Evaluation prévisionnelle de l'impact de réalisation de la sûreté de fonctionnement d'un « produit »

Anne-Lise Benaben
Safran Engineering Services
Toulouse France

Daniel Noyes/ François Pérès
Laboratoire Génie de Production - ENIT-INPT
Tarbes, France

***Abstract*—Nous proposons dans ce travail une approche d'évaluation, en amont du cycle de développement d'un produit, de l'impact des exigences de sûreté de fonctionnement (SdF) sur la réalisation du projet associé. La nécessité d'allier les connaissances SdF et celles « métier » sur les dimensions fonctionnelles et structurelles du produit nous fait utiliser un formalisme de représentation matricielle. Nous présentons ce type de modèle et illustrons la démarche d'exploitation pour évaluer, tôt dans le projet, les effets de la dimension SdF du produit.**

***Index Terms*— Evaluation prévisionnelle de sûreté, satisfaction des exigences, modèle matriciel.**

I. INTRODUCTION

La sûreté de fonctionnement (SdF) des produits, des systèmes et des services est une préoccupation permanente de tous les acteurs industriels.

Les exigences SdF forment une part importante de la plupart des CdC de réalisation de ces entités et, souvent même, elles constituent la « partie dure » du CdC. C'est notamment le cas lorsque sont fixés des niveaux d'intégrité de sécurité (SIL) à valider par rapport à des objectifs de sécurité fixés.

Dans ces situations, alors que le client n'était initialement intéressé que par les résultats, il requiert aujourd'hui, dès les négociations (dans l'appel d'offre (AO) par exemple), une information précise sur la démarche même que le prestataire prévoit de mettre en place pour satisfaire à ces exigences.

De même, le soumissionnaire à un appel d'offre s'appuie souvent sur sa capacité à satisfaire les attentes SDF du client pour décider de sa participation à l'AO.

Aussi, dans ce type de contexte, il devient essentiel de savoir identifier très tôt, en amont du cycle de développement du produit, l'impact des exigences SDF sur la réalisation et le devenir du projet.

La démarche SdF pour analyser, réaliser et valider les exigences SdF est assurée par l'engagement séquentiel ou combiné de méthodes SdF organisées autour des axes fonctionnel et dysfonctionnel de « l'objet » d'étude [1] (cf. figure 1).

Les différents travaux sur la SdF sont unanimes sur le fait que la phase préalable à toute analyse SdF est la réalisation d'une analyse fonctionnelle souvent formée d'une analyse fonctionnelle externe (AFE) suivie d'une analyse fonctionnelle interne (AFI) [2] [3].

L'AFE permet de définir les limites du système ainsi que la définition des fonctions de service (ce pour quoi le système est conçu) et des 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.

En sortie, l'analyste dispose de l'ensemble des fonctions qui devront être reliées à leurs supports matériels afin de permettre, dans les étapes d'analyse suivantes, d'identifier, pour un mode de défaillance particulier, les causes et les effets de cette défaillance.

La phase suivante consiste à identifier les risques. Plusieurs méthodes peuvent être engagées, l'analyse préliminaire des risques (APR) étant la plus courante. La méthode consiste à identifier les points du système qui peuvent être critiques en termes de sécurité, à évaluer les risques correspondants, les scénarios associés et à définir des critères de conception à respecter. A ce niveau, l'étude des défaillances du « produit » pourra être menée à partir d'AMDEC(s) [4], [5]. 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) et les plans d'actions à mettre en œuvre afin de diminuer la criticité en faisant varier un des trois facteurs.

