Aide à la décision pour l'intégration de la sécurité au plus tôt en phase de conception : approche innovante de reconception de machines agricoles

Leyla Sadeghi

EDSP
École Doctorale
Sciences Pratiques

ENS CACHAN

ENSC-2014-XXX

THESE DE DOCTORAT
DE L'ECOLE NORMALE SUPERIEURE DE CACHAN

Présentée par

Leyla SADEGHI

en vue de l'obtention du grade de

DOCTEUR DE L'ECOLE NORMALE SUPERIEURE DE CACHAN

Domaine :
MECANIQUE- GENIE MECANIQUE – GENIE CIVIL

Sujet de la thèse :

Aide à la décision pour l'intégration de la sécurité au plus tôt en phase de conception - Approche innovante de reconception de machines agricoles

Thèse présentée et soutenue à Cachan le 21 juillet 2014 devant le jury composé de :

Pascal RAY	P.U. - IFMA	Président
Elie FADIER	D.R. - INRS	Rapporteur
Jean-Yves DANTAN	P.U. - Arts et Métiers ParisTech, Metz	Rapporteur
Luc MATHIEU	P.U. - Université Paris-Sud	Directeur de thèse
Lama AL-BASSIT	I.R. - Irstea Antony	Co-encadrant
Nicolas TRICOT	C.R. - Irstea Antony	Co-encadrant
Dominique DUFUMIER	Référent agricole et maritime - DGT	Invité

Laboratoire Universitaire de Recherche en Production Automatisée
ENS CACHAN / Paris-Sud XI / EA 1385
61, avenue du Président Wilson, 94235 CACHAN CEDEX (France)

Remerciements

Le travail de recherche exposé dans ce mémoire de thèse a été réalisé dans le cadre d'une convention entre le Laboratoire Universitaire de Recherche en Production Automatisée (LURPA – EA 1385) de l'École Normale Supérieure de Cachan / Paris-Sud et l'Unité de Recherche Technologies pour la Sécurité et les Performances des Agroéquipements (TSAN) du Centre de Recherche de l'Irstea (Institut National de Recherche en Sciences et Technologies pour l'Environnement et l'Agriculture) d'Antony.

Je tiens tout d'abord à remercier les responsables de l'Irstea qui m'ont confié et financé ce projet de recherche.

Je remercie le Professeur Luc Mathieu, de l'Université Paris-Sud, pour avoir assuré la direction scientifique de mes travaux. Je le remercie également pour ses nombreux conseils et son écoute.

Je remercie Monsieur Nicolas Tricot, chargé de recherche à l'Irstea, pour sa disponibilité et ses conseils tout au long de ce travail et son aide précieux pour la rédaction de ce manuscrit.

Je remercie Madame Lama Al Bassit, ingénieur de recherche à l'Irstea, pour son aide et ses conseils qui m'ont permis de progresser dans mon travail.

Je remercie le Professeur Jean-Yves Dantan et le Directeur de Recherche Elie Fadier d'avoir accepté d'être rapporteurs de cette thèse. J'adresse également mes remerciements aux Professeur Pascal Ray et Monsieur Dominique Dufumier d'avoir accepté de participer au jury.

Merci aux membres du LURPA pour leur accueil et leur sympathie.

Merci à l'ensemble du personnel de l'Unité TSAN pour son soutien et sa bonne humeur.

Enfin, je souhaite exprimer ma plus grande reconnaissance à mes parents. Un grand merci à eux, pour leur amour, leur soutien inébranlable et leurs encouragements. Je remercie Mohsen, Hossein, Samira, Rezvan et Behnam qui m'ont toujours encouragé et soutenu sans limite.

Table des matières

Liste des Figures

Liste des tableaux

Acronymes utilisés

Symboles et abréviations	Description
AD	Axiomatic Design
AdC	Arbre des Causes
AdD	Arbre de Défaillance
AMDEC	Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
ARM	Arbre Récepteur Machine
ATC	Arbre de Transmission à Cardans
BDF	Bloc Diagramme Fonctionnel
Dom	Dommage
Ed	Evénement dangereux
F_s	Facteurs de Risque liés au système
F_h	Facteur de Risque lié à l'humain
F_e	Facteur de Risque lié à l'environnement
FRES	Functional Reverse Engineering for Safety
FR2ES	Functional RE-Engineering for Safety
IDEF0	Icam DEFinition for Function Modeling, où "Icam" correspond à Integrated computer aided manufacturing
IRAD	Innovative Risk Assessment Design
P_D	Présence de Danger
P_{Ed}	Présence d'un Evénement dangereux
P_{Pd}	Présence d'un Phénomène dangereux
P_{Sd}	Présence d'une Situation dangereuse
I_S	Indicateur de Sécurité
I_{Smp}	Indicateur de Sécurité du moyen de protection
I_{Ss}	Indicateur de Sécurité du système
I_{Sssmp}	Indicateur de Sécurité du système sans moyen de protection
LTP	Liaison Trois Points
N_f	Niveau de fiabilité
N_R	Niveau de Risque
N_{REd}	Niveau de Risque lié à l'Evénement dangereux
N_{RPd}	Niveau de Risque lié au Phénomène dangereux
N_{RSd}	Niveau de Risque lié à la Situation dangereuse
OTé	Organigramme Technique étendu
Pd	Phénomènes dangereux
PdF	Prise de Force
Q_C	Qualité de conception
Sd	Situation dangereuse
SdT	Situation de Travail
T	Temps
TRIZ	Théorie de la Résolution des Problèmes d'invention

Introduction générale

L'utilisation des machines agricoles est à l'origine de nombreux accidents. Ces accidents ne diminuent que très peu malgré l'ensemble des mesures prises pour les endiguer. La réglementation, les normes de sécurité et les nouvelles technologies utilisées pour améliorer la sécurité et le confort des utilisateurs telles que proposées aujourd'hui sont soit insuffisantes soit non ou mal appliquées.

La discipline de la **conception** des produits tente de répondre aux besoins des clients en se basant sur des lois et théories. La discipline de la **sécurité humaine** est, quant à elle, régie par des observations et des constats en situation d'utilisation ou par l'analyse du produit proposé. La discipline de **l'aide à la décision** aide les ingénieurs dans leur démarche de choix pour augmenter la qualité des produits, réduire le coût de fabrication, etc. Notre problématique est à l'intersection de ces trois disciplines.

Cette problématique à laquelle chercheurs et concepteurs sont confrontés est la suivante : *Comment intégrer la **sécurité humaine** dans le processus de **conception** des machines ?*

Dans un précédent travail de thèse, le développement d'une nouvelle méthode (IRAD : Innovative Risk Assessment Design) de conception par Rima Ghemraoui a permis de tracer les grandes lignes permettant de cadrer l'intégration de la sécurité au plut tôt au cours du processus de conception des machines. Cependant, cette méthode n'est pas utilisable en l'état par les concepteurs car nécessitant des approfondissements et des outils de mise en œuvre afin de la rendre opérationnelle.

Dans ce contexte, la présentation de ce travail de thèse est articulée autour de six chapitres nous permettant d'exposer les problématiques industrielles et scientifiques de nos travaux, nos contributions ainsi que leur mise en œuvre.

Le **chapitre 1** débute par une présentation des besoins industriels et problématiques scientifiques de la thèse. Ensuite, il présente un état de l'art des méthodes et des approches de conception sécuritaire des points de vue normatif et scientifique. Cet état de l'art se poursuit par la présentation de la structure et de la mise en œuvre de la méthode IRAD. A partir de ce cadre bibliographique, une liste des problématiques à résoudre est établie et un cadre méthodologique pour la conception sécuritaire est défini. Ce cadre méthodologique s'appuie sur deux développements complémentaires : une approche d'ingénierie inverse fonctionnelle pour la sécurité (ou FRES pour Functional Reverse Engineering for Safety) et une approche de réingénierie fonctionnelle pour la sécurité (ou FR2ES pour Functional ReEngineering for Safety).

Le Retour d'EXpérience (REX) manque de formalisation pour être intégré de manière structurée dans la conception sécuritaire. Le **chapitre 2** répond en partie à ce manquement en proposant une structure type de rapport d'accident. Cette dernière est ensuite utilisée pour décrire quatre accidents impliquant deux systèmes (la liaison trois points et l'arbre de transmission à cardans) très accidentogènes.

S'appuyant sur les démarches FRES et FR2ES, l'opérationnalisation d'IRAD est réalisée dans les **chapitres 3, 4 et 5**. Chacun de ces chapitres comporte deux sections principales et chaque section comporte cinq sous sections : l'introduction, l'état de l'art, le

développement de l'approche, l'application de l'approche proposé sur l'arbre de transmission à cardans, la conclusion, la discussion et les perspectives.

Les **chapitres 3 et 4** présentent le développement de l'approche FRES.

Le **chapitre 3** propose, dans un premier temps, une approche d'extraction des connaissances sur les accidents à partir de l'analyse des rapports formels d'accident et, dans un deuxième temps, une approche d'extraction des connaissances de la conception de la partie du système impliquée dans l'accident.

Le **chapitre 4** porte sur l'évaluation de la sécurité en identifiant le type de risque lié au système et en mesurant son niveau de sécurité. Il propose dans un premier temps une approche d'identification et de ventilation du risque selon les phases de la conception et dans un deuxième temps un indicateur de sécurité pour l'évaluation du niveau de sécurité d'un système.

Le **chapitre 5** décrit l'approche FR2ES. Il comporte deux sections principales. La première section propose une approche pour la définition et la priorisation des objectifs de sécurité pour un risque donné. La seconde section définit une approche de reconception sécuritaire.

Le **chapitre 6** est consacré au développement d'une approche de conception sécuritaire synthèse des démarches FRES et FR2ES présentées auparavant, dans laquelle l'opérationnalisation d'IRAD est démontrée. Cette approche y est ensuite mise en œuvre en vue de la reconception de la liaison trois points.

Finalement, et après avoir rappelé de manière synthétique les résultats obtenus, ce manuscrit se conclut par la proposition de perspectives de recherche.

Chapitre 1. Contexte, état de l'art et proposition d'un cadre de conception sécuritaire

1.1. Introduction

Ce premier chapitre a pour objectif d'exprimer le contexte et la problématique de nos travaux et de proposer un cadre méthodologique pour la conception sécuritaire.

Dans ce sens, la section 1.2 présente les contextes, besoins industriels et problématiques scientifiques de la thèse. La section 1.3 présente une étude bibliographique sur les méthodes et les approches de conception sécuritaire des points de vue normatif et scientifique. Elle se poursuit par la présentation du principe, de la structure, des caractéristiques clés et des cas d'application de la méthode IRAD. Cette section se termine par une liste des problématiques à résoudre. Enfin, dans la section 1.4, nous construisons un cadre méthodologique pour la conception sécuritaire en nous basant sur les problématiques listées en fin de section 1.3. Nous clôturons ce chapitre par la section 1.5.

1.2. Contexte, besoin industriel et problématique scientifique

1.2.1. Contexte industriel et besoin industriel

Le secteur agricole est un secteur très accidentogène. Une partie de ces accidents est liée à l'utilisation des machines agricoles. Ces accidents ne diminuent que très peu, malgré la réglementation, les normes de sécurité et les nouvelles technologies utilisées pour améliorer la sécurité et le confort des utilisateurs.

Dans le domaine agricole comme dans d'autres domaines, une des voies explorées pour l'amélioration de la sécurité des utilisateurs des machines est la prise en compte des risques en fin de conception. En effet, cette démarche intervient à la fin du processus de conception de la machine c'est-à-dire en phase de conception détaillée où les choix techniques sont quasiment voire complètement validés. La conception collaborative répond en partie à ces manquements en faisant intervenir des experts en sécurité dans le processus de conception. Cependant ce type de conception n'est que très rarement mise en œuvre dans le domaine agricole pour des raisons de taille de structure (en particulier dans les TPE et PME) et de moyens et ne solutionne pas tous les problèmes. Dans ce contexte, les concepteurs ne prennent souvent en compte la sécurité du système conçu que selon leur expérience et sans se baser sur une démarche méthodique d'intégration de la sécurité en conception [De La Garza, 2005].

Le besoin industriel peut être défini ainsi: Disposer d'une méthode de conception opérationnalisée sous la forme d'un outil d'aide à la décision permettant d'améliorer la sécurité de tout type de machine par l'intégration des contraintes de sécurité au plus tôt en phase de conception. Notre travail de recherche porte donc sur la définition d'une méthode d'intégration optimale de la santé-sécurité à la conception du produit. L'objectif industriel final est la mise à disposition d'un outil permettant de mettre en œuvre cette méthode par les concepteurs des systèmes.

1.2.2. Contexte et problématique scientifique

Il est apparu nécessaire d'avoir une approche systémique et de prendre en compte les deux disciplines sécurité et aide à la décision tout au long de la conception des produits. Le problème peut être formulé ainsi: *Comment intégrer le retour d'expérience issus des rapports d'accidents et les contraintes de sécurité telles que définies dans les normes par exemple, au plus tôt en phase de conception de la machine ?*

Dans ce contexte, les travaux initiés par la thèse de Rima Ghemraoui [Ghemraoui, 2009] ont permis d'élaborer une méthode de conception sécuritaire. La méthode a été baptisée IRAD, acronyme anglais de méthode de conception innovante pour l'évaluation des risques (*Innovative Risk Assessment Design)*. Pour des applications pratiques, IRAD permet trois cas

d'emploi : (1) l'expression des objectifs de sécurité à partir de l'analyse du retour d'expérience ; (2) l'expression des objectifs de sécurité à partir de l'analyse des risques relatifs aux choix de la conception; (3) la synthèse des solutions « sécuritaires » à la base des exigences fonctionnelles de sécurité et techniques. L'applicabilité de la méthode IRAD a été montrée sur le cas de la liaison entre un tracteur agricole et un outil attelé.

Le principe de la méthode IRAD est basé sur la mise en parallèle d'un processus de conception, décomposé suivant les principes de la conception systématique et de la conception axiomatique, et d'un processus de risque.

Cette méthode n'est pas utilisable en l'état par les concepteurs de machines. Elle nécessite en particulier des approfondissements et des outils. En d'autres termes, le travail de cette recherche va consister à rendre la méthode IRAD opérationnelle. En conséquence, nous serons amenés à prendre en compte les documents normatifs traitant de la sécurité.

Pour illustrer les solutions proposées par cette recherche, nous considérerons également la liaison tracteur-outil, système très accidentogène. Nous nous intéresserons en plus du système « liaison trois points » déjà traité dans la thèse de Rima Ghemraoui, au système « arbre de transmission à cardans ».

1.2.3. Explicitation du sujet

Cette thèse intitulée « Aide à la décision pour l'intégration de la sécurité au plus tôt en phase de conception - Approche innovante de reconception de machines agricoles » s'insère dans le domaine du « Design for X », et plus spécifiquement dans le domaine du « Design for safety » que l'on peut traduire par « Conception Sécuritaire ». Ces travaux se trouvent à la croisée de trois domaines : la **conception**, la **sécurité** et l'**aide à la décision** (figure 1.1). Le domaine de l'aide à la décision, non utilisé dans IRAD, est intégré dans le champ d'investigation de cette thèse dans l'objectif de rendre opérationnelle la méthode IRAD.

Nous proposons dans cette partie de définir les différentes notions et concepts importants utilisés plus tard dans ce manuscrit ainsi que, suivant les cas, les travaux scientifiques fondateurs ou les documents normatifs de référence. Une synthèse où les choix terminologiques sont précisés est ensuite proposée.

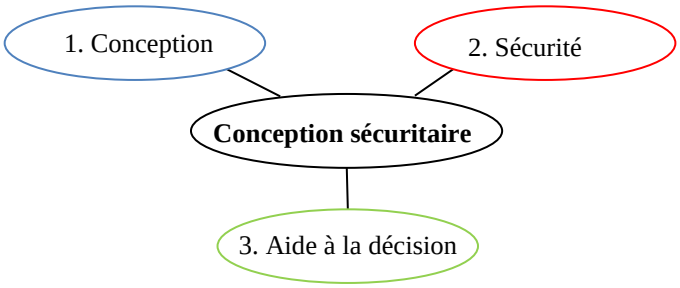


Figure 1.1. Les trois principaux domaines de notre recherche.

1.2.3.1. Conception

Pour présenter le concept de « conception », nous nous basons sur la méthode IRAD [Ghemraoui, 2009]. IRAD repose sur un modèle d'intégration de la sécurité au plus tôt en phase de conception basé sur les méthodes de la conception systématique [Pahl et Betz, 2007] et la théorie de la conception axiomatique [Suh, 1990]. IRAD définit un processus de conception et le décompose en six phases. Nous présentons ci-dessous les notions de « processus de conception » et de « phase de conception » de façon à mieux cerner cette notion de conception.

