj-Hamou, 02] Hadj-Hamou K.. Contribution à la conception de produits à forte diversité et de leur chaîne logistique : une approche par contraintes, Thèse de doctorat, Institut national polytechnique de Toulouse, Toulouse (France), 2002.

[Hamon, 05] Hamon J-C.. Méthodes et outils de la conception amont pour les systèmes et les microsystèmes, Thèse de doctorat, Institut national polytechnique de Toulouse, Toulouse (France), 2005.

[Harmel, 07] Harmel G.. Vers une conception conjointe des architectures du produit et de l'organisation du projet dans le cadre de l'Ingénierie Système, Thèse de doctorat, Université de Franche-Comté, 2007.

[Harmel&al, 06] Harmel G., Bonjour E., Dulmet M.. Architecture des produits et des organisations : modélisation et pilotage par l'incertitude, Congrès international de Modélisation et de Simulation MOSIM'06, 3-5 avril 2006, Rabat (Maroc).

[HMida&al, 07] H'Mida F., Martin P.. L'estimation des coûts en phase de conception : un cadre d'aide à la décision, 5ème conférence internationale en Conception et Production intégrées CPI 2007, 22-24 octobre 2007, Rabat (Maroc).

[Ho-Dac&al, 04] Ho-Dac L-M., Jacques M-P., Rebeyrolle J.. Sur la fonction discursive des titres, dans S. Porhiel & D. Klingler (Eds). L'unité texte, Pleyben, Perspectives, pp.125-152, 2004.

[IDEF, WEB] http://www.idef.com/idef0.html

[IEC 60300-2] NF EN 60300-2 : Gestion de la sûreté de fonctionnement - Partie 2 : ligne directrices pour la gestion de la sûreté de fonctionnement, juillet 2004.

[IEC 61508] IEC 61508 : 1998 "Functional safety of electrical / electronic / programmable electronic safety related systems", International Electrotechnical Commission, 170p, juin 1998.

[IEC 61508-4] Norme IEC 61508 : Sécurité fonctionnelle des systèmes électriques / électroniques /électroniques programmables relatifs à la sécurité - Partie 4: Définitions et abréviations, 1998.

[IEC 61508-5] Norme Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité - Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité, 1998.

[IEC 61508-6] Norme IEC 61508 : Sécurité fonctionnelle des systèmes électriques / électroniques /électroniques programmables relatifs à la sécurité – Partie 6 : Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3, 2000.

[IMDR_SdF_07] Groupe de travail Management Méthodes Outils Standard (M2OS). Fiches méthodes. Révision en date du 1er juin 2007.

[ISO 26262] ISO/WD 26262, TC22/SC3 : Road Vehicles – Functional Safety, à paraître.

[ISO 26262-3] Norme ISO 26262 : Road Vehicles – Functional Safety – Part 3 : Concept Phase, Draft en date du 29 février 2008.

[ISO 26262-5] Norme ISO 26262 : Road Vehicles – Functional Safety – Part 5 : Product development : hardware level, Draft en date du 30 mai 2008.

[Jacquemin&al, 02] Jacquemin C., Jardino M.. Multi-dimensional and Multi-scale Visualizer of Large XML Documents, Proceedings of EUROGRAPHICS, Saarbrucken (Allemagne), 2002.

[Joannon&al, 06] Joannon Y., Beroulle V., Khouri R., Robach C., Tedjini S., Carbonero J-L.. Behavioral modeling of WCDMA transceiver with VHDL-AMS language, 9th IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems DDECS'06, 18-21 avril 2006, Prague (Republique tchèque).

[Jose-Flores, 05] Jose Flores A.. Contribution aux méthodes de Conception modulaire de produits et processus Industriels, Thèse de doctorat, Institut National Polytechnique de Grenoble, Grenoble (France), 2005.