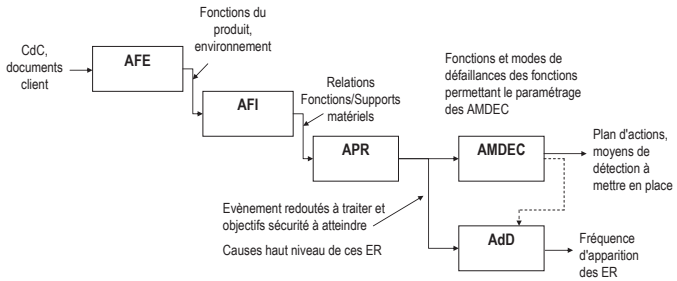

Fig.1 – Processus d'analyse SDF

Enfin, l'appui des arbres de défaillances (AdD), notamment pour la gestion de l'aspect sécurité, permettra pour un évènement donné, d'étudier les combinaisons de défaillances pouvant conduire à celui-ci. On obtient en sortie les scénarios de défaillance 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.

Toutes ces phases sont « classiques » mais difficilement réalisables en phase préliminaire du projet (lors du processus de réponse à l'appel d'offre, par exemple) car :

- la réactivité souhaitée 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 et, notamment, des décideurs concernés ; les représentations du produit sont assez éloignées des représentations métiers classiques alors même que l'étude de la SDF ne peut être décorrélée des connaissances métiers intervenant pour la réalisation du produit,
- 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.

C'est à ce niveau qu'est située notre contribution qui concerne les phases amont du cycle de développement du produit, au stade des négociations client-prestataire, à l'intersection des domaines de la sûreté de fonctionnement et de la conception de produit.

Dans ce contexte, nous proposons « d'associer » aux méthodes classiques, l'emploi de modèles « produit », basés sur une représentation matricielle afin de :

- réaliser des études rapides pour affiner ou compléter une exigence SDF particulière, non analysable en l'état (car nécessitant des méthodes et outils utilisés lors des phases de développement),
- 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,
- 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.

Soulignons immédiatement que nous avons conduit cette étude dans un cadre partenarial avec un équipementier automobile, profession confrontée à des clients de plus en plus exigeants en matière de SDF.

Le papier est organisé en trois sections principales. Nous décrivons d'abord les éléments de représentation matricielle permettant d'appréhender les « dimensions » significatives du produit pour aider à l'estimation de l'impact de la SDF sur celui-ci. Nous présentons ensuite des éléments de saisie de l'expertise métier. Nous proposons enfin un scénario de traitement d'exigences de sécurité utilisant la connaissance ainsi formalisée.

II. MODELES MATRICIELS

Comme nous venons de l'évoquer, l'étude de la SdF d'un système consiste à identifier et analyser 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.

Nous nous intéressons aux caractéristiques de fiabilité et de sécurité du produit que nous allons considérer à travers ces mêmes caractéristiques fonctionnelles (corrélées à la vue client), structurelles (proches de l'expertise métier) et comportementales (liées aux exigences SdF).

Nous retrouvons cette approche dans [6] où l'auteur s'intéresse à l'intégration de la validation dans le processus de conception. Dans ce papier, Zwingmann fait état d'un manque de travaux concernant l'évaluation des performances dans la conception et 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.

A. Représentation matricielle

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 qui unissent ces deux formes de caractérisation du produit.

Dans [7], les auteurs explicitent ces trois éléments.

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, A_F) dans lequel les nœuds Fi représentent les fonctions et les arcs A_Fi→Fj les échanges de données de Fi à Fj.

De la même façon, l'architecture matérielle peut être vue comme un graphe orienté (BS, A_BS) dans lequel les nœuds BS représentent les supports ou "Blocs Structurels" réalisant les fonctions et les arcs A_BSi→BSj représentent les connexions entre les différents blocs du système.

Enfin, il faut modéliser la façon dont les fonctions sont supportées par les solutions matérielles en exprimant les liens d'allocations entre ces deux espaces de réalisation.

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 Chakrabarti dans [8], 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 2.