Processus de conception

Selon [Suh, 1990], le processus de conception est un cheminement itératif et séquentiel entre quatre domaines : le domaine client, le domaine fonctionnel, le domaine physique et le domaine du processus. Il considère que la conception consiste en un processus de mappage entre ces différents domaines. Ce mappage décrit la transition d'un domaine à un autre. Pour [Pahl et Beitz, 2007], le processus de conception est un processus systématique en quatre phases : la clarification de la tâche, la conception conceptuelle, la conception architecturale, et la conception détaillée.

Phase de conception

IRAD propose six phases pour le processus de conception en faisant le lien entre les deux domaines de la conception axiomatique (le domaine fonctionnel et le domaine physique) et les trois phases de l'approche systématique (la conception conceptuelle, la conception architecturale et la conception détaillée). Nous présentons ces six phases dans le §1.3.4.1 de ce mémoire.

1.2.3.2. Sécurité

Nous trouvons deux types de sécurité concernant les systèmes: la **Sécurité du produit** qui concerne la qualité du produit et son utilisation sans risque et la **Sécurité au travail** qui concerne la prévention des accidents du travail. Comme nous l'avons exprimé précédemment, nous nous intéressons à l'amélioration de la sécurité des utilisateurs de machines agricoles. La notion de sécurité couvre donc ici la santé et la sécurité au travail. Dans la suite, la notion de sécurité et son évolution dans le temps sont détaillées.

Dans le dictionnaire Larousse, la sécurité est définie de trois manières différentes mais complémentaires :

- « *Situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger, à aucun risque, en particulier d'agression physique, d'accidents, de vol, de détérioration* » ;
- « *Situation de quelqu'un qui se sent à l'abri du danger, qui est rassuré* » ;
- « *Absence ou limitation des risques dans un domaine précis* ».

Selon [Polet, 2002], la sécurité est l'aptitude d'une entité à éviter des événements critiques ou catastrophiques qui peuvent endommager les humains, les biens ou l'environnement. [Hollnagel, 2008] lie également la sécurité et le risque. Il considère la sécurité comme le processus conduisant à l'absence d'un effet indésirable, ce qui signifie globalement, l'absence de risque. La définition de la sécurité proposée par [Mazouni, 2008] est l'absence de danger ou de conditions susceptibles de créer un risque inacceptable. C'est aussi la mesure d'un niveau de confiance vis-à-vis de l'acceptabilité d'un risque.

D'après les définitions présentées ci-dessus, la notion de sécurité est directement liée aux notions de danger et de risque. Nous appliquons la définition présentée par [Mazouni, 2008] à notre recherche : « *la sécurité est l'absence de danger ou de conditions susceptibles de créer un risque inacceptable* ». L'évaluation de la sécurité doit prendre en compte non seulement le système mais également l'homme et l'environnement dans lequel il évolue. Cette façon de faire a été utilisée dans les travaux de [Hasan, 2002] et [Shahrokhi, 2006] par la prise en compte du concept de Situation de Travail (SdT). La méthode IRAD n'a pas considéré explicitement ce concept de Situation de Travail.

Pour mieux cerner cette notion de sécurité, nous présentons ci-après les notions de Situation de Travail (SdT), de danger et de risque.

Situation de Travail (SdT)

Le concept de SdT intègre les concepts de « système de travail », de « poste de travail » et « d'activité de travail ». La norme [NF EN ISO 6385, 2004] définit la SdT comme : « *un système constitué d'un ou de plusieurs travailleurs et des équipements de travail, agissant ensemble pour accomplir la fonction du système, à l'intérieur de l'espace de travail, dans l'environnement de travail, selon les conditions d'exécution des tâches à effectuer* ». La figure 1.2 montre le concept de l'activité de travail.

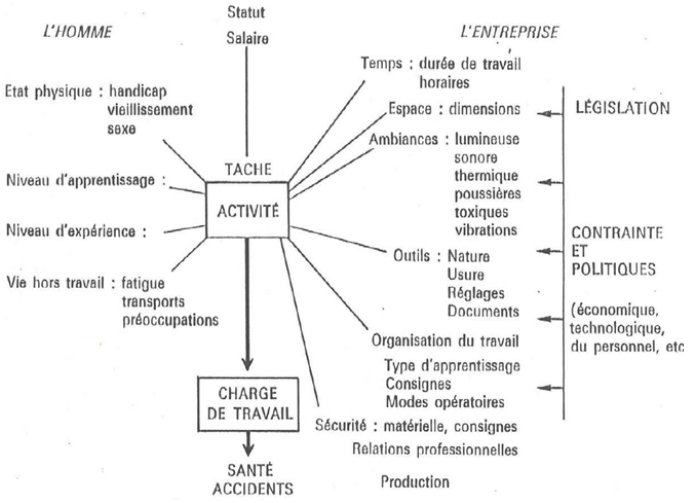
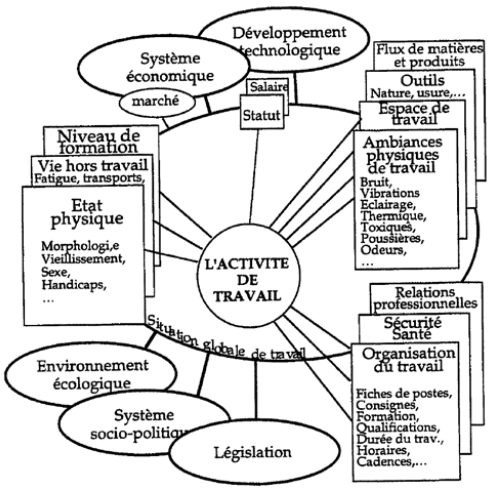


Schéma général des déterminants de l'activité [Laville, 1986] cité dans [Karnas, 2011]



La situation globale de travail et son environnement [Pomian et al., 1997]

Figure 1.2. Activité de Travail.

Les travaux de recherche de [Hasan, 2002] et [Shahrokhi, 2006] sont fondés sur le concept de SdT. [Hasan, 2002], en adoptant les deux notions de situation et de travail, propose de définir la SdT par « *l'existence des relations entre les utilisateurs et la machine (système de production), l'ensemble coopérant pour atteindre une performance donnée dans la réalisation d'une mission bien déterminée* ». Il présente ce concept en montrant les liens entre la SdT et plusieurs entités telles que le système, les risques, les événements dangereux, la tâche, l'équipe de travail, la zone dangereuse ou encore le phénomène dangereux. [Shahrokhi, 2006] adopte la définition proposée par [Licht et al., 2005] : la SdT pour un opérateur est « *un ensemble comprenant l'environnement ambiant de travail et également ses outils et matériaux, ses méthodes de travail, l'organisation de son travail, et les interactions psychologiques et sociologiques* ». [Shahrokhi, 2006] précise que la SdT peut être vue comme « *un système artificiel, socio-technique, dynamique et ouvert* » dont « *les entrées sont des matériaux, de l'énergie, du travail et de l'information* », ses sorties attendues sont « *des produits et des matériaux secondaires* » et ses sorties indésirables « *les pollutions et les conséquences des accidents* ».

Danger

Le deuxième terme lié à la sécurité est la notion de danger, qui peut apparaitre comme le résultat d'un événement indésirable (accident). Selon la directive 2006/42/CE, le danger est « *une source éventuelle de blessure ou d'atteinte à la santé* ». La norme [NF EN ISO 12100, 2010] utilise le terme dommage comme « *blessure physique ou atteinte à la santé* ». Selon cette norme, les éléments entrainant un dommage sont le phénomène dangereux, la situation dangereuse et l'événement dangereux (Voir § 3.2.2). En effet, un dommage est la conséquence d'un accident. Selon [Didelot, 2002], l'accident est « *ce qui expose à un mal*

quelconque qui peut compromettre la sécurité ou l'existence de quelqu'un ou de quelque chose ». Le tableau 1.1 détaille les éléments entrainant un dommage et leur définition selon la norme [NF EN ISO 12100, 2010].

Tableau 1.1. Les éléments entrainant un dommage [NF EN ISO 12100, 2010].

Terme français	**Traduction anglaise**	**Définition**
Phénomènes dangereux	Hazard	source potentielle du dommage
Evénement dangereux	Hazardous event	événement susceptible de causer un dommage
Situation dangereuse	Hazardous situation	situation dans laquelle une personne est exposée à au moins un phénomène dangereux

Risque

Le risque est défini dans la littérature de nombreuses façons différentes. Selon la norme [NF EN ISO 12100, 2010], le risque est la combinaison de la probabilité et de la gravité d'un dommage pouvant survenir dans une situation dangereuse, comme présenté à la figure 1.3.

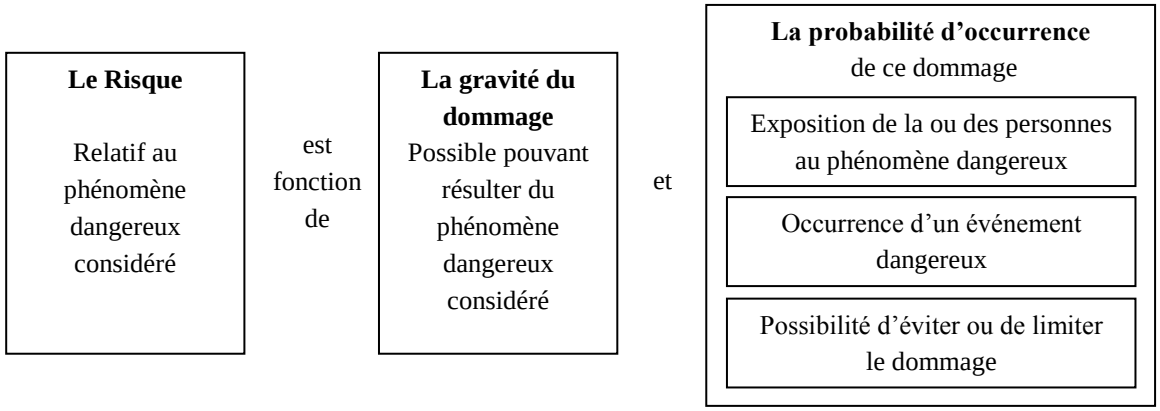


Figure 1.3. Eléments de risque [NF EN ISO 12100, 2010].

Selon [Sienou, 2009 cité dans Mili, 2009], « *la notion de risque est associée à la crainte du danger. Un risque est le résultat d'une exposition potentielle à un phénomène dangereux, qu'il soit de l'ordre de la sécurité des personnes. Le terme de risque désigne aussi bien la cause d'un événement (redouté ou recherché) que sa conséquence éventuelle* ». Aven [Aven, 2009] a listé onze définitions différentes du risque trouvées dans des articles de revue datés de 1976 à 2008 qu'il propose de regrouper en trois catégories :

- Les définitions pour lesquelles le risque est exprimé par des moyennes de probabilité et des valeurs attendues;
- Les définitions pour lesquelles le risque est défini comme un événement ou une conséquence;
- Les définitions pour lesquelles le risque s'exprime à travers des événements / conséquences et des incertitudes.

1.2.3.3. Aide à la décision

De nombreux travaux scientifiques ont pour sujet l'aide à la décision durant le processus de conception. Ces différents travaux ont pour objectif d'aider les concepteurs dans leur démarche de choix. Concevoir un produit, dans notre cas un produit plus sécuritaire, consiste à apporter une ou plusieurs solutions à un ou plusieurs

besoins précédemment explicités. Pour cela, la prise de **décision** pendant les phases de conception, spécialement les premières phases de conception, s'avère une tâche complexe. Pour prendre une décision, il faut faire appel à des **connaissances**. Donc un système d'aide à la décision a pour objectif d'éclairer les décisions prises dans le processus de conception. Un système d'aide à la conception peut alors être vu comme une application d'un système d'aide à la décision, dans lequel la décision portera sur les choix de conception à effectuer. Cette démarche d'aide à la décision doit être soutenue par une **formalisation des connaissances**. Trois notions sont capitales dans le cadre de l'aide à la décision : la connaissance, la formalisation des connaissances et la décision. Ces trois notions sont définies ci-dessous.

Connaissance

D'une manière générale et pratique, la connaissance est définie comme une combinaison d'informations ou d'observations. La classification [Sallaou, 2008] proposée pour les connaissances est : « ***La connaissance explicite*** *qui peut être formulée, écrite, reproduite et redémontrée. Cette connaissance correspond au savoir. Et* ***la connaissance tacite*** *qui n'est pas encore formulée ou non formulable. Elle correspond aux compétences innées ou acquises, le savoir-faire et l'expérience*».

La conception sécuritaire se base sur un ensemble de connaissances sur l'accident lié au système et sur le processus de conception de ce système.

Formalisation des connaissances

La formalisation des connaissances a pour but la modélisation d'un domaine afin de faciliter la gestion et le partage des connaissances. L'Ingénierie des Connaissances (IC) ou Knowledge Engineering (KE) propose des concepts, méthodes et techniques permettant de modéliser, de formaliser et d'acquérir des connaissances (le système expert, l'ontologie, le raisonnement à partir de cas, etc.). En effet, l'ingénierie des connaissances intervient pour définir une aide à l'utilisateur (méthodes, outils logiciels, organisation du travail), modéliser des connaissances (individuelles ou collectives, explicites ou implicites, stabilisées ou évolutives, expertes ou techniques, …) et rendre ces connaissances accessibles sous une forme définie.

Décision

Dans le dictionnaire Larousse, la décision est définie comme un « acte par lequel quelqu'un opte pour une solution, décide quelque chose ; résolution, choix ». [Seguy, 2008], après avoir listé plusieurs définitions de la décision dans les travaux scientifiques, a extrait les points communs suivants : «

- *une décision a pour objectif de résoudre un problème ;*
- *elle doit se concrétiser par une action ;*
- *elle peut être individuelle ou collective et, parfois, distribuée ;*
- *elle peut être construite à partir de solutions existantes partielles parmi lesquelles le décideur choisit une solution pouvant répondre au problème posé* ».

Dans le cadre de la conception sécuritaire d'un système, il faut être capable d'intégrer des connaissances sur la sécurité et sur la conception, mais il faut aussi mettre en place des moyens et outils, pour aider le concepteur dans le choix de la solution sécuritaire. Ces critères pilotent le choix, mais le choix final de la solution reste de la responsabilité du concepteur. Cette démarche d'intégration des connaissances sur l'accident lié au système et sur son processus de conception doit s'appuyer sur des méthodes et outils d'aide à la décision.

1.2.3.4. Synthèse

Dans cette partie, nous avons précisé le contexte, le besoin industriel ainsi que la problématique scientifique de nos travaux de recherche. Nous avons ensuite passé en revue les concepts principaux liés à notre recherche. Ces concepts sont présentés à la figure 1.4.

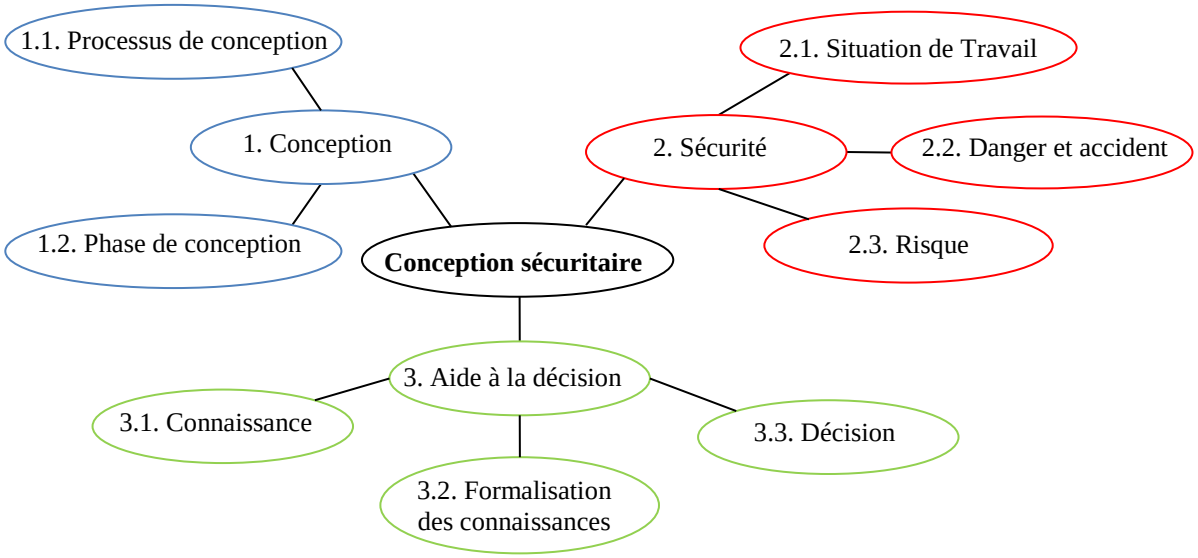


Figure 1.4. Les concepts liés à la conception sécuritaire.