[Khalfaoui, 03] Khalfaoui S.. Méthode de recherche des scénarios redoutés pour l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile, Thèse de doctorat, Institut national polytechnique de Toulouse, Toulouse (France), 2003.

[Kundert, 01] Kundert K.. A Formal Top-Down Design Process for Mixed-Signal Circuits, 8ème workshop processus de conception électronique, 8-10 avril 2001, Monterey (Californie/USA).

[Lamy, 02] Lamy P.. Probabilité de défaillance dangereuse d'un système : explications et exemple de calcul, Note scientifique et technique n°225, Institut National de Recherche et de Sécurité, septembre, 2002.

[Laprie, 96] Laprie J-C.. Guide de la sûreté de fonctionnement, édition Cépaduès, 1996, ISBN 2854283821.

[Lavagno&al, 03] Lavagno L., Chen R., Sgroi M., Martin G., Sangiovanni-Vincentelli A., Rabaey J.., UML for REAL : design of embedded real-time systems, Chapter 5 : UML and platform-based design, ISBN1402075014, 9781402075018, 2003.

[Le-Bars, 08] Le Bars A.. Les mutations de la sous-traitance automobile en Rhône-Alpes, Observatoire des mutations économiques : La sous-traitance automobile, Présentation, 2008.

[Lonchampt, 04] Lonchampt P.. Coévolution et processus de conception intégrée de produits : Modèle et support de l'activité de conception, Thèse de doctorat, Institut national polytechnique de Grenoble, Grenoble (France), 2004.

[Macmillan&al, 01] Macmillan S., Steele J., Austin S., Kirby P., Spence R.. Development and verification of a generic framework for conceptual design, Design Studies, vol 22, no 2, pp 161-191, 2001.

[Mallard, 07] Mallard O.. Fiabilité : Relation Client/fournisseur. Atelier SIA (Société des ingénieurs de l'automobile) Management de la fiabilité, 30 Novembre 2007, Suresnes (France).

[Malmqvist, 02] Malmqvist J.. A classification of matrix-based methods for product modeling, 7th international design conference, 14-17 Mai 2002, Dubrovnik (Croatie).

[Martin, 01] Martin C.. Modélisation du Processus de Conception par l'Intégration Méthodologique, Thèse de doctorat, Ecole centrale des arts et manufactures, Chatenay-Malabry (France), 2001.

[Mazouni&al, 08] Mazouni M-H., Aubry J-F., El Koursi M.. Méthode systémique et organisationnelle d'Analyse Préliminaire des Risques basée sur une ontologie générique, Publié dans Workshop Surveillance, Sûreté et Sécurité des Grands Systèmes, 3SGS'08, 4-5 juin 2008, Troyes (France).

[McCorquodale&al, 03] McCorquodale M.S., Gebara F.H., Kraver K.L., Marsman E.D., Senger R.M., Brown R.B.. A Top-Down Microsystems Design Methodology and Associated Challenges, Conference and Exhibition Design Automation and Test in Europe, 3-7 mars 2003, Munich (Allemagne).

[Medjoudj, 06] Medjoudj M.. Contribution à l'analyse des systèmes pilotés par calculateurs : Extraction de scénarios redoutés et vérification de contraintes temporelles, Thèse de doctorat, Université Paul Sabatier, Toulouse (France), 2006.

[Menand, 02] Menand S.. Modélisation pour la réutilisation du processus de conception multi acteurs de produits industriels, Thèse de doctorat, Institut national polytechnique de Grenoble, Grenoble (France), 2002.

[Mercantini, 08], Mercantini J-M.. Construction d'ontologies pour la résolution de problèmes de sécurité : une étape vers l'ontologie du risque, 16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement (lm16), 7-9 octobre 2008, Avignon (France).

[Minel, 04] Minel J-L.. Texte et fouille textuelle. Réseau thématique " Médiation des savoirs, des langues et des cultures ", 3 Avril 2004, Lille (France).