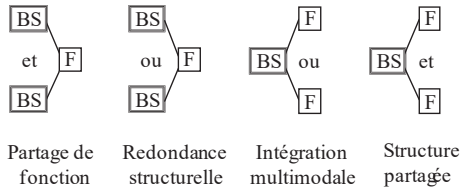

Fig.2. Types de relation F – BS adaptés de Chakrabarti

Au final, 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.
Dans [9], l'auteur présente différents types de méthodes de modélisation à base de matrices. Il définit notamment les matrices au niveau élément afin de représenter les liens existants entre différents éléments du système ou du produit.
Ces liens peuvent exprimer :

- les 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,...,) ; il s'agit de matrices intra-domaines,
- les couplages entre éléments de différents types (fonction/bloc structurel,...,) ; il s'agit alors de matrices inter-domaines.

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. Toujours dans [9], Malmqvist 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, il définit les représentations envisageables pour ces liens dans les matrices :
- relations existantes ou non : matérialisées par la présence ou l'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, optionnel, recommandé,...,
- importance quantitative selon une échelle déterminée : -3, -2,..,+1,+2,...

Nous nous sommes appuyés sur ces résultats pour établir, via les matrices intra-domaine et inter-domaine, les liens que nous souhaitons modéliser.

B. Matrices intra-domaine

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

Deux types de matrices sont distingués :

- les matrices symétriques lorsque la matrice n'a pas de sens de lecture ; ce sont des « 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) ; il s'agit de « matrices temporelles ».

Deux éléments peuvent être liés par une relation. Ce type de relation inclut les fonctions de transfert : information, énergie, matériel.
Dans [10], les auteurs définissent pour les interactions dans un produit (fonctionnel et structurel) 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 cette approche au cas des fonctions que nous considérons. Deux fonctions F1 et F2 peuvent être liées par un lien de type :

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

D'autres formes d'interactions sont possibles selon les produits concernés.

Nous considérons maintenant les interactions entre blocs structurels. 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 : un des deux blocs structurels est susceptible de se substituer à l'autre en cas de défaillance de ce dernier,
- spatial (i.e. relation spatiale) : BS1 est lié physiquement à BS2 soit de façon nécessaire au fonctionnement, soit de façon optionnelle mais qui peuvent être volontaires (protection,...,).

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

C. 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 le biais des blocs structurels.

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 présent de façon volontaire : protection de la fonction, surveillance,...

D. Choix de modélisation des interactions et notations utilisées

Nous présentons les notations que nous utilisons pour les différents types de matrices. Afin de faire apparaître dans les matrices intra-domaines des relations orientées, nous faisons le choix d'utilisation des matrices temporelles dont le sens de lecture est « lignes vers colonnes ».

Nous avons adopté l'exploitation de vecteurs pour la modélisation des liens. Nous détaillons ceux-ci.

- Relations Fonctions/Fonctions
  Nous utilisons un vecteur [L T N] formé de trois composantes :
  - 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 ∩[Ei/Ej] si le lien existe de Ei vers Ej et L = 0 à l'intersection ∩[Ei/Ej] si le lien existe de Ej vers Ei,
  - T définit le type du lien : T = I à l'intersection ∩[Ei/Ej] dans le cas où Ei envoie des informations à Ej, T = E si 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,
  - N définit la (ou les) nature(s) du lien et peut comporter deux informations : i) A ou R pour l'existence d'un lien de réalisation R ou d'assistance A, ii) S, C ou P pour l'existence d'un lien pour la sécurité S, le contrôle C ou la protection P.

- Relations Blocs Structurels/Blocs Structurels
  On retrouve le même type de lien. Nous utiliserons par conséquent le même formalisme de représentation basé sur l'instanciation d'un vecteur [L T N].

- Relations Fonctions/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. Souvent, une composante 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.

  Nous illustrons ces notations matricielles par les exemples de la figure 3.