Après avoir cadré ces concepts, nous abordons dans la section suivante, la « conception sécuritaire ».

1.3. Etat de l'art sur la conception sécuritaire

1.3.1. Introduction

L'un des objectifs principaux de cette thèse est d'opérationnaliser la méthode IRAD. Afin d'y arriver, une synthèse des travaux normatifs et scientifiques sur l'intégration de la sécurité en conception est présentée dans cette section. La méthode IRAD y est détaillée et les problèmes et manques à résoudre sont mis en avant. Cette section se termine par une conclusion sur cette notion de conception sécuritaire.

1.3.2. Cadre normatif pour la conception sécuritaire

1.3.2.1. La Directive Machine

La réglementation et notamment le Code du Travail précisent les dispositions applicables aux employeurs de droit privé ainsi qu'à leurs salariés (article L1111-1 du Code du Travail). Certaines de ces dispositions concernent « les exigences essentielles de santé et de sécurité relatives à la conception et à la construction des machines ». Ces exigences sont précisées dans la directive 2006/42/CE dite « Directive Machine » codifiée à l'annexe I de l'article R 4312-1 du Code du Travail. Des normes ont été élaborées dans l'objectif de transcrire cette réglementation de façon à fournir aux concepteurs des éléments (technologies, savoir-faire, …) permettant d'assurer la sécurité des futurs utilisateurs des machines conçues.

La Directive Machine 2006/42/CE s'adresse aux fabricants et aux sociétés mettant en circulation des machines et des composants de sécurité. Elle définit les tâches à exécuter pour respecter les exigences de santé et de sécurité applicables aux machines neuves, afin d'abolir les barrières commerciales au sein de l'Europe et de garantir un niveau élevé de sécurité et de protection de la santé aux utilisateurs et aux opérateurs. Elle s'applique à la construction de machines et de composants de sécurité mis en circulation individuellement, ainsi qu'aux

machines d'occasion et aux appareils provenant de pays tiers mis sur le marché pour la première fois dans l'espace économique européen.

En 1989, le Conseil de l'Union Européenne a promulgué la Directive concernant le rapprochement des législations des États membres relative aux machines, connue sous le nom de Directive Machine (89/392/CEE). En 1995, cette directive devait s'appliquer dans tous les États membres de l'Union Européenne. En 1998, diverses modifications ont été regroupées et consolidées dans la Directive Machine en vigueur (98/37/CE). En 2006, une « Nouvelle Directive Machine » (2006/42/CE) a été promulguée. Elle remplace les versions précédentes et son application est obligatoire dans les États membres de l'UE depuis le 29 décembre 2009.

1.3.2.2. La normalisation liée à la sécurité

Les normes sont des documents établis pour faire « face à des problèmes réels ou potentiels, des dispositions destinées à un usage commun et répété », et « visant à l'obtention du degré optimal d'ordre dans un contexte donné » [NF EN 45020, 2007]. Les normes françaises sont établies par trois instances à trois échelles différentes:

- **Internationales :** ISO (International Standardization Organisation) est un réseau mondial d'organismes de normalisation de 157 pays. L'ISO élabore et publie des normes internationales en se concentrant sur les technologies non électriques.
- **Européennes :** CEN (Comité Européen de Normalisation) est un groupe d'organismes de normalisation des pays membres de l'UE, de l'AELE (Association européenne de libre-échange) ainsi que des futurs membres de l'UE. Le CEN élabore les normes européennes (EN) dans le domaine non électrique. Pour éviter que ces normes présentent des obstacles au commerce, le CEN s'efforce de travailler en étroite collaboration avec l'ISO. Le CEN détermine par un vote si les normes ISO doivent être reprises et les publie comme normes européennes.
- **Françaises** : La normalisation en France est réglementée par la loi du 24 mai 1941 qui a créé l'Association Française de Normalisation (AFNOR) et définit la procédure d'homologation des normes. L'**AFNOR** est l'organisme officiel français de normalisation, membre de l'ISO auprès de laquelle, elle représente la France. L'AFNOR a été créée en 1926 ; elle est placée sous la tutelle du ministère chargé de l'Industrie. Elle compte environ 3 000 entreprises adhérentes.

Les organismes de normalisation (AFNOR, CEN et ISO) catégorisent les normes de sécurité selon trois types [NF EN ISO 12100, 2010] :

- Les normes de **type A** précisent des notions fondamentales de sécurité, des principes de conception et des aspects généraux valables pour tout type de machines.
- Les normes de **type B** traitent un aspect de la sécurité ou un type de dispositif conditionnant la sécurité. Elles sont valables pour une large gamme de machines.
    - Les normes de **type B1** traitent des aspects particuliers de la sécurité (par exemple distances de sécurité, température superficielle, bruit) ;
    - Les normes de **type B2** traitent de dispositifs conditionnant la sécurité (par exemple commandes biannuelles, dispositifs de verrouillage, dispositifs sensibles à la pression, protecteurs).
- Les normes de **type C** indiquent des prescriptions de sécurité détaillées s'appliquant à une machine particulière ou à un groupe de machines.

Nous avons résumé ces trois types de normes de sécurité dans le tableau 1.2.

Tableau 1.2. Les trois types (A, B et C) de normes de sécurité.

<table>
<tr><th></th><th>Type A</th><th colspan="2">Type B</th><th>Type C</th></tr>
<tr><td>Concept général</td><td>Norme fondamentales de sécurité</td><td colspan="2">Norme génériques de sécurité</td><td>Norme de sécurité par catégorie de machines</td></tr>
<tr><td>Mots clés</td><td>Sécurité, Risque, Conception, Machine, Exigences</td><td colspan="2">Sécurité, Dispositif, Gamme de machine</td><td>Sécurité détaillée, Exigences de sécurité, Machine particulière</td></tr>
<tr><td rowspan="3">Définit</td><td rowspan="3">- des notions fondamentales de sécurité
- des principes de conception
- des aspects généraux</td><td colspan="2">- un aspect de la sécurité ou
- un type de dispositif conditionnant de la sécurité</td><td rowspan="3">- des prescriptions de sécurité détaillées
- des exigences de sécurité pour une machine particulière</td></tr>
<tr><td>Type B1</td><td>Type B2</td></tr>
<tr><td>Aspects particuliers de la sécurité</td><td>Dispositifs conditionnant la sécurité / moyens de protection</td></tr>
<tr><td>S'appliquent à</td><td>Tous types de machines</td><td>Une large gamme de machines</td><td>Une large gamme de machines</td><td>Une machine particulière ou à un groupe de machines</td></tr>
<tr><td>Normes</td><td>NF EN ISO 12100, 2010</td><td>ISO13857, 2008
ISO14738, 2002
etc.</td><td>ISO13850, 2006
ISO 4414, 2010
etc.</td><td>ISO 4254-1, 2013
NF EN 690, 2013
etc.</td></tr>
</table>

1.3.2.3. Prise en compte de la sécurité en conception dans les normes

Dans cette partie, nous nous focalisons sur la stratégie d'appréciation et de réduction du risque dans les normes de type A. Les normes relatives à ce sujet sont au nombre de deux. La norme [NF EN ISO 12100, 2010] donne les principes généraux de conception d'une application de sécurité. Elle propose un processus d'appréciation des risques destiné à déterminer les mesures à mettre en place pour leur réduction. Le rapport technique [ISO/TR 14121-2, 2008] guide les concepteurs pour la réalisation de l'appréciation du risque. Elle n'aborde pas le sujet des mesures de réduction des risques. Selon ces normes, afin d'apprécier et de réduire le risque, le concepteur doit accomplir les actions suivantes :

Phase d'appréciation du risque. L'appréciation des risques est réalisée suivant quatre étapes:

1. **Déterminer les limites de la machine.** L'appréciation du risque commence par la détermination des limites de la machine relatives à son utilisation, à l'espace disponible, au temps imparti et à d'autres limites (nettoyage, conditions environnementales, …).
2. **Identifier les phénomènes dangereux et les situations dangereuses qui leur sont liées.** L'objectif de l'identification des phénomènes dangereux est la création d'une liste des phénomènes dangereux, des situations dangereuses et des événements dangereux permettant ensuite de décrire l'ensemble des scénarios possibles pour lesquels une situation dangereuse peut causer un dommage.
3. **Estimer le risque pour chacun des phénomènes dangereux et situations dangereuses identifiés.** Cette estimation du risque consiste à évaluer les deux éléments constitutifs du risque, à savoir la gravité du dommage et la probabilité d'occurrence de ce dommage.

4. **Evaluer le risque et prendre des décisions quant à la nécessité de le réduire.** Il convient ici de choisir quelle situation dangereuse nécessite une réduction du risque et de déterminer si la réduction du risque requise a été effectuée sans introduction de phénomènes dangereux supplémentaires ou sans augmentation des autres risques.

Phase de réduction de risque. Dans la norme la phase de réduction du risque est obtenue en mettant en place des mesures de protection. Elle est constituée de huit étapes précisées par ordre d'efficacité ci-après. Les deux premières étapes concernent la conception de la machine. Il s'agit de l'élimination des phénomènes dangereux par conception et de la réduction des risques par conception. Les troisième et quatrième étapes concernent les dispositifs et les mesures de protection complémentaires. Les quatre dernières étapes sont l'information sur l'utilisation, la formation des utilisateurs, la mise à disposition d'équipements de protection individuelle et enfin la rédaction de procédures de fonctionnement normal de la machine. Les huit étapes pour la réduction des risques sont :

1. Eliminer les phénomènes dangereux par conception ;
2. Réduire le risque par conception;
3. Définir des dispositifs de protection;
4. Proposer des mesures de protection complémentaires ;
5. Informer sur l'utilisation ;
6. Former à l'utilisation;
7. Définir des équipements de protection individuelle ;
8. Décrire les procédures de fonctionnement normal.

L'objectif, dans notre cas, est d'éliminer ou de réduire les risques par conception. Il s'agit donc de mettre en œuvre les deux premières étapes du processus de réduction du risque. Les mesures de protection visant à réduire le risque par conception sont citées dans le chapitre 5 par ordre d'efficacité.

1.3.2.4. Conclusion et discussion sur les normes de sécurité

L'approche globale de la prise en compte de la sécurité dans la phase de conception est définie par les normes de type A et B1. Les normes de type A précisent la démarche permettant d'identifier les mesures de réduction du risque à partir des spécifications fonctionnelles du système. Les normes de types B1 prescrivent des outils et méthodes pour la réalisation de ces mesures.

La norme [NF EN ISO 12100, 2010] et le rapport technique [FD ISO/TR 14121-2, 2008] proposent des démarches structurées permettant d'apprécier et de réduire les risques identifiés. Cependant, elles restent générales et laissent la responsabilité aux concepteurs quant à la manière de réaliser cette démarche. Un de nos objectifs est de combler ce manque.

1.3.3. Travaux scientifiques sur la conception sécuritaire

Cette section porte sur la prise en compte de la sécurité dans la conception de produits dans les travaux scientifiques. Elle est structurée en deux parties suivant que les travaux étudiés portent sur une approche globale de la sécurité ou sur une approche basée sur le processus de conception.

1.3.3.1. Approche globale sécuritaire

D'un point de vue général, les modes d'intégration de la sécurité, dans les processus de conception s'effectuent suivant deux voies [De La Garza, 2005]:

1. **Intégration de la sécurité par voies « directes » :** Les voies dites "directes" sont des modes d'intégration explicites de la sécurité. Elles sont basées sur des normes, guides

ou autres documents officiels. Elles constituent des référentiels communs facilitant le dialogue et la coopération entre les acteurs de la conception.

2. **Intégration de la sécurité par voies « indirectes » :** Les voies dites "indirectes" sont des modes d'intégration implicites. Ces connaissances sont fondées sur le retour d'expérience des différents acteurs sur la situation d'exploitation (exigences et contraintes du travail réel, retours du terrain et d'accidents).

L'intégration de la sécurité par voies directes « *implique le partage d'un « référentiel opératif commun » en relation avec un système collectif de connaissances, mais un seul expert sécurité en est responsable* ». Celle par voies indirectes « *implique des connaissances sur le travail réel, ses exigences et contraintes et/ou des retours du terrain ou d'accidents. Elles sont liées à un système individuel de connaissances* ». De La Garza [De La Garza, 2005] proposent quatre axes principaux afin d'améliorer la prise en compte de la sécurité lors de la conception :

a. **Aller au-delà du savoir technique** : Les exigences réelles du travail, des dysfonctionnements, des usages et des modes opératoires, l'utilisation de données anthropométriques sont autant de paramètres à prendre en compte pour l'intégration de la sécurité des humains dans un projet de conception [Fadier et al., 2003]. IRAD applique cette directive dans la définition de son processus de risque en prenant en compte l'interaction entre l'humain et la machine. Il est possible d'aller au-delà en considérant le retour d'expérience sur les accidents en phase d'utilisation ainsi que les normes de sécurité. C'est un des objectifs des travaux présentés ici.

b. **Favoriser la conception participative** : Cet axe exprime le fait que la conception participative et le dialogue doivent être encouragés, avec, la mise en place de réunions de conception spécifiques « sécurité » et la participation d'experts différents à des stades particuliers de la conception [De La Garza, 2005]. IRAD ne propose rien allant dans ce sens. Cet aspect ne sera pas traité dans cette thèse.

c. **Enrichir les phases de la conception en introduisant des objectifs de sécurité** : Des objectifs santé-sécurité doivent être intégrés dans les cahiers des charges au même titre que les performances et les spécifications techniques [De La Garza, 2005]. IRAD propose de définir les exigences de sécurité à intégrer à chaque phase de la conception. Cependant, elle ne définit pas comment réaliser cela pratiquement. Nous devons résoudre ce problème.

d. **Intégrer la sécurité portée par l'organisation des REXs** : Le Retour d'EXpérience (REX) reste actuellement pauvre et non formel, en particulier par rapport à la sécurité et à l'usage des équipements industriels [De La Garza et Fadier, 2007]. Le premier cas d'emploi d'IRAD essaye d'aller dans ce sens en proposant de définir les objectifs de sécurité à travers l'analyse du REX. Cependant, elle ne propose pas de formalisation pour le REX. Il convient de résoudre ce problème.

1.3.3.2. Approche basée sur le processus de conception

Des travaux de recherche ont été réalisés sur la sécurité du point de vue des méthodes et théories de la conception des produits. Les chercheurs y ont proposé de nouvelles approches pour améliorer la sécurité des équipements à travers la conception.

[Hasan et al., 2004] ont présenté les résultats d'une analyse du processus de conception employée dans une société de design et proposent une manière d'intégrer la sécurité dans le processus de conception. Ils décrivent un modèle basé sur la notion de situation de travail et sur les éléments qui caractérisent cette situation ; leur objectif étant de proposer un outil

d'aide aux concepteurs pour la prise en compte des exigences de sécurité dans le processus de conception.

Ce modèle n'intègre pas les méthodes de conception largement connues par les concepteurs et utilisées dans la majorité des bureaux d'étude. L'objectif de nos travaux étant d'aider les concepteurs dans leurs choix, nous prenons le parti de nous baser sur les méthodes et théories de conception (approche systématique, analyse fonctionnelle, conception axiomatique) le plus souvent déjà connues par les concepteurs.

[Shahrokhi, 2006] s'est également basé sur la notion de situation de travail. L'objectif de son travail était de définir des modèles d'humains pour leur prise en compte dans les situations de travail durant les phases de conception des systèmes industriels. Pour cela, il a proposé une approche pour définir les zones dangereuses des situations de travail dans un environnement virtuel ou augmenté. La critique principale de ce travail est la même que celle relative aux travaux de Hasan. A savoir la proposition de Shahrokhi n'intègre pas les méthodes de conception largement connues par les concepteurs et utilisées dans la majorité des bureaux d'étude.

[Houssin et Coulibaly, 2011][1] ont proposé une approche afin d'améliorer la performance du produit dans les situations d'utilisation. L'approche proposée est basée sur 4 étapes: (1) l'intégration systémique de la sécurité par l'utilisation d'un modèle de situation de travail; (2) la prise en compte des exigences des directives et des normes de sécurité ; (3) l'identification de la contradiction résultant du choix du concepteur ; (4) la résolution de ces contradictions en utilisant des méthodes adaptées comme TRIZ.