[Mortureux, 01] Mortureux Y.. La sûreté de fonctionnement : méthodes pour maîtriser les risques. Dossier AG 4670 des Techniques de l'ingénieur, 2001.

[Nancy, WEB] http://web.univ-pau.fr/~nancy/sadt/.

[Noyes&al, 07] Noyes D., Peres F.. Analyse des systèmes : Sûreté de fonctionnement. Dossier AG 3520 des Techniques de l'ingénieur, 2007.

[Oliveira&al, 06] Oliveira M.F., Brião E.W., Nascimento F.A., Brisolara L., Carro L., Wagner F.R.. Multi-objective Design Space Exploration based on UML, 43ème conférence Design Automation, 24-28 juillet 2006, San Francisco (Californie/USA).

[Pahl et Beitz, 96] Pahl G., Beitz W.. *Engineering Design: a Systematic Approach*, Springer-Verlag, London, 2nd édition, ISBN 3540199179, 1996.

[Perepletichov, 05] Perepletichov M., Ryan C., Tari Z.. The Impact of Software Development Strategies on Project and Structural Software Attributes in SOA, p442-451, On the Move to Meaningful Internet Systems 2005: OTM Workshops, ISBN 9783540297390, 2005.

[Perrin&al, 03] Perrin F., Millet D., Camous R., Aoussat A.. Amélioration des reflexes de conception par intégration de nouvelles méthodes : Proposition d'un processus d'apprentissage, 3ème conférence internationale en Conception et Production intégrées CPI 2003, 22-24 octobre 2003, Méknès (Maroc).

[Perry, 07] Perry N.. Industrialisation des connaissances : approches d'intégration pour une utilisation optimale en ingénierie (cas de l'évaluation économique), Habilitation à diriger les recherches, Université de Nantes, Nantes (France), 2007.

[PRIMA, 99] Prima consortium. Project Risk Management. Disponible sur : Http:// http://www.esi2.us.es/prima/ (dernière consultation le 06/02/2009).

[Qualite_online, WEB] Site dédié au management de la qualité, disponible sur http://www.qualiteonline.com/.

[Quatrain&al, 04] Quatrain Y., Nugier S., Peradotto A., Garrouste D.. Évaluation d'outils de Text Mining : démarche et résultats, 7ème journées internationales d'analyse des données textuelles JADT 2004, 10-12 mars 2004, Louvain (Belgique).

[Rakoto&al, 04] Rakoto H., Clermont P., Geneste L., Poret G.. Proposition d'une architecture de retour d'expérience pour la gestion des connaissances dans les processus industriels, 2ème Colloque du groupe de travail C2EI : Modélisation et pilotage de systèmes de Connaissances et de Compétences dans les Entreprises Industrielles, 1-2 Décembre 2004, Nancy (France).

[Ribiere&al, 99] Ribière M., Matta N., Corby 0.. Définition d'un Modèle de mémoire de projet, Rapport de recherche INRIA N° 3720, Juin 1999.

[Rigamonti&al, 04] Rigamonti M., Hadjar K., Lalanne D., Ingold R.. Xed : un outil pour l'extraction et l'analyse de documents PDF, Colloque International Francophone sur l'écrit et le document CIFED 2004, 21-25 juin 2004, La Rochelle (France).

[Roure, 06] Roure J-M.. Forecast reliability for electronic Boards, Atelier SIA Profil de mission, 29 novembre 2006, Suresnes (France).

[Sadou, 07] Sadou N.. Aide à la conception des systèmes embarqués sûrs de fonctionnement, Thèse de doctorat, Université Paul Sabatier, Toulouse (France), 2007.

[Sallaou&al, 05] Sallaou M., Pailhes J., Nadeau J.P.. Formulation d'une base de connaissances pour l'aide en conception, 4ème Conférence Internationale en Conception et Production Intégrées CPI 2005, 9-11 novembre 2005, Casablanca (Maroc).