M[F/F]	.....	Alimenter	Sécuriser
.....	.....	.....	.....
Alimenter	.....		[2 E/I A/C]
Sécuriser	.....	[2 I ./S]	

M[BS/BS]	.....	Alimentation	Superviseur
.....	.....	.....	.....
Alimentation	.....		[2 E A/.]
Superviseur	.....	[2 I ./S]	

M[F/BS]	.....	Alimentation	Superviseur
.....	.....	.....	.....
Alimenter	.....	[R/.]	[./S]
Sécuriser	.....	[A/.]	[R/.]

Fig.3. Exemples de notation matricielle

III. MODELISATION 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.

Dans la modélisation matricielle, nous formalisons les connaissances issues de :

- l'analyse du CdC client,
- 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 encore 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 la structure cognitive utile à sa définition.

Cette étude nous a orientés vers la définition d'attributs permettant de capitaliser l'ensemble des connaissances 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 dans la table I (colonnes 1 et 2) et donnons une illustration pour un bloc structurel de type « Alimentation » (colonne 3).

TABLE I. ATTRIBUTS DES BLOCS STRUCTURELS

	Bloc Structurel BSi	Commentaires	Exemple Alimentation
1	Paramètres de choix du bloc		Tension à fournir
2	Solution standard	Matériel minimum pour remplir la fonction	1 régulateur / 1 circuit standard
3	Variantes	Autres solutions	2 régulateurs / 2 circuits
4	Coût de la solution standard		Coût standard
5	Cout de la solution		Coût solution
6	Fiabilité et/ou λ	$\lambda = \Sigma\, \lambda_{(composants\ de\ la\ solution)}$	$\lambda = \Sigma\, \lambda i$
7	Défaillances	Liste de défaillances possibles de BS	Perte régulateur, perte tension batterie
8	Moyens de détection/protection	Données issues de normes/expériences, permet d'évaluer la couverture de diagostic CD en fonction des mouens mis en place	Vérification de la tension batterie (CD bas)

IV. APPLICATION DE SECURITE

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 (évoquée dans l'introduction) dans la mesure où elle consiste : i) à définir les fonctions impliquées pour un évènement redouté donné (si le client donne les ER à traiter), ii) 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 apparaît que les informations dont nous avons besoin sont les liens entre les états du système et les fonctions. Nous considérons donc 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 égaux à 1 figurant aux intersections ligne/colonne représentent les défaillances de fonctions minimales conduisant à l'ER de la ligne correspondante [11].

Nous présentons sur la table II un exemple de matrice de correspondance entre ER et F.

TABLE II. EXEMPLE DE MATRICE M[ER/F]

	$F1$	$F2$	$F3$	$F4$
$ER1$	1	0	1	0
$ER2$	1	1	0	0
$ER2$	0	0	1	0
$ER3$	0	0	1	1

En explicitant cette matrice, on constate, par exemple que ER 1 apparaît si F1 et F3 sont défaillantes : $ER1 = \overline{F1} \wedge \overline{F3}$.

Plusieurs conditions indépendantes peuvent cependant être à l'origine d'un évènement redouté comme, par exemple, pour ER2 : $ER = (\overline{F1} \wedge \overline{F2}) \vee \overline{F3}$.

A. Démarche générale

Notre objectif 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 de la méthodologie matricielle que nous résumons ci-après.

La démarche comprend cinq phases formées, chacune, de plusieurs activité permettant la définition et l'évaluation des conséquences de la prise en compte des exigences SdF. Nous ne donnons ci-après les trois premières que nous reprenons par la suite (table III). Le lecteur intéressé par l'ensemble de la démarche pourra consulter [12].

- La phase 1 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.).
  Dans [12], Bénaben propose deux algorithmes de paramétrage, dédiés aux matrices [F/F] et [BS/BS] pour l'un et [F/BS] pour l'autre, pour assister l'analyste dans cette phase.
- La phase 2 concerne l'analyse prévisionnelle de la fiabilité du produit. Elle consiste à un calcul du taux de

défaillance du produit par rapport aux taux de défaillance des différents blocs structurels sélectionnés.