Ces travaux montrent la possibilité d'utiliser les fonctionnalités et les principes de la méthode TRIZ. TRIZ permet de résoudre des problèmes d'organisation en revenant à l'origine du problème du système technique. Ainsi, dans l'objectif d'adapter TRIZ aux objectifs de la sécurité, [Hasan et al., 2004] ont développé et utilisé une approche pour la formalisation des problèmes de sécurité comme un point d'entrée dans TRIZ. La sécurité y est considérée comme un paramètre en opposition à la productivité.

[Marsot, 2005] utilise le Quality Function Deployment dans la conception d'un couteau ergonomique. Il part d'une liste d'exigences de sécurité et techniques et montre leur corrélation avec les solutions techniques par l'utilisation de la matrice du QFD. La définition des exigences ergonomiques provient de l'analyse de l'activité des utilisateurs. Cette approche consiste en une analyse de la conception détaillée par rapport aux objectifs initiaux.

De nombreux travaux ont également été réalisés à partir de la mise en œuvre de la méthode de conception axiomatique pour l'analyse du produit du point de vue ergonomique. En se basant sur la matrice de conception, [Lo et Helander. 2007 ; Helander, 2007] ont développé la méthodologie DESA (acronyme anglais pour Equation de Conception pour l'Analyse des Systèmes). Cette méthodologie permet d'étudier les systèmes homme-machine par leur modélisation des points de vue fonctionnels et structurels. Elle est basée sur quatre domaines : objectifs utilisateurs, exigences fonctionnelles, paramètres de conception et actions des utilisateurs. Cette méthodologie décrit les règles d'une conception utilisable et ne prend en considération que l'étude de l'action humaine pour atteindre certains objectifs. Elle consiste en une analyse globale de la solution des points de vue conception et utilisation.

Le tableau 1.3 présente un ensemble de thèses effectuées dans le domaine de la santé et de la sécurité au travail et celui de l'intégration de la sécurité en conception. Une synthèse sur ces travaux de thèses montre qu'il n'existe pas :

[1] Rémy Houssin et Raid Hasan sont une même personne

- d'approche définie permettant la formalisation des connaissances liées à l'intégration de la sécurité dans le processus de conception (hormis dans la thèse de Rima Ghemraoui) ;
- d'approche définie afin de mesurer la sécurité tout au long du processus de conception ;
- d'approche définie pour aider à choisir les solutions sécuritaires optimales.

Tableau 1.3. Thèses effectuées dans le domaine de l'intégration de la sécurité en conception.

Année	Par	Titre de thèse	Lieu
1995	Abord de Chatillon, E.	Accident du travail et gestion de la sécurité - Représentation des acteurs et efficacité des outils.	Chambéry
1999	Damien Jouffroy	Vers une démarche d'intégration de la sécurité à la conception des machines à bois semi-automatisées. Application au développement d'un système de captage des poussières pour défonceuse à commande numérique	Université Henri Poincaré, Nancy I
2000	Jean-Christophe Blaise	Apport d'une modélisation de l'information normative à l'intégration des règles de sécurité des machines en conception	Université Henri Poincaré, Nancy I
2002	Armelle Didelot	Contribution à l'identification et au contrôle des risques dans le processus de conception	ENGSI, Université de Nancy
2002	Raid Hasan	Contribution à l'amélioration des performances des systèmes complexes par la prise en compte des aspects socio techniques dès la conception : proposition d'un modèle original de situation de travail pour une nouvelle approche de conception	CRAN, Université de Lorraine
2006	Mahmoud Shahrokhi	Intégration d'un modèle de situation de travail pour l'aide à la formation et à la simulation lors de la conception et l'industrialisation de systèmes	IRCCyN, Ecole Centrale Nantes
2007	Julien Cambon	Vers une nouvelle méthodologie de mesure de la performance des systèmes de management de la santé-sécurité au travail	Ecole des Mines de Paris
2009	Rima Ghemraoui	Méthodologie de conception innovante intégrant la sécurité des utilisateurs : application aux liaisons tracteur-outils	LURPA, ENS Cachan, ParisSud
2012	Huichao Sun	L'amélioration de la performance du produit par l'intégration des taches d'utilisation dès la phase de conception : une approche de conception comportementale	LGéCo, INSA de Strasbourg
2012	Frédéric Juglaret	Indicateurs et Tableaux de Bord pour la prévention des risques en Santé-Sécurité au Travail	CRC, Mines-ParisTech

1.3.3.3. Conclusion et discussion sur les travaux scientifiques

Chacune des méthodes que nous venons de citer répond à un objectif de recherche très précis. Elles ne permettent pas une modélisation des ressources immatérielles intégrant les aspects quantitatifs et qualitatifs nécessaires pour avoir une vision complète de ces ressources et pouvoir les traiter convenablement. De plus, elles s'intéressent essentiellement aux connaissances, sans toujours prendre en compte les dimensions compétences, savoir-faire ou savoir-être. Citons les travaux de Hasan [Hasan, 2002] qui montrent toute la difficulté à exprimer et à récupérer les ressources détenues par des acteurs mais ne s'attardent pas sur les techniques de formalisation utilisées pour ces ressources. Notre travail de recherche s'inscrit dans cette deuxième catégorie de solution.

Les trois principaux domaines de notre recherche sont la conception, la sécurité et l'aide à la décision. L'état de l'art montre, qu'hormis la méthode IRAD, il n'existe

pas d'approche permettant la formalisation des connaissances liées à l'intégration de la sécurité dans le processus de conception. Il n'existe aucune approche permettant de mesurer la sécurité tout au long du processus de conception et qu'il n'existe pas d'approche permettant d'aider à choisir les solutions sécuritaires.

A la vue des travaux présentés ci-dessus et à notre connaissance, l'approche systémique proposée par Rima Ghemraoui [Ghemraoui, 2009] est la seule permettant la formalisation et l'intégration de la sécurité dès le début et tout au long du processus de conception. Cette méthode détaillée dans la section suivante répond au cahier des charges que nous nous sommes fixés. Elle sera donc la base de nos travaux méthodologiques.

1.3.4. La méthode IRAD

Cette présentation va nous permettre d'énoncer les problématiques scientifiques de nos travaux de recherche. Ghemraoui R. [Ghemraoui, 2009], dans le cadre de sa thèse, a élaboré une méthode pour l'intégration structurée de la sécurité des utilisateurs dans les phases amont de la conception. La méthode IRAD (Innovative Risk Assessment Design) est une méthode d'intégration de la santé-sécurité à la conception des produits.

Cette section est organisée en trois parties. La première partie concerne la description de la structure de la méthode IRAD. Cette partie présente le modèle d'intégration de la sécurité au plus tôt en phase de conception du produit. La deuxième partie introduit l'utilisation d'IRAD par la présentation de ses trois cas d'emploi. Enfin, cette partie se *conclut* par la présentation des avantages et inconvénients d'IRAD et liste les problèmes de mise en œuvre de la méthode que nous proposons de résoudre.

1.3.4.1. Structure de la méthode IRAD

Modèle d'intégration de la sécurité en conception. IRAD repose sur un modèle d'intégration de la sécurité au plus tôt en phase de conception du produit (figure 1.5). Ce modèle est basé sur les méthodes de conception systématique [Pahl et Betz, 2007] et axiomatique [Suh, 1990]. Il explique la relation entre le processus de conception et un processus du risque.

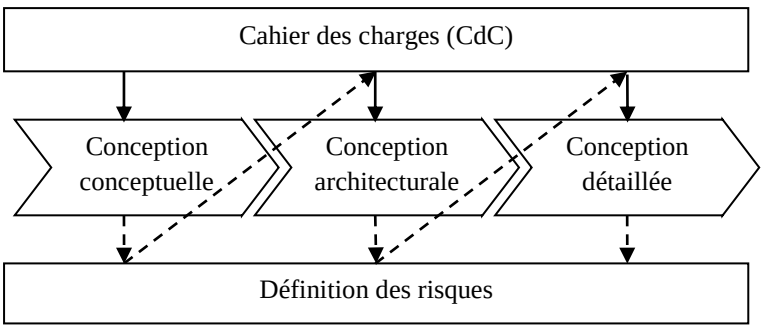


Figure 1.5. Modèle d'intégration de la sécurité au plus tôt en phase de conception du produit [Ghemraoui, 2009].

Dans ce modèle, la définition des risques est effectuée à chaque étape du processus de conception et la spécification des exigences (Cahier des Charges : CdC) est mise à jour après chaque étape de la conception. Cette définition des risques et l'élaboration des exigences de sécurité correspondent à ce que nous appelons le « processus du risque ».

Selon ce modèle, l'intégration de la sécurité au plus tôt dans la conception des produits consiste à : (1) identifier les risques à travers l'analyse des choix technologiques et du retour d'expérience ; (2) traduire ces risques en exigences de sécurité ; et (3) prendre en considération ces exigences systématiquement dans la synthèse de nouvelles solutions au même titre que les exigences techniques.

Processus de conception de la méthode IRAD. Selon l'approche systématique décrite par Pahl et Beitz [Pahl et Beitz, 2007], le processus de conception est constitué de 4 phases : la clarification et la planification des tâches (définition du besoin), la conception conceptuelle (définition des principes), la conception architecturale (définition de la structure globale) et la conception détaillée (définition des plans). Les trois dernières phases citées sont considérées dans l'analyse des risques. Selon Suh [Suh, 1990], le processus de conception est un cheminement itératif et séquentiel entre 4 espaces : le domaine client, le domaine fonctionnel, le domaine physique et le domaine du processus. Il considère que la conception consiste en un processus de mappage entre ces différents domaines. Ce mappage décrit la transition d'un domaine à un autre. L'Extended Axiomatic Design (EAD) décrit par Ge, Lu et Suh [Ge et al., 2002] montre la relation entre la conception axiomatique et la conception systématique.

A partir de ces considérations [Ghemraoui et al., 2009] ont proposé la méthode IRAD mettant en parallèle les deux processus de conception et du risque. Le processus de conception y est constitué de six phases (figure 1.6). Le processus de conception proposé s'inspire de cette méthode dont elle ne reprend que les domaines fonctionnel et physique de la conception axiomatique (AD). Dans le cas de la conception d'une machine, le domaine fonctionnel correspond aux exigences techniques et le domaine physique aux solutions techniques. Ce processus est constitué de six phases :

- La **phase P1** fait le lien entre la conception conceptuelle et le domaine fonctionnel. Elle permet de définir les exigences de conceptualisation;
- La **phase P2** fait le lien entre la conception conceptuelle et le domaine physique. Elle permet de définir les principes de solutions;
- La **phase P3** fait le lien entre la conception architecturale et le domaine fonctionnel. Elle permet de définir les exigences de structuration de la solution;
- La **phase P4** fait le lien entre la conception architecturale et le domaine physique. Elle permet de définir les structures de la solution;
- La **phase P5** fait le lien entre la conception détaillée et le domaine fonctionnel. Elle permet de définir les exigences de finition de la solution;
- La **phase P6** fait le lien entre la conception détaillée et le domaine physique. Elle permet de définir les détails de la solution.

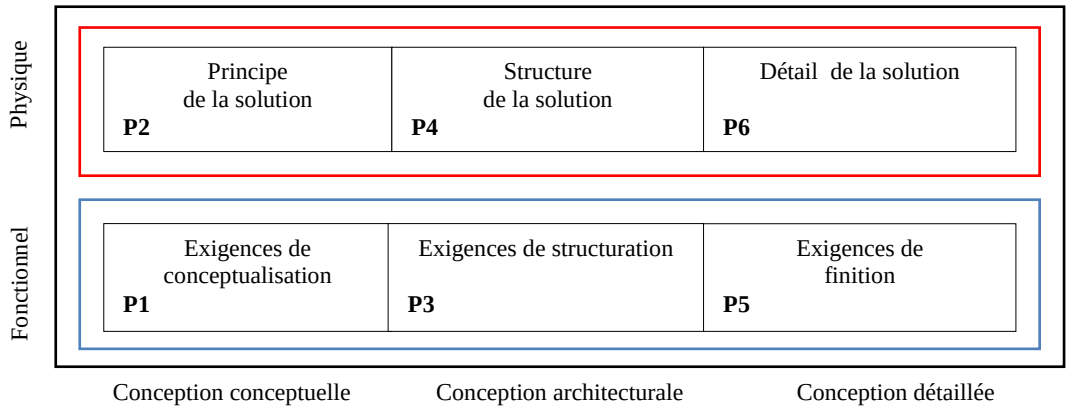


Figure 1.6. Processus de conception de la méthode IRAD.

Processus du risque de la méthode IRAD . A partir des considérations sur l'approche systématique et l'approche axiomatique détaillées précédemment, [Ghemraoui et al., 2009] ont proposé la méthode IRAD mettant en parallèle les deux processus de conception et du risque. Le processus du risque est similairement divisé en six contextes (figure 1.7).

Celui-ci correspond à la description des risques issus de l'interaction de l'homme avec les résultats de la conception à chacune des étapes de celle-ci (conceptuelle, architecturale et détaillée). Les six contextes de processus du risque sont :

- Le **contexte C1** qui correspond au mappage entre les risques relatifs à la conception conceptuelle et le domaine fonctionnel. Il permet de définir les exigences de sécurité au niveau conceptuel ;
- Le **contexte C2** qui correspond au mappage entre les risques relatifs à la conception conceptuelle et le domaine physique. Il permet de définir les risques d'accidents;
- Le **contexte C3** qui correspond au mappage entre les risques relatifs à la conception architecturale et le domaine fonctionnel. Il permet de définir les exigences de sécurité au niveau architectural;
- Le **contexte C4** qui correspond au mappage entre les risques relatifs à la conception architecturale et le domaine physique. Il permet de définir les risques anthropométriques et de non fiabilité technique;
- Le **contexte C5** qui correspond au mappage entre les risques relatifs à la conception détaillée et le domaine fonctionnel. Il permet de définir les exigences de sécurité au niveau de la conception détaillée;
- Le **contexte C6** qui correspond au mappage entre les risques relatifs à la conception détaillée et le domaine physique. Il permet de définir les risques d'usage.

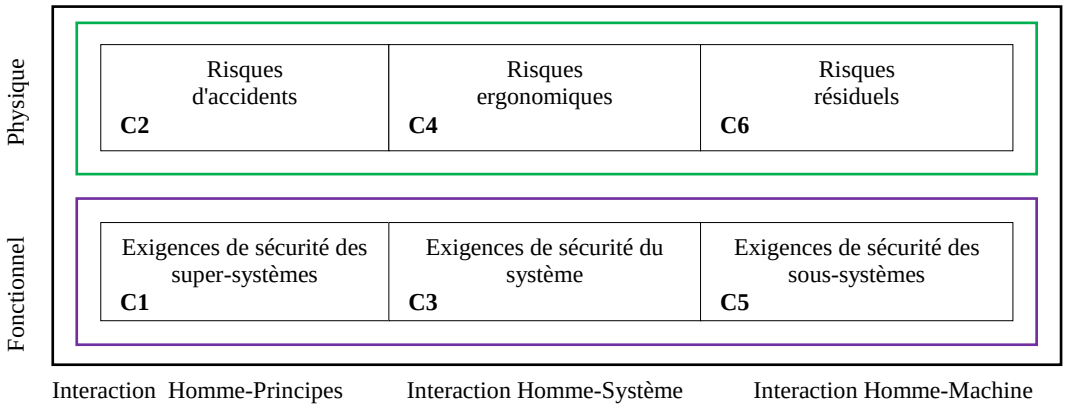


Figure 1.7. Processus du risque de la méthode IRAD.

La méthode IRAD exprime la relation entre un processus de conception et un processus de risque détaillée ci-dessus. Ainsi à chaque phase du processus de conception correspond un contexte du processus du risque. Chaque contrainte de sécurité est ainsi intégrée au plus tôt dans le processus de conception.

Cette méthode est régie par 3 principes: (1) Définir les objectifs de la conception des points de vue technique et de sécurité; (2) Conserver l'indépendance des exigences fonctionnelles techniques et de sécurité; (3) Minimiser l'incompatibilité entre les caractéristiques humaines et les paramètres de la conception.

1.3.4.2. Mise en œuvre de la méthode IRAD

Cas d'emploi 1 d'IRAD. Le premier cas d'emploi de la méthode IRAD décrit la formalisation structurée du Retour d'EXpérience (REX). Ce cas permet d'élaborer des exigences de sécurité à partir du retour d'expérience (figure 1.8). Dans un premier temps, les rapports d'accidents et d'incidents, la réglementation, les normes, les données relatives à l'utilisation réelles de la machine et l'étude de solutions existantes sont utilisées afin de générer un arbre des causes. Celui-ci permet de mettre en avant les éléments ayant entrainé l'incident, l'accident ou la dérive comportementale de l'utilisateur.