[Scaravetti, 04] Scaravetti D.. Formalisation d'un problème de conception pour l'aide à la décision en conception préliminaire, Thèse de doctorat, Ecole nationale supérieure d'arts et métiers - Centre de Bordeaux, Bordeaux (France), 2004.

[Schoenig, 04] Schoenig R.. Définition d'une méthodologie de conception des systèmes mécatroniques sûrs de fonctionnement, Thèse de doctorat, Institut national polytechnique de Lorraine, Nancy (France), 2004.

[Simeu, 05] Simeu E.. Test et surveillance intégrés des systèmes embarqués, Habilitation à diriger les recherches, Université Joseph Fourier de Grenoble, Grenoble (France), 2005.

[Simonot-Lion&al, 06] Simonot-Lion F., Song Y.. Design and validation process of in-vehicle embedded electronic systems, The Embedded Systems Handbook par Zurawski R. chapitre 41, ISBN 0849328241, 9780849328244, 2006.

[Souchier&al, 03] Souchier E., Jeanneret Y, Le Marec J. Lire, écrire, récrire. Etudes et Recherche de la Bibliothèque du Centre Pompidou, édition 2003.

[Tassinari, 06] Tassinari R.. Pratique de l'analyse fonctionnelle, 4ème édition, ISBN 2100500384, Dunod, 2006.

[Tounkara, 02] Tounkara T.. Gestion des connaissances et Veille : vers un guide méthodologique pour améliorer la collecte d'informations », Thèse de doctorat, Université Paris IX, Paris (France), 2002.

[Tuffery, 06] Tuffery S.. Data-mining et statistique décisionnelle, Cours de data-mining. Disponible sur http://data.mining.free.fr, 2006.

[Turinetti, 83] Turinetti D.. Calcul de blocs diagrammes complexes de fiabilité par la méthode dite des "matrices de conditions", Revue de statistique appliquée, tome 31, n°3, p. 27-37, disponible sur http://www.numdam.org/item?id=RSA_1983__31_3_27_0, 1993.

[Turner&al, 05] TURNER H.R., Stepneys S., Polack F.A.C.. Rule Migration: Exploring a design framework for emergence, disponible sur http://www-users.cs.york.ac.uk/~susan/bib/ss/nonstd/ijuc2-4.pdf, International Journal of Unconventional Computing, 2007.

[VEMS, 05] Valeo. Exigences de fiabilité et leurs validations : Application au ECUs, Atelier SIA Exigences de fiabilité et leurs validations pour un système électronique, 15 décembre 2005, Suresnes (France).

[Villemur, 97], Villemur A.. Sûreté de fonctionnement des systèmes industriels, édition Eyrolles, 1997, ISBN : 2212016158.

[Wagner, 07] Wagner C.. Specification risk analysis : avoiding product performance deviations through an FMEA-based method, Thèse de doctorat, Technische Universität München, Munich (Allemagne), 2007.

[Wu&al, 08] Wu C-H., FanJiang Y-Y.. Towards the Integration of UPES and UML-RT for Developing an Embedded Software, 22nd ACM International Conference on Supercomputing, 7-12 juin 2008, Ile de Kos (Grèce).

[Zafra-Cabeza&al, 02] Zafra-Cabeza A., Ridao M.A., Camacho E.F.. A decision support system for bidding process. Actes du 15ème congrès mondial de contrôle automatique IFAC 2002, 21-26 juillet 2002, Barcelone (Espagne).

[Ziegler, 05] Ziegler R.J.. Complexity reduction in automotive design and development, Rapport de master en science de l'ingénieur et management, Massachusetts institute of technology, 2005.

[Zwingmann, 05] Zwingmann X.. Modèle d'évaluation de la fiabilité et de la maintenabilité au stade de la conception, Thèse de doctorat en cotutelle, Faculté des sciences et de génie industriel de Laval (Québec/Canada) / Université Louis-Pasteur, Strasbourg (France), 2005.