- La phase 3 porte sur l'analyse la sécurité du produit et est composée de plusieurs activités :
  -le calcul du taux de défaillance résiduels 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.

TABLE III. PHASES PRINCIPALES DE LA DEMARCHE

Paramétrage Matrices (phase1)	Etablissement M[F/F] (s/phase 1.1)
	Etablissement M[F/BS]] (s/phase 1.2)
	Etablissement M[BS/BS]] (s/phase 1.3)
	Attributs] (s/phase 1.4)
Analyse Fiabilité (phase 2)	Evaluation PPM] (s/phase 2.1)
	Evaluation l] (s/phase 2.2)
Analyse Sécurité (phase 3)	Calcul taux de défaillances résiduelles (s/phase 3.1)
	Analyse des fonctions hors et avec sécurité (s/phase 3.2)
	Calcul des fréquences d'appartion des ER (s/phase 3.3)
	Analyse Temps Réel (s/phase 3.4)
	Analyse des causes de mode commun (s/phase 3.5)

B. Analyse de sécurité

Cette phase correspond à la troisième phase de la démarche présentée dans la table 2. Plusieurs études peuvent être menées dans cette phase.

La première activité (3.1) concerne le calcul du taux de défaillances résiduelles par rapport aux mécanismes de sécurité implémentés (i.e. défaillances susceptibles de survenir malgré les mécanismes de détection des défaillances implémentés sur les différents blocs structurels). 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 point particulier et l'analyse des causes de modes communs.

Nous nous focalisons sur les activités 3.2 et 3.3 qui permettent d'illustrer les principes d'utilisation de la structure matricielle et des calculs y afférents tels qu'ils ont été présentés précédemment.

Soulignons que la démarche que nous présentons ici a été appliquée aux différents éléments de sécurité embarqués dans un environnement automobile pour réaliser les fonctions Suspension Active, ABS et Direction Assistée (figure 4). Pour plus de détails, le lecteur pourra consulter [12].

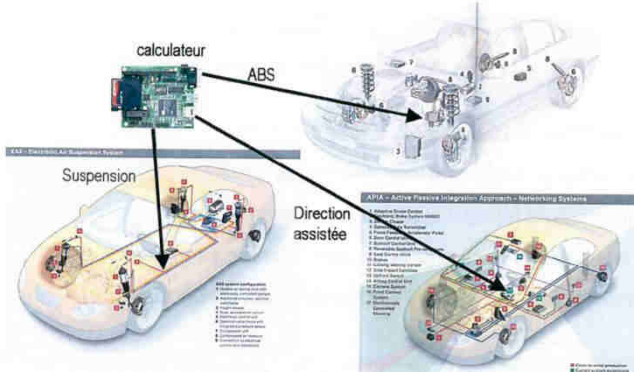

Fig.4. Cas d'application

Comme dans beaucoup de problèmes SdF, les calculs sur le système complet ne permettaient pas d'observer les points faibles du système ce qui justifiait l'utilisation des matrices qui permettent de procéder à des évaluations locales sur des fonctions ou des composants. Pour des raisons de limitation de place et de confidentialité, les résultats afférents ne seront pas exposés.

Analyse des fonctions hors et avec sécurité (Activité 3.2)

Différentes études peuvent être menées sur le fonctionnement du produit :

- 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. La matrice M[F/BS] est utilisée pour la réalisation des calculs correspondants. Comme nous l'avons précisé dans les notations, on ne considèrera 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/j] telles que R = 1 ou A = 1. On ajoute entre eux les taux de défaillances des différents BS ainsi identifiés (en considérant que la perte d'un BS entraîne la perte de la fonction) pour obtenir le taux de défaillance de la fonction :

M[F/BS] ⇒ perte de Fi ⇒ pour les BSk tels que, dans ∩[i/j], la première information de N est égale à R ou A.