Une Analyse Fonctionnelle est également réalisée. Elle permet de définir les fonctions auxquelles doit répondre la machine ainsi que les contraintes dues à l'environnement dans lequel la machine est utilisée. La confrontation des résultats de cette analyse avec les résultats de l'application de la méthode de l'arbre des causes demande ensuite de catégoriser les contraintes de sécurité définie en fonction de la phase de conception impliquée. On obtient ainsi des contraintes de sécurité plus facilement intégrable en phase de conception ou de reconception d'une machine.

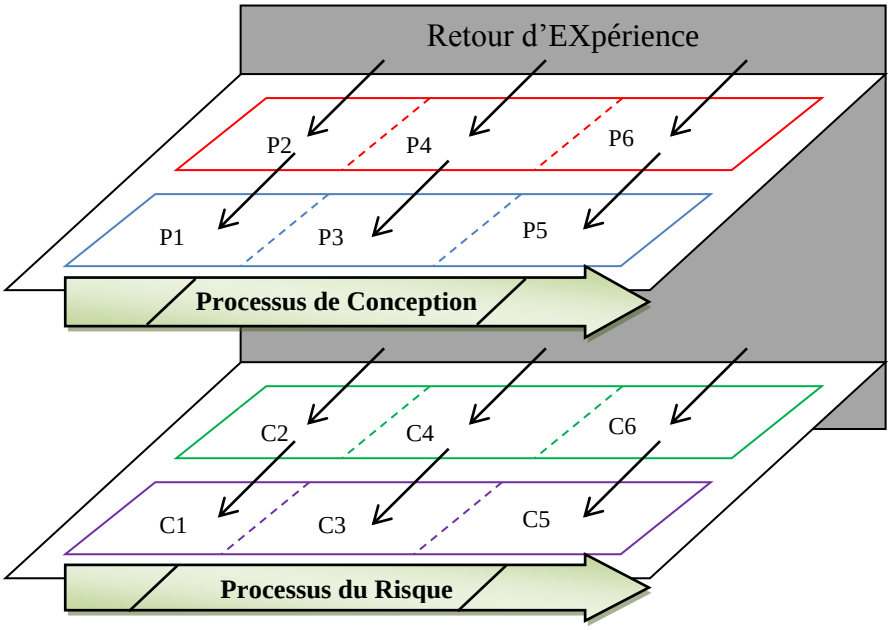


Figure 1.8. Cas d'emploi 1 pour l'expression des exigences de sécurité à travers l'analyse du REX.

Cas d'emploi 2 d'IRAD. Le cas d'emploi 2 permet d'analyser la solution technique pour l'expression des exigences de sécurité. Ce cas débute par l'analyse du REX et de solutions existantes. Il convient ensuite de déterminer si la conception est une conception couplée ou découplée par l'utilisation de la matrice de conception (figure 1.9). Le cas d'emploi 2 évalue chaque phase du processus de conception (conception conceptuelle, architecturale et détaillée) pas à pas et analyse les risques dans chacune de ces phases. En effet, ce cas montre comment détecter les problèmes de sécurité au plus tôt de la conception grâce à la décomposition fonctionnelle de la solution existante. Enfin ce cas permet d'exprimer les exigences de sécurité pour chaque phase de conception.

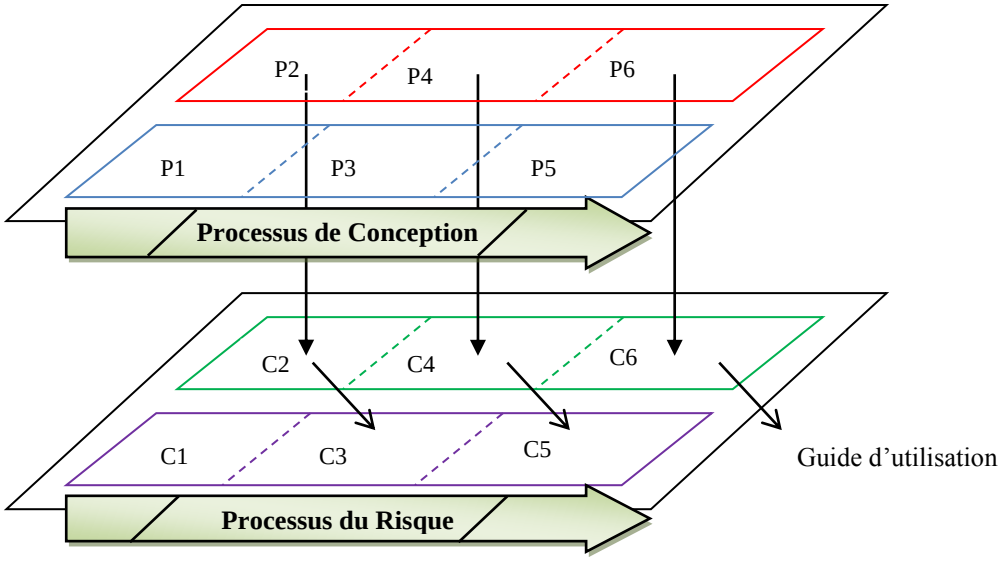


Figure 1.9. Cas d'emploi 2 pour l'expression des exigences de sécurité à travers l'analyse des choix techniques.

Cas d'emploi 3 d'IRAD. Dans la méthode IRAD, les exigences fonctionnelles sont composées d'exigences techniques et de sécurité. La figure 1.10 montre le schéma des opérations de synthèse à la base des exigences techniques et de sécurité définies. La synthèse des solutions à partir des exigences techniques et de sécurité permettra à la sécurité de faire partie intégrante de la solution technique. L'opération de synthèse peut consister à générer de nouvelles solutions ou à découpler les exigences techniques d'une conception.

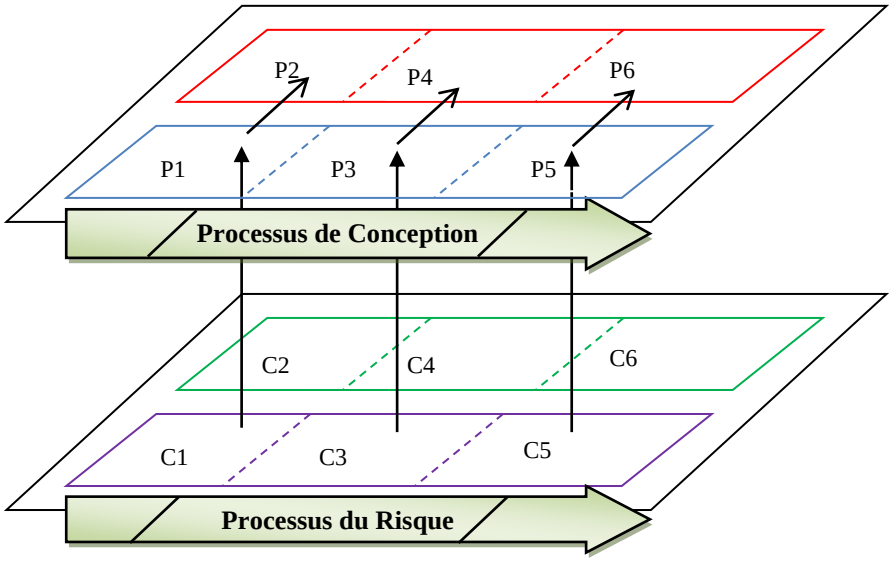


Figure 1.10. Cas d'emploi 3 pour la synthèse de solutions sécuritaires.

1.3.4.3. Conclusion sur la méthode IRAD

Dans cette section, nous avons présenté la méthode IRAD, une méthode de conception pour l'intégration de la sécurité dans le processus de conception. Elle vise à expliquer la relation entre les deux processus de conception et du risque en proposant trois cas d'emploi : (1) l'expression des exigences de sécurité à travers l'analyse du REX.; (2) l'expression des exigences de sécurité à travers l'analyse des choix techniques; (3) la synthèse de solutions sécuritaires.

Cette méthode est la seule méthode qui propose un cadre méthodologique permettant la formalisation et l'intégration de la sécurité dès le début et tout au long du processus de conception. Mais il y a des manques et des points à améliorer dans cette méthode :

- Elle propose d'analyser le REX pour identifier les risques et définir les exigences de sécurité relatives, mais ne propose pas de solution formelle d'extraction et d'utilisation des connaissances issues du REX ;
- Elle propose de définir les risques suivant les trois contextes selon les phases de conception, mais ne précise pas comment définir les risques ;
- Elle propose de définir les exigences de sécurité pour un risque donné, mais ne guide pas le concepteur pour définir ces exigences de sécurité ;
- Elle ne propose pas de solution pour évaluer le niveau de sécurité d'un système tout au long de la conception.

Cette méthode est donc difficilement utilisable en l'état par les concepteurs de machines. En particulier, elle nécessite des approfondissements et des outils afin de la rendre opérationnelle.

1.3.5. Synthèse

Nous avons positionné nos travaux de recherche dans le domaine de la conception sécuritaire. Comme présenté à la figure 1.3, les trois principaux domaines de notre recherche sont la conception, la sécurité et l'aide à la décision. La question posé est : **Comment pouvons-nous opérationnaliser la méthode IRAD ?**

Répondre à cette question amène à se poser les sous-questions suivantes:

1. *Comment formaliser le REX en lien avec les problèmes de sécurité ?*
2. *Comment extraire les connaissances d'un accident ?*
3. *Comment extraire les connaissances de la conception d'un système ?*
4. *Comment ventiler les risques selon les phases du processus de conception ?*
5. *Comment mesurer le niveau de sécurité d'un système ?*
6. *Comment transcrire de manière formelle et systématique les risques en exigences de sécurité ?*
7. *Comment intégrer ces exigences de sécurité dans le processus de conception ?*
8. *Comment formuler des connaissances, des données et des contraintes relatives à la sécurité pour aider aux choix faits lors de la conception?*
9. *Comment faire pour que la méthode IRAD soit facile à utiliser par les concepteurs, les bureaux d'études, les équipes de R & D, les fabricants, ...?*

Répondre à ces questions demande de (figure 1.11):

1. Structurer une démarche concrétisant l'intégration de la sécurité dans les phases de conception ;
2. Trouver un formalisme permettant de représenter les connaissances faisant le lien entre sécurité et phases de conception ;
3. Architecturer un outil expérimental support de la démarche et exploitant le formalisme proposé.

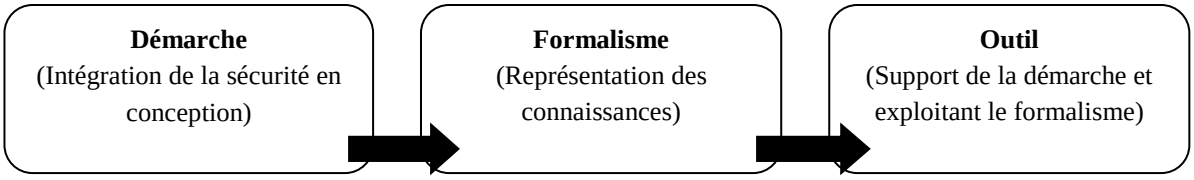


Figure 1.11. Principaux objectifs de la recherche.

1.4. Construction d'un cadre méthodologique pour la conception sécuritaire

1.4.1. Opérationnalisation d'IRAD

L'objectif, ici, est de répondre aux questions posées dans la section précédente. Afin d'y parvenir, nous proposons un modèle d'activités, un processus, afin d'analyser la dimension connaissance de cette opérationnalisation. La vue globale d'un processus de conception sécuritaire est présentée à la figure 1.12 sous la forme d'un diagramme IDEF0. Ce diagramme permet de décrire un processus, ses entrées, sorties, ses contrôles (règles, instruction ou procédure) et ses mécanismes. Ce diagramme traduit le fait que l'on souhaite concevoir un système avec un niveau de sécurité optimal, en se basant sur une description du besoin, en prenant en compte les normes, le REX, les documents techniques et les solutions existantes. L'idée est de produire un système sécuritaire au moyen de méthodes, théories et outils de conception, mais aussi des méthodes et outils de l'analyse des risques ainsi que des outils d'aide à la décision.

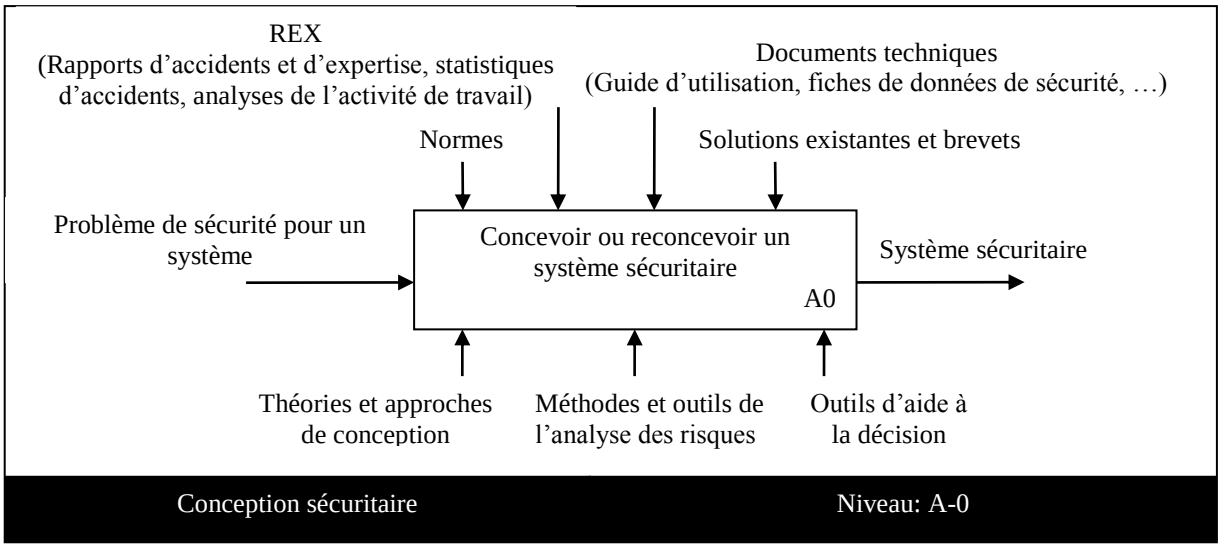


Figure 1.12. Diagramme IDEF0 niveau A-0 du processus de conception sécuritaire.

Pour **opérationnaliser le cas d'emploi 1 d'IRAD**, il faut répondre aux questions de 1 à 6 posées dans le §1.3.5.

Pour la question 1 : Nous proposons de formaliser un type de REX en définissant une structure type de rapport d'accident.

Pour les questions 2 et 3 : Nous proposons d'extraire, à la fois, les connaissances sur l'accident et sur la conception du système impliqué.

Pour les questions 4 et 5 : Nous proposons d'évaluer, de ventiler les risques et de calculer le niveau de sécurité du système. L'ingénierie inverse est assez communément utilisée pour obtenir un retour d'informations sur la conception et la connaissance sur un système existant [Urbanic et al., 2008; Tang et al, 2010]. Dans le but de l'intégration de la sécurité dans le processus de conception, il est nécessaire d'obtenir les connaissances originales intrinsèques qui se trouvent dans le modèle de fonctionnement du système existant.

Cependant, jusqu'à aujourd'hui, la majorité des recherches en Reverse Engineering (RE) est axée sur les aspects liés à la géométrie et à la structure de la conception plutôt que sur les aspects fonctionnels de la conception [Urbanic et al., 2008; Tang et al, 2010.]. Par conséquent, il est nécessaire d'élargir l'ingénierie inverse à **l'ingénierie inverse fonctionnelle pour la sécurité** (ou FRES pour Functional Reverse Engineering for Safety) dans notre travail.

Pour la question 6 ; Nous proposons de définir les objectifs de sécurité pour éliminer ou réduire les risques. La réingénierie est communément utilisée pour l'examen et la modification d'un système dans l'objectif de le reconstituer sous une nouvelle forme. Nous proposons d'élargir la **réingénierie à la réingénierie fonctionnelle pour la sécurité** (ou FR2ES pour Functional RE-Engineering for Safety) dans le cadre de notre travail. La démarche FR2ES doit également répondre à la question 7 qui correspond à **l'opérationnalisation des cas d'emploi 2 et 3 de la méthode IRAD**.

1.4.2. Construction d'un cadre de conception sécuritaire pour l'opérationnalisation d'IRAD

Tout produit connaît plusieurs états à partir du moment où il est souhaité, imaginé, jusqu'au moment où il est détruit voire recyclé. L'ensemble de ces phases est appelé le « cycle de vie d'un produit ». D'après la norme [ISO 15226, 1999], le cycle de vie d'un produit est défini comme étant le temps écoulé entre l'élaboration du concept même du produit et sa mise au rebut. Une décomposition possible de ce cycle est représentée par Alting [Alting, 1993] en 6 phases (figure 1.13). Par rapport à cette représentation du cycle de vie d'un produit, la « Conception sécuritaire » va impacter deux phases : la conception et l'usage.

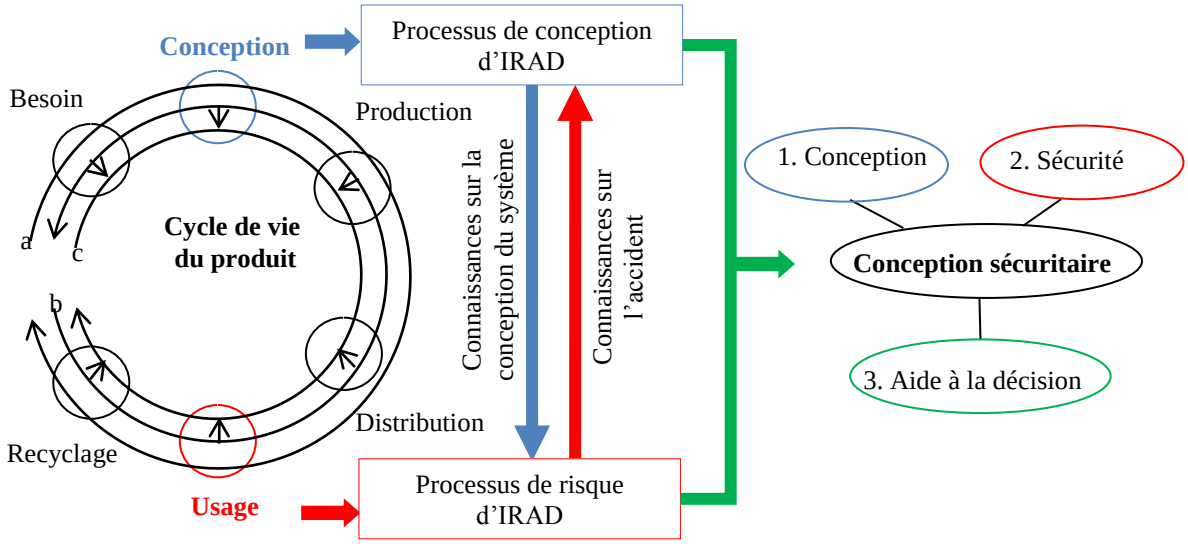


Figure 1.13. Cadre de la conception sécuritaire.

La méthode IRAD combinée au développement d'une méthode d'aide à la décision doit permettre l'intégration de la sécurité en conception. Afin d'y parvenir, nous proposons :

- de nous baser sur l'ingénierie inverse pour opérationnaliser le cas d'emploi 1 d'IRAD ;
- de nous baser sur la réingénierie pour opérationnaliser les cas d'emploi 2 et 3 ;
- d'utiliser les approches de l'ingénierie des connaissances pour la représentation et l'utilisation des connaissances.

Notre démarche porte donc sur deux développements complémentaires :

- L'ingénierie inverse fonctionnelle pour la sécurité (ou FRES pour Functional Reverse Engineering for Safety). L'objectif de cette phase est d'extraire et de formaliser les connaissances technique et de sécurité du système existant à partir de l'analyse du REX. Les résultats de la mise en œuvre de cette démarche sont des connaissances sur l'accidentologie et sur la conception du système ainsi que le type de risque et la mesure de la sécurité [Sadeghi et al., 2013a].
- La Réingénierie fonctionnelle pour la sécurité (ou FR2ES pour Functional RE-Engineering for Safety). L'objectif de cette phase est d'intégrer les connaissances issues de la démarche FRES afin de définir des objectifs de sécurité et ses niveaux d'intervention et proposer un processus de conception sécuritaire [Sadeghi et al., 2013b].

La figure 1.14 présente le diagramme IDEF0 niveau A0 du processus de conception sécuritaire proposé.

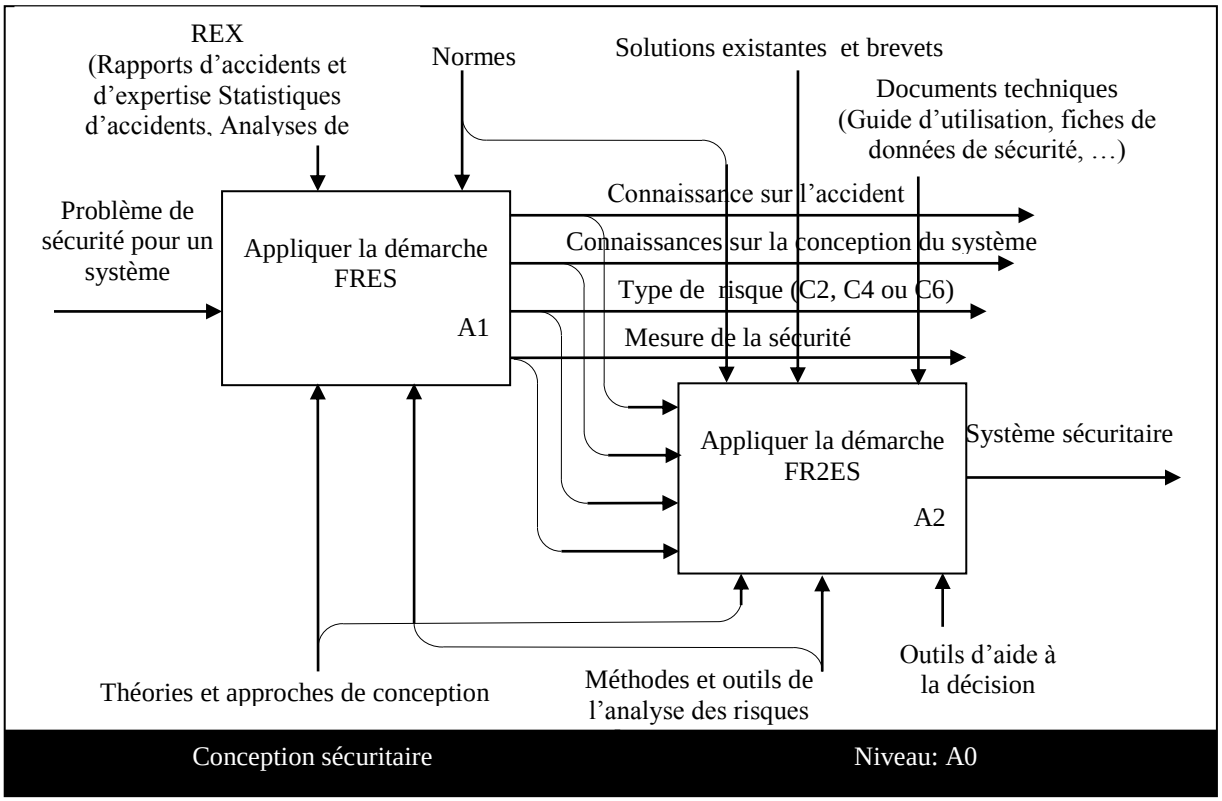


Figure 1.14. Diagramme IDEF0 niveau A0 du processus de conception sécuritaire.

1.4.3. Conclusion sur le cadre méthodologique pour la conception sécuritaire

Cette partie a présenté une synthèse des travaux normatifs et scientifiques d'intégration de la sécurité en conception. IRAD en est ressortie comme proposant le meilleur cadre méthodologique pour la conception sécuritaire. Pour cette raison, elle fait ensuite l'objet d'une étude plus approfondie afin d'en identifier les problèmes et manques que l'on peut rencontrer lors de sa mise en œuvre. Suite à cette synthèse, nous proposons un cadre méthodologique pour l'opérationnalisation d'IRAD. Ce cadre est basé sur deux démarches complémentaires : l'Ingénierie inverse fonctionnelle pour la sécurité (FRES) et la Réingénierie fonctionnelle pour la sécurité (FR2ES) ; chacune d'elles comportant plusieurs phases d'évaluation de la sécurité des choix proposés.

1.5. Conclusion

Dans ce chapitre, nous avons présenté, dans un premier temps, les contextes, le besoin industriel et les problématiques scientifiques de la thèse. Dans un deuxième temps, nous avons expliqué les travaux normatifs et scientifiques sur la conception sécuritaire. Dans un troisième temps, dans le cadre de l'opérationnalisation de la méthode IRAD, nous avons proposé un cadre méthodologique pour l'intégration de la sécurité en conception. Ce cadre s'appuie sur deux développements complémentaires : l'ingénierie inverse fonctionnelle pour la sécurité (FRES) et la Réingénierie fonctionnelle pour la sécurité (FR2ES).

Dans ce mémoire, nous allons répondre aux questions présentées dans le §1.3.5 comme suit :

- Le chapitre suivant (**chapitre 2**) présente la formalisation des rapports d'accidents afin de répondre à la première question.
- Les **chapitres 3, 4 et 5** détaillent le processus de conception sécuritaire proposé.
    - Le **chapitre 3** expose l'approche FRES afin de répondre aux questions 2 et 3 ;
    - Le **chapitre 4** présente l'approche d'évaluation de et pour la sécurité pour répondre aux questions 4 et 5 ;
    - Le **chapitre 5** développe l'approche FR2ES pour répondre aux questions 6 et 7.

Chapitre 2. Formalisation du REX : Proposition d'une structure type de rapport d'accident

2.1. Introduction

Comme cela a été évoqué dans le chapitre précédant, et dans le cadre de l'opérationnalisation de la méthode IRAD, la question à laquelle nous devons répondre est : *Comment formaliser le Retour d'EXpérience (REX) ?* Dans le contexte de l'amélioration de la sécurité des systèmes, toute information sur les circonstances d'une altération de la sécurité d'opérateurs utilisant un système peut s'avérer essentielle. Dans le contexte agricole, le ministère en charge de l'agriculture et les assureurs collectent ce type d'informations dans le cas d'accidents graves. Ces informations sont retranscrites dans un rapport d'accident. Cependant, il n'existe pas de rapport d'accident type et les données collectées ne sont souvent pas assez précises pour être exploitées afin d'améliorer le système incriminé. Nous proposons ici de combler ce manque de formalisme.

Avant de décrire la méthode proposée pour atteindre cet objectif, nous proposons dans la section suivante (section 2.2) un état de l'art sur le REX. Tout d'abord, nous introduisons la notion de REX. Ensuite, nous détaillons les classifications du REX et précisons leur intérêt pour nos travaux. La section 2.3 détaille la structure type proposée d'un rapport d'accident. La section 2.4 présente le cas d'application de notre recherche, les liaisons tracteurs-outils. Ensuite, la section 2.5 décrit comment compléter la structure de rapport proposée à partir de deux accidents différents, un premier incriminant un arbre de transmission à cardans et un second impliquant la liaison trois points. Pour finir, la section 2.6 comprend la conclusion et les perceptives de cette partie.

2.2. Le Retour d'EXpérience

2.2.1. Qu'est-ce que le Retour d'Expérience ?

Il existe différents travaux portant sur le Retour d'EXpérience (« Experience Feedback » en anglais) ainsi que de nombreuses définitions. Selon [Ghemraoui, 2009], les connaissances issues du REX sont relatives au fonctionnement d'un produit connu, dans un contexte spécifique, pour un utilisateur et une activité spécifique.

[Rakoto, 2004] précise que le « *REX est construit à partir de la description de l'événement lui-même et de l'environnement dans lequel il est apparu, de l'expérience acquise pour pallier ou favoriser l'occurrence de l'événement et de la création de connaissances* ».

Selon [Mazouni, 2008] « *Le REX est le fait d'exploiter des connaissances historiques archivées afin de dégager un savoir-faire en matière de management de la sécurité* ». L'auteur propose une méthode de management des risques (Management Préliminaire des Risques - MPR) basée sur une ontologie générique permettant de canaliser les mécanismes de capitalisation et d'exploitation des connaissances relatives aux scénarios d'accident. Cette méthode comporte quatre phases : la phase d'identification des scénarios d'accident, la phase d'estimation des risques, la phase d'évaluation des risques et la phase de maitrise des risques.

[Kamsu Goguemn et al., 2008] ont défini le retour d'expérience comme « *un processus de capitalisation et d'exploitation des connaissances visant essentiellement à transformer la compréhension acquise par l'expérience en connaissances* ». Ils ont proposé de formaliser ces connaissances sur le REX en utilisant l'ontologie. Les auteurs proposent un cadre du REX qui distingue cinq types d'information : l'événement, le contexte, l'analyse, la solution et les leçons apprises.

Se basant sur [Rakoto et al., 2002] et [Clermont et al., 2007], [Béler, 2008] propose la définition suivante : « *Le retour d'expérience est une démarche structurée de capitalisation et d'exploitation des connaissances issues de l'analyse d'événements positifs et/ou négatifs. Elle*

met en œuvre un ensemble de ressources humaines et technologiques qui doivent être organisées pour contribuer à réduire les répétitions d'erreurs et à favoriser certaines pratiques performantes ». Il présente les différentes entrées et sorties du processus de capitalisation et d'exploitation des connaissances (figure 2.1).

Il définit deux catégories d'entrées : les événements positifs et négatifs. Parmi ces entrées, les REX « événementiel » (accidents, événements à perte)) sont les plus courants. Il classe ensuite le REX en trois grandes classes [Béler, 2008]:

- **Retour d'expérience positif ou négatif**. Cette classe distingue les situations considérées anormales (écart à la norme et au fonctionnement normal du système) et les bonnes pratiques;
- **Retour d'expérience statique ou dynamique**. Contrairement à l'approche dynamique, l'approche statique permet de collecter et de diffuser la connaissance sans traitement « intelligent ». ;
- **Retour d'expérience statistique ou cognitif.** Le REX statistique est utilisé lorsque les informations stockées le sont en quantité suffisante. Dans le cas contraire, il devient nécessaire d'y adjoindre des connaissances issues d'analyses expertes.

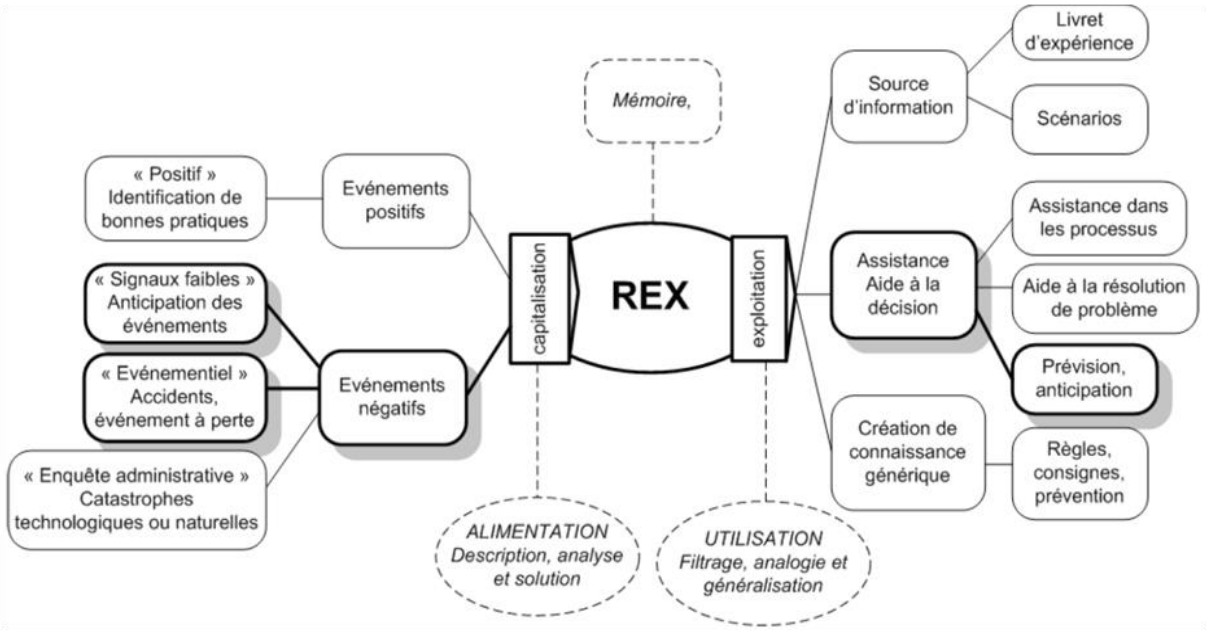


Figure 2.1. Vue d'ensemble des applications du retour d'expérience [Béler, 2008].