On peut aussi analyser le fonctionnement d'une fonction avec l'ensemble des mécanismes de détection et de protection implémentés. Il faut alors ajouter l'ensemble des taux de défaillance 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 ajouter entre eux les taux de défaillances résiduels des différents BS identifiés comme défini ci-après :

M[F/BS] $\Rightarrow$ perte de Fi $\Rightarrow$ pour les BSk tels que $\cap[i/j] \neq 0$.

On peut réaliser ce calcul de façon plus précise en identifiant les blocs communiquant. Le calcul est effectué en plusieurs étapes :

- on identifie, dans la matrice M[F/BS] tous les blocs participant à la fonction dans la réalisation ou l'assistance (R ou A égal à 1),
- dans la matrice M[BS/BS], on identifie ensuite les blocs dédiés à la surveillance, la protection ou la sécurisation (en recherchant les liens de type P, C, S) des blocs précédents.
- on étudie enfin les blocs BSi correspondant à la sécurité de la fonction.

Calcul de la fréquence d'apparition des évènements redoutés (Activité 3.3)

Nous avons montré (cf Table II) comment la matrice de condition M[ER/F] permet l'identification des différentes fonctions impliquées dans l'apparition d'un ER.

Dans cet exemple, F1 était 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. Nous donnons celle-ci pour le même exemple (table IV) dans laquelle 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.

TABLE IV. MATRICE INTER-DOMAINES M[F/BS] CONSIDEREE

	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 cette matrice inter-domaines :

- F1 est réalisée par BS1 et BS2, assistée par BS4, contrôlée par BS5 et sécurisée par BS6,
- F2 est réalisée par BS2 et BS3, assistée par BS4, contrôlée par BS5 et sécurisée par BS6,
- F3 est réalisée par BS4,
- F4 est 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 (table V).

TABLE V. MATRICE INTRA-DOMAINE M[BS/BS] CONSIDEREE

	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/.]	

Il est mis en évidence dans la matrice V le fait 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 ER2 devient :

$$\begin{aligned} ER2 &= (\overline{F1} \wedge \overline{F2}) \vee \overline{F3} \\ &= [((\overline{BS1} \vee \overline{BS2}) \wedge (\overline{BS5} \vee \overline{BS6})) \vee \overline{BS4}] \\ &\quad \wedge [((\overline{BS2} \vee \overline{BS3}) \wedge (\overline{BS5} \vee \overline{BS6})) \vee \overline{BS4}] \\ &\quad \vee \overline{BS4} \\ &= [(\overline{BS1} \wedge \overline{BS5}) \vee (\overline{BS1} \wedge \overline{BS6}) \vee (\overline{BS2} \wedge \overline{BS5}) \vee (\overline{BS2} \wedge \overline{BS6}) \vee \overline{BS4}] \\ &\wedge [(\overline{BS2} \wedge \overline{BS5}) \vee (\overline{BS2} \wedge \overline{BS6}) \vee (\overline{BS3} \wedge \overline{BS5}) \vee (\overline{BS3} \wedge \overline{BS6}) \vee \overline{BS4}] \\ &\vee \overline{BS4} \end{aligned}$$

ce qui, après simplification, donne :

$$ER2 = [(\overline{BS5} \vee \overline{BS6}) \wedge [(\overline{BS1} \wedge \overline{BS3}) \vee \overline{BS2})]] \vee \overline{BS4}]$$

L'arbre correspondant peut être établi pour les blocs structurels à partir des analyses précédentes (figure 5).

Sur l'arbre, la spécificité de stratégie de sécurité des produits considérés apparaît sous la forme de l'opérateur ET reliant les Blocs Structurels 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.