Selon [Kjellén, 2000], le retour d'expérience joue un rôle central dans la prévention des accidents. Selon elle, il regroupe des informations provenant de différents canaux comme les **rapports d'accident** et de **pré-accident** et l'inspection de la situation de travail. Il se base sur un modèle de système d'information SHE (SHE pour Safety, Health and Environment) présenté à la figure 2.2.

Un système d'information SHE assure les fonctions de prévention des accidents suivants:

1. **Collecte de données** sur les risques d'accident en utilisant les rapports d'accident et quasi-accidents, inspections de la situation de travail, audits et analyses des risques. Les méthodes de collecte de données comprennent l'observation, des entrevues, l'auto-évaluation, des discussions de groupe, etc.

2. **Stockage de données** dans une mémoire (fichier papier, électronique, etc.) et la récupération de données à partir de celui-ci.
3. **Traitement de l'information**, c'est-à-dire la récupération et l'analyse des données, la compilation en informations utiles, le développement de mesures correctives, etc.
4. **Distribution des informations** aux décideurs dans l'organisation.

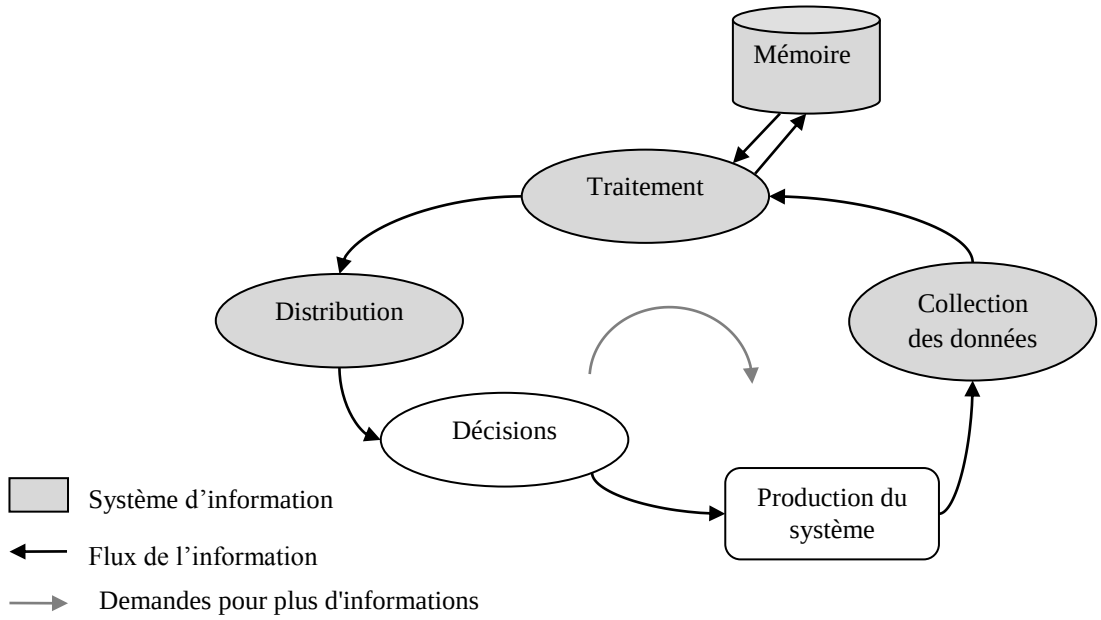


Figure 2.2. Flux de l'information dans un système information SHE [Kjellén, 2000].

Des effets positifs sur la sécurité ne sont obtenus que lorsque la boucle est bouclée. C'est à dire lorsque les résultats de ces décisions sont mises en œuvre d'une manière qui affecte les situations de travail (existantes ou futures).

2.2.2. Utilisation du REX dans notre recherche

L'intérêt du REX dans notre recherche peut être vu selon trois angles différents :

- **REX et sécurité :** Du point de vue sécurité, le REX permet d'obtenir des informations sur les accidents. En effet, il permet de recueillir les faits reliés aux éléments d'une situation de travail qui ont mené à l'accident. Les connaissances sur l'accident doivent être extraites à partir de ces éléments.
- **REX et conception :** Du point de vue conception, le REX permet de déterminer le système ou la partie du système impliquée dans un accident. Les connaissances sur la conception doivent être extraites en analysant le système ou la partie du système identifiée.
- **REX et aide à la décision :** Le REX permet de regrouper les informations sur les différents accidents impliquant un système ou une partie du système. Le stockage de ces informations dans une base de connaissances peut ensuite servir à évaluer le niveau de sécurité du système pour enfin aider à la décision parmi les choix de solutions dans le cadre de la reconception sécuritaire de ce système. Ces informations peuvent également être utilisées pour la conception sécuritaire d'un nouveau système similaire à celui pour lequel les informations ont été récoltées.

2.2.3. Conclusion

Dans notre travail et comme dans [Mazouni, 2008] et [Kjellén, 2000], nous nous intéressons au REX sur l'accident. Nous reprenons la catégorisation du REX de [Béler, 2008] en trois grandes classes : REX positif ou négatif, REX statique ou dynamique et REX statistique ou cognitif. Dans notre contexte, notre démarche est basée sur un REX négatif, statique et cognitif ; négatif car nous basons nos travaux sur la prise en compte des causes des accidents, statique car nous considérons l'expérience pour la génération de connaissances et cognitif car le manque d'informations sur les causes des accidents nous amène à intégrer des éléments clés d'analyses expertes.

Un des documents clés du REX sur l'accident est le rapport d'accident [Kjellé, 2000], sur lequel nous proposons de nous pencher davantage. Celui-ci détaille les faits liés aux éléments d'une situation de travail et à des événements qui ont mené à l'accident. Dans le contexte de la conception sécuritaire de machines agricoles, les connaissances issues de rapports d'accidents s'avèrent prépondérantes afin d'améliorer la sécurité au plut tôt lors du processus de conception. Cependant, les contenus de ces rapports sont très hétérogènes et, pour cette raison, souvent inexploitables.

Le but de la section suivante est de répondre à ce problème en proposant une structure type de rapport d'accident. D'un rapport correctement complété, il est possible d'extraire des connaissances utiles et applicables afin de les utiliser dans le processus de reconception du système ou de la partie du système impliquée dans l'accident. En effet, nous allons analyser cette structure type de rapport d'accident proposée afin d'extraire les connaissances sur l'accident et sur la conception du système.

2.3. Proposition d'une structure type de rapport d'accident

2.3.1. Les rapports d'accident existants

Dans un premier temps, nous avons analysé 12 rapports d'accidents impliquant l'Arbre de Transmission à Cardans (ATC). Ces rapports nous ont été fournis par la Caisse Centrale de la Mutualité Sociale Agricole[2] (CCMSA) et le Bureau Santé Sécurité au Travail[3] (BSST) du Ministère de l'Agriculture, de l'Agroalimentaire et de la Forêt. Ces rapports font en moyenne 8 pages (3 pages min, 22 pages max). Ils comportent entre 7 et 10 parties différentes contenant des renseignements sur l'accident notamment sur les victimes, une description des systèmes et les conditions d'utilisation au moment de l'accident. Ces rapports ont été réalisés par un inspecteur du travail, un contrôleur du travail ou un conseiller en prévention de la CCMSA.

2.3.2. Structuration d'un rapport d'accident

Comme nous l'avons cité précédemment, le but du rapport d'accident est de recueillir les faits reliés aux éléments d'une situation de travail qui ont mené à l'accident. Les questions principales auxquelles nous devons pouvoir répondre sont :

1. ***Qui** a été blessé ?* Répondre à cette question demande des **informations sur la victime** ;

[2] La CCMSA est un organisme qui s'occupe de la protection sociale des agriculteurs et des personnes travaillant dans le monde agricole ainsi que leurs familles.

[3] Le BSST du MAAF a pour missions principales l'élaboration de la réglementation relative à la santé et à la sécurité au travail des salariés et des non-salariés et la définition, avec la CCMSA, de la politique de prévention des accidents du travail et des maladies professionnelles en direction des salariés et des non-salariés agricoles.

2. ***Quand*** *et* ***Où*** *la victime a été blessée ?* Répondre à cette question demande des **informations sur les circonstances de l'accident** ;
3. ***Qui*** *a été témoin de l'accident ?* Répondre à cette question demande des **informations sur le(s) témoin(s)** ;
4. ***Quel*** *est le système en cause ?* Répondre à cette question demande des **informations sur le système en cause**;
5. ***Quelle*** *est la blessure de la victime?* Répondre à cette question demande d'identifier le **dommage**;
6. ***Que*** *s'est-il passé ?* Répondre à cette question demande d'identifier le **type d'accident**;
7. ***Comment*** *et* ***Pourquoi*** *cela s'est-il passé ?* Répondre à cette question demande une **description de l'accident**;
8. ***Que*** *peut-on faire afin d'éviter qu'un tel accident ne se reproduise ?* Répondre à cette question demande de déterminer les **mesures correctives** ;
9. ***Quels*** *ont été les premiers soins apportés à la victime ?* Répondre à cette question demande des **informations sur les premiers soins apportés**.

Le rapport d'accident doit être **signé** par le(s) personne(s) ayant rédigé le rapport. Une **annexe** peut être utile pour compléter le rapport par des photos du système ou de la partie du système mise en cause dans l'accident.

Nous proposons donc que le rapport type comporte « neuf +deux » parties pouvant être complétées facilement et utilisées soit par un expert en sécurité soit par un concepteur (figure 2.3).

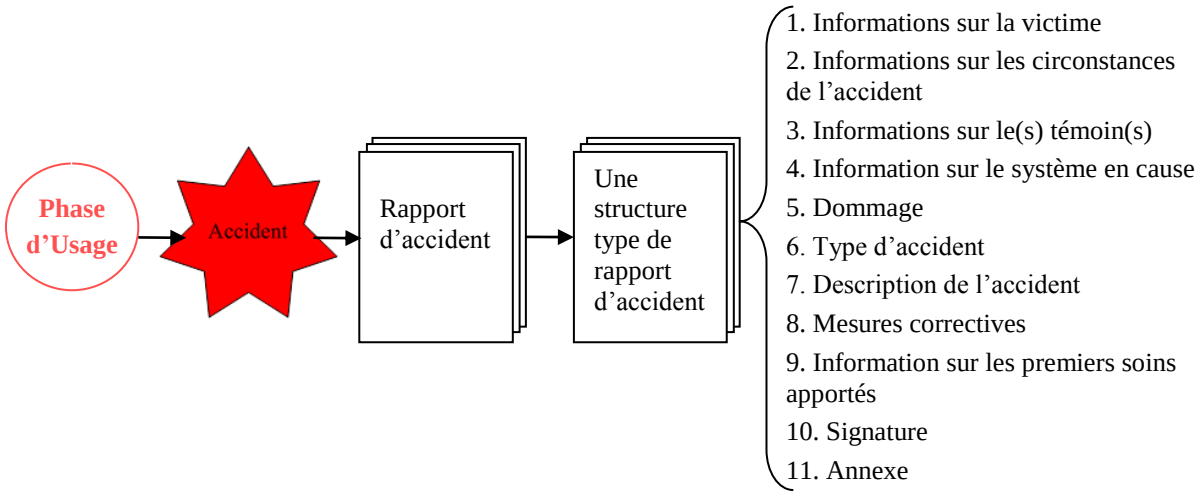


Figure 2.3. Vue générale du développement d'une structure type de rapport d'accident.

2.3.3. Présentation des différentes parties d'une structure type de rapport d'accident

Dans cette section, nous présentons les onze parties d'une structure type de rapports d'accident listés à la figure 2.3. A la fin de cette section, le tableau 2.3 montre la structure type de ce rapport.

1. Informations sur la victime

Cette partie a pour but de répondre à la première question : ***Qui*** *a été blessé ?* Pour cela, il faut renseigner les informations personnelles et les informations professionnelles de la victime :

- **Informations personnelles** : Nom, Prénom, Date de naissance (JJ/MM/AA), Lieu de naissance (Ville, N° et Rue, Code postal), Sexe, N° de Téléphone, et Adresse (Ville, N° et Rue, Code postal).
- **Informations professionnelles** : Division, Département, Unité, N° de Téléphone, Nombre d'années d'expérience (si moins d'un an : mettre 0).

Ces informations devraient être les mêmes quelle que soit la personne qui remplit le rapport d'accident.

2. Informations sur les circonstances de l'accident

Cette partie a pour but de répondre à la question : ***Quand et Où*** *la victime a été blessée?* Elle demande de déterminer les informations sur les circonstances de l'accident. Ces informations sont relatives à l'accident et à la déclaration de l'accident :

- **Informations relatives à la déclaration de l'accident** : Date de la déclaration de l'accident (JJ/MM/AA) ; Heure de la déclaration de l'accident ; Par qui l'accident a-t-il été déclaré? Si l'accident n'a pas été déclaré tout de suite, pourquoi?
- **Information relatives à l'accident** : Date de l'accident (JJ/MM/AA), Heure de l'accident, Lieu de l'accident (Nom et adresse du lieu de l'accident ou Nom et adresse du chantier).

Ces informations devraient être les mêmes quelle que soit la personne qui remplit le rapport d'accident.

3. Informations sur le(s) témoin(s) (ou la 1ère personne avisée en cas d'absence de témoin)

La troisième question à laquelle il faut répondre est : ***Qui a*** *été témoin de l'accident ?* Cette partie demande de renseigner des informations sur le ou les témoins de l'accident. En cas l'absence de témoin, il faut indiquer la 1ère personne qui a été avisée de l'accident. Les informations à indiquer sont :

- Nom, Prénom, Poste, Téléphone, Adresse (Ville, N° et Rue et Code postal).

Ces informations devraient être les mêmes quelle que soit la personne qui remplit le rapport d'accident.

4. Informations sur le système en cause

Le but de cette partie est de répondre à la question : ***Quel*** *est le système en cause ?* Pour cela, il faut indiquer le type du système et déterminer les informations sur la fabrication du système :

- **Le type de système** : Il existe plusieurs types de système. Nous définissons les catégories suivantes :
    - Tracteur ;
    - Liaison Tracteur-Outil :
        - Liaisons d'accrochage mécanique :
            - Pour les outils portés (Liaison trois points) ;
            - Pour les outils semi-portés ;
            - Pour les outils trainés.
        - Liaisons de transmission de puissance :
            - Mécanique (Arbre de transmission à cardans) ;
            - Hydraulique/ Pneumatique ; et
            - Electrique/ Electronique.

- Outil :
    - Outils portés : Cultivateur porté ; et Etc.
    - Outils semi-portés : Cultivateur semi-porté ; et Etc.
    - Outils trainés : Remorque trainé ; et Etc.
- Etc.

Information sur la fabrication du système: Pour cette partie, il faut indiquer la marque, le modèle et l'année de fabrication du système.

Ces informations devraient être les mêmes quelle que soit la personne qui remplit le rapport d'accident.

5. Dommage

La question est : ***Quelle*** *est la blessure de la victime?* Pour répondre à cette question, nous reprenons la proposition faites dans les documents normatifs. Dans la norme [NF EN ISO 12100, 2010], le dommage est défini comme une « *blessure physique ou atteinte à la santé* ». Y est définie, la gravité du dommage comme « *la gravité de lésions ou de l'atteinte à la santé* » (voir § 1.2.3.2). Cette norme donne la classification de la gravité du dommage suivante: légère, grave, décès. Dans le document technique [FD ISO/TR 14121-2, 2008], nous trouvons plusieurs exemples de classification des niveaux de gravité du dommage (tableau 2.1) :

Tableau 2.1. Exemples de classification des niveaux gravités du dommage [FD ISO/TR 14121-2, 2008].

	Exemples de classification des niveaux de gravité du dommage
1	- Catastrophique : décès ou blessure ou maladie invalidante permanente (impossibilité de reprendre le travail) ; - Sérieuse : blessure ou maladie débilitante sérieuse (possibilité de reprendre le travail un jour) ; - Mineure : blessure ou maladie significative nécessitant plus que les premiers soins (possibilité de reprendre le travail au même poste) ; - Modérée : aucune blessure ou blessure légère ne nécessitant que les premiers soins (peu voire aucun temps de travail perdu).
2	- Blessure légère (habituellement réversible) ; exemples : égratignure, lacération, coupure légère nécessitant les premiers soins, etc. - Blessure sérieuse (habituellement irréversible) ; exemples : membre cassé ou arraché ou écrasé, fracture, blessure sérieuse nécessitant des points de suture, troubles musculo-squelettiques majeurs, décès, etc.
3	- Décès ou handicap sérieux permanent; exemples : Quadriplégie, Paraplégie, Inconscience prolongée (coma), Dommage cérébral permette, etc. - Blessure majeure; exemples : Tout type de fracture (autre que les doigts, les pouces et les orteils), Perte de conscience, Dislocation de l'épaule, de la hanche, du genou ou des vertèbres, Traitement nécessaire en raison d'une exposition à des émanations, etc. - Blessure mineure; exemples : Fracture des os mineure (doigts, orteils), Coupures et bleus, Cause quelconque nécessitant des premiers soins seulement, etc. - Aucune blessure ou accident; exemples : Aucune blessure pouvant être évitée.
4	- Égratignures, bleus soignés par des premiers soins ou un procédé semblable ; - Égratignures, bleus et agressions plus sévères nécessitant une attention médicale effectuée par des professionnels ; - Blessure normalement irréversible. Il sera légèrement difficile de continuer à travailler après la guérison ; - Blessure irréversible telle qu'il sera très difficile de continuer à travailler après la guérison, si c'est le cas.