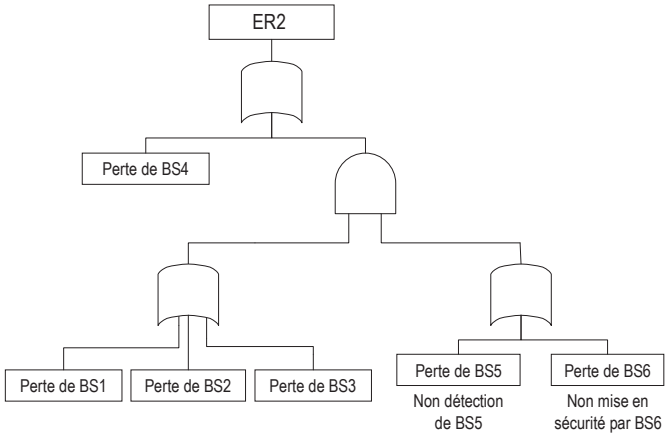

Fig.5. Arbre de fautes

C. Conclusion

Nous avons proposé une approche d'évaluation prévisionnelle de l'impact des exigences SdF sur la réalisation d'un produit. Nous nous sommes appuyés pour cela sur une représentation de la connaissance « métier » sur les vues fonctionnelle, organisationnelle et comportementale du produit.

La représentation matricielle que nous préconisons fournit un support efficace pour les analyses SdF à partir d'une représentation facilement utilisable par les acteurs.

Cette méthodologie dont nous avons défini les principes mais aussi le mode de mise en oeuvre est applicable à de nombreux contextes dès lors que le produit décomposable en fonctions et en blocs structurels.

Son instanciation pourrait conduire à la mise en oeuvre de bibliothèques dédiées constituées de primitives descriptives du produit ou de modèles de comportements situés au niveau le plus bas de généricité. Leur utilisation devrait favoriser très fortement la réactivité du processus d'analyse SdF dans les phases amont des projets.

REFERENCES

[1] D. Noyes et F. Pérès. Analyse des systèmes : Sûreté de fonctionnement. Dossier AG3520 des Techniques de l'ingénieur, 2007.

[2] M. Medjoudj. Contribution à l'analyse des systèmes pilotes par calculateurs : extraction de scénarios redoutés et vérification de contraintes temporelles, Thèse de doctorat, Université Paul Sabatier, Toulouse (France), 2006.

[3] A. Demri, A. Charki, F. Guerin, P. Kahn, H. Christofol. Analyse Qualitative et Quantitative d'un Système Mécatronique, 5ème confèrence internationale en Conception et Production intégrées CPI 2007, 22-24 octobre 2007, Rabat (Maroc).

[4] C. Wagner. Specification risk analysis: avoiding product performance deviations through an FMEA-based method, Thèse de doctorat, Technische Universitat Munchen, Munich (Allemagne), 2007.

[5] VEMS-Valeo. Exigences de fiabilité et leurs validations : Application au ECUs, Atelier SIA Exigences de fiabilité et leurs validations pour un système électronique, déc. 2005, Suresnes (France).

[6] X. Zwingmann. 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.

[7] X. Dumas, C. Pagetti, L. Sagaspe, P. Bieber, P. Dhaussy. 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).

[8] A. Chakrabarti. Sharing in design - categories, importance, and issues, International Conference on Engineering Design ICED 01, 21-23 aout 2001, Glasgow (U.K.).

[9] J. Malmqvist. A classification of matrix-based methods for product modeling, 7th international design conference, 14-17 Mai 2002, Dubrovnik (Croatie).

[10] S.D. Eppinger, T.U. Pimmler. Integration Analysis of Product Decompositions, ASME Design Theory and Method Conference DTM'94, Vol 68, pp. 343-351, Sept. 1994, Minneapolis (USA).

[11] D. Turinetti. Calcul de blocs diagrammes complexes de fiabilite par la méthode dite des "matrices de conditions", Revue de statistique appliquee, tome 31, n°3, 1983.

[12] A.L. Benaben. Méthodologie d'identification et d'évaluation de la sûreté de fonctionnement en phase de réponse à appel d'offre. Thèse de doctorat, INP Toulouse, 2009.