Le tableau ci-dessus montre que la gravité du dommage est liée soit à la partie du corps touchée (doigts, orteils, …), soit au type de blessure (Blessure légère, Blessure sérieuse, …). En se basant sur ces différentes classifications des niveaux de gravité du dommage, nous proposons que la gravité du dommage soit catégorisée en deux rubriques : la partie du corps touchée et le type de blessure.

La partie du corps touchée : dans un premier temps, il faut indiquer l'endroit du corps où la victime a été atteinte en précisant, s'il y a lieu, droite ou gauche (figure 2.4). En cas de localisation multiple, il faut indiquer la case correspondant au siège de la lésion principale, et à partir de trois lésions indiquer « lésions multiples ».

Le type de blessure : Nous proposons la classification suivante pour le type de blessure :

- Blessures réversibles grâce à des premiers secours ;
- Blessures réversibles grâce à des soins médicaux ;
- Blessures sans incapacité permanente (Perte de doigts, ...) ;
- Blessures avec incapacité permanente (Perte d'un œil, d'un bras, …) ;
- Décès.

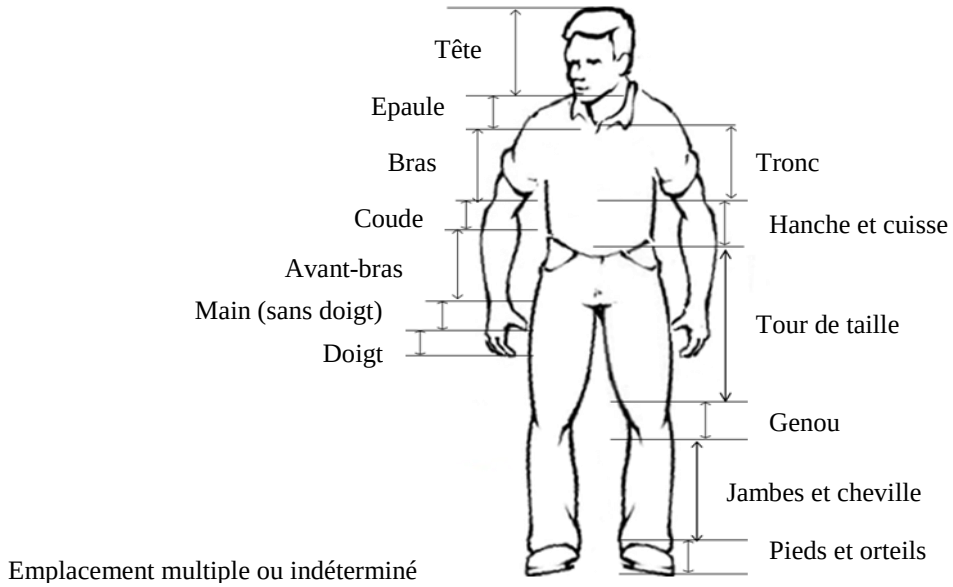


Figure 2.4. Les parties du corps.

6. Type d'accident

Cette partie a pour objectif de répondre à la question : ***Que*** *s'est-il passé ?* Il convient ici d'identifier le type d'accident. Un type d'accident regroupe les accidents ayant les mêmes conséquences, les mêmes sources de phénomènes dangereux et causés par le même type de système ou sous-système. Nous reprenons la classification de la norme [NF EN ISO 121000, 2010] en ce qui concerne les conséquences et les sources de phénomènes dangereux (tableau 2.2). Ces derniers y sont listés sans catégorisation ni ordre apparent.

Tableau 2.2. Types d'accidents basés sur la classification des conséquences et des sources de phénomènes dangereux mécanique [NF EN ISO 12100, 2010].

Conséquences de phénomène dangereux	Sources de phénomène dangereux
. renversement (par une machine mobile); . éjection; . écrasement; . coupure ou sectionnement; . entraînement ou emprisonnement; . happement, enroulement; . frottement ou abrasion; . choc; . injection; . cisaillement; . glissade, trébuchement et chute; . perforation ou piqûre; . suffocation ; . autre.	. accélération, décélération; . pièces de forme aiguë; . rapprochement d'un élément en mouvement avec une pièce fixe; . éléments coupants; . éléments élastiques; . chute d'objets; . pesanteur; . hauteur par rapport au sol; . pression élevée; . instabilité; . énergie cinétique; . mobilité de la machine; . éléments en mouvement; . éléments en rotation; . surface rugueuse, glissante; . arêtes vives . énergie accumulée; . vide ; . autre.

7. Conditions de l'accident

Cette partie a pour but de répondre à la question ***Comment*** *et* ***Pourquoi*** *cela s'est-il passé?* Les informations demandées ici sont une description précise et la séquence d'événements qui a mené à l'accident.

Les accidents peuvent survenir suite aux conditions de fonctionnement du système, à l'activité de l'opérateur et aux conditions environnementales (figure 2.5). Cela signifie qu'il convient ici de décrire les conditions de fonctionnement du système, de l'activité de l'opérateur, et des conditions environnementales afin d'extraire des informations accidentelles. Il est à noter que trouver les causes de l'accident n'est pas l'objectif de cette partie.

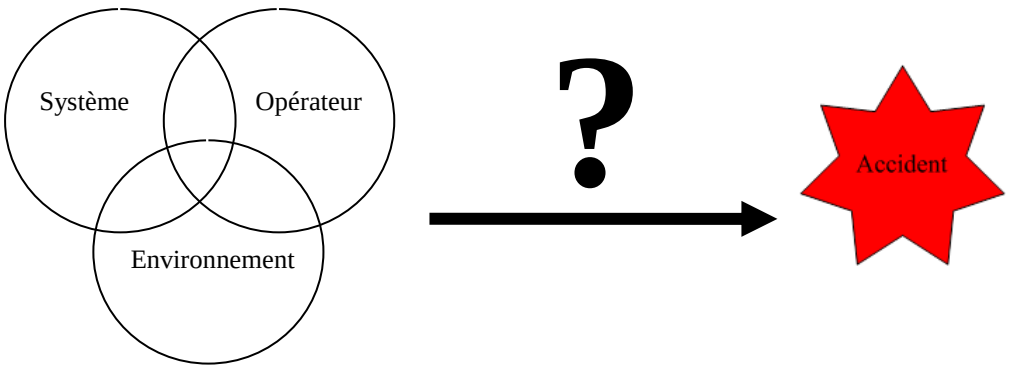


Figure 2.5. Situation de travail et accident.

L'extraction des conditions d'un accident demande donc de décrire les trois éléments suivant :

7.1. Les conditions de fonctionnement du système

A cet effet, les trois aspects suivants doivent être définis et décrits :

La sous-phase de la phase d'usage du système : Comme nous l'avons cité dans le chapitre 2, nous nous intéressons aux accidents qui se produisent dans la phase d'usage du système. Plusieurs classifications des sous-phases de la phase d'usage du système existent. La norme [NF NE ISO 12100, 2010] propose la classification suivante: transport, montage et installation, mise en service, utilisation, démontage, mise hors service et mise au rebut. Pour la phase d'usage, [Caputo et al., 2013] utilisent le terme de « phase opérationnelle » et proposent les activités suivantes pour cette phase: installation, fonctionnement, nettoyage, maintenance et mise hors service. En se basant sur ces deux classifications, nous adoptons une classification regroupant l'ensemble des activités et des états du système en phases d'usage sous cinq sous-phases :

- **Montage, installation, mise en service** (ex: attelage, raccordement, fixation, réglage et vérification avant utilisation, etc.) ;
- **Transport** (ex: déplacer le système du lieu de stockage jusqu'au lieu d'utilisation, chargement et déchargement du système, mise du système en configuration de transport, etc.) ;
- **Utilisation** (ex: démarrage et fonctionnement du système, alimentation en substance, réglage et contrôle sous fonctionnement, etc.) ;
- **Démontage, mise hors service** (ex: débranchement, dételage, stockage entre deux utilisations, etc.) ;
- **Maintenance** (ex: entretien, graissage, nettoyage, débourrage, recherche de panne, réparation, etc.).

La tâche : La tâche est définie dans la norme [NF EN ISO 12100, 2010] comme une activité spécifique réalisée par une ou plusieurs personnes sur ou autour du système pendant son cycle de vie. En général, les procédures de réalisation des tâches qu'un opérateur doit effectuer sont fournies par le constructeur via le guide d'utilisation ou des indications présentes sur le système lui-même. La norme [NF EN ISO 12100, 2010] liste un certain nombre de tâches:

- Alimentation de la machine ;
- Apprentissage/programmation ;
- Arrêt de la machine ;
- Arrêt de la machine en cas d'urgence ;
- Changement de processus/outil ;
- Démarrage ;
- Essais ;
- Maintenance préventive ;
- Maintenance corrective ;
- Manipulation de consommable ;
- Nettoyage et entretien ;
- Recherche de défauts/de pannes (intervention de l'opérateur) ;
- Redémarrage après arrêt imprévu ;
- Réglage ;
- Reprise du fonctionnement après bourrage ou blocage ;
- Retrait de consommable de la machine ;
- Autre.

Ici aussi, les tâches définies sont listées sans catégorisation ni ordre apparent. Nous utiliserons cette liste de tâche dans notre travail.

L'état du système : Il est nécessaire ici de savoir si le système accomplissait la fonction prévue ou non.

7. 2. Description du comportement et des capacités de l'opérateur

L'opérateur peut être l'élément déclencheur de l'accident. Il est donc nécessaire de décrire son activité et les conditions dans lesquelles il se trouvait au moment de l'accident. Pour cela, nous mettons en évidence, à partir de l'analyse des différents rapports d'accident, les éléments suivants afin de décrire l'activité de l'opérateur :

Le comportement de l'opérateur : Identifier le comportement de l'opérateur revient à répondre à la question : *Est-ce que l'opérateur utilisait le système en respectant la procédure et les consignes de sécurité fournies par le constructeur ?*

Les capacités de l'opérateur : Il faut vérifier que l'opérateur était capable d'utiliser le système. Nous synthétisons, à partir de l'analyse des différents rapports d'accidents, quatre déterminants permettant de décrire la capacité de l'opérateur à réaliser la tâche avec le système :

- La formation : personne avec formation ou sans formation ;
- L'expérience : personne expérimentée ou personne inexpérimentée ;
- L'état physique : capacités physiques limitées ;
- L'aptitude : stress, fatigue, préoccupations, etc.

7. 3. Description des conditions environnementales

Comme déjà indiqué précédemment, nous considérons toute autre personne que l'opérateur comme faisant partie de l'environnement. Les conditions environnementales telles que les facteurs physiques, chimiques, climatiques et organisationnels caractérisant le milieu de travail peuvent causer un accident. Selon la norme [NF EN ISO 12100, 2010], les conditions d'environnement sont les températures minimale et maximale recommandées, l'utilisation éventuelle de la machine à l'intérieur ou à l'extérieur, par temps sec ou humide, l'exposition directe au rayonnement solaire, la tolérance à la poussière et à l'humidité, etc. Nous regroupons ces conditions environnementales en trois classes :

- La présence de tiers (étranger à la tâche) : toute autre personne que l'opérateur ;
- L'environnement fermé ou ouvert : température, humidité, vent, luminosité, bruit, poussière, etc. ;
- Le milieu structuré ou naturel : inclinaison du sol, nature du sol, glissement du sol, objets ou obstacles fixes, objets ou obstacles mobiles, etc.

8. Mesures correctives

Cette partie demande de lister les mesures de prévention applicables afin d'éviter qu'un tel accident ne se reproduise ainsi que la réglementation applicable. Elle est davantage à destination des experts sécurité remplissant cette partie du rapport. Ces éléments sont bien trop limités pour être utilisables par les concepteurs. L'objectif de nos travaux est de traiter cet aspect d'un point de vue scientifique.

9. Informations sur les premiers soins apportés

Les premiers soins apportés à la victime sont décrits dans cette partie. Elle permet de savoir si la victime a reçu des soins médicaux, si elle s'est rendue à l'hôpital et quel médecin s'en est chargé. Les informations à indiquer sont les suivantes :

- **Informations sur le médecin**: Nom, Prénom, N° de Téléphone.
- **Adresse d'hôpital**: Ville, N° et Rue et Code postal.

10. Signature

Le rapport d'accident doit être signé par le(s) personne(s) ayant complété le rapport.

11. Annexe

Cette partie permet de compléter le rapport par des photos du système ou de la partie du système mis en cause dans l'accident et dans la situation dans laquelle il a été retrouvé.

2.3.4. Conclusion

La présente structure de rapport d'accident a pour but :

- de collecter des informations factuelles sur les accidents de travail d'une manière efficace en onze différentes parties;
- de fournir un cadre de manière à avoir un maximum d'informations identiques d'un rapport à l'autre, quelle que soit la personne qui le remplit;
- d'aider à déterminer les conditions de causalité des accidents à partir des données restituées dans les parties dommage, type d'accident et conditions de l'accident;
- de collecter des données factuelles de manière systématique afin de pouvoir réaliser des analyses de tendances (statistiques).

Il convient de noter que nous souhaitons que les rubriques du rapport d'accident soit facilement compréhensibles. Pour cela, nous y remplaçons certains termes utilisés jusqu'à maintenant par d'autres (système par machine, conséquence du phénomène dangereux par conséquence de l'accident, source du phénomène dangereux par source de l'accident). La structure type du rapport d'accident est donc la suivante (tableau 2.3):

Tableau 2.3. Structure type de rapport d'accident.

Rapport d'accident

1. Informations sur la victime

▪ Informations personnelles
. Nom : …… . Prénom : …… . Date de naissance (JJ/MM/AA): |__|__|/|__|__|/|__|__|
. Lieu de naissance : Ville : ……..N° et Rue : …….. Code postal : |__|__|__|__|__|
. Sexe : Masculin ☐ Féminin ☐
. N° de Téléphone : |__|__|__|__| __|__|__|__|__|__|
. Adresse (résidence) : Ville : …….. N° et Rue : ……Code postal : |__|__|__|__|__|

▪ Informations professionnelles
. Division :
. Département :
. Unité :
. N° de Téléphone : |__|__|__|__| __|__|__|__|__|__|
. Nombre d'années d'expérience : |__|__|an (si moins d'un an : mettre 0)

2. Informations sur les circonstances de l'accident

▪ Information relatives à l'accident
. Date de l'accident (JJ/MM/AA): |__|__|/|__|__|/|__|__| . Heure de l'accident : |__|__|h|__|__|mn

. Lieu de l'accident (Nom et adresse du lieu de l'accident ou Nom et adresse du chantier) :
Nom : ……. Adresse : Ville : …….. N° et Rue : ……Code postal : |__|__|__|__|__|

▪ Information relatives à la déclaration de l'accident
. Date de la déclaration de l'accident (JJ/MM/AA):|__|__|/|__|__|/|__|__|
. Heure de la déclaration de l'accident : |__|__|h|__|__|mn
. Par qui l'accident a-t-il été déclaré? ……..
. Si l'accident n'a pas été déclaré tout de suite, pourquoi? ……

3. Informations sur le(s) témoin(s) (ou la 1ère personne avisée en cas d'absence de témoin)

▪ Témoin □ ▪ 1ère personne avisée□
. Nom : …… . Prénom : …… . Poste : …….
. Téléphone : |__|__|__|__| __|__|__|__|__|__|
. Adresse : Ville : ……. N° et Rue : ……. Code postal : |__|__|__|__|__|

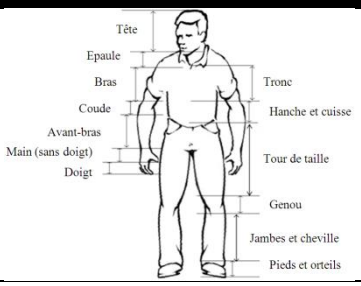
4. Informations sur la machine en cause

▪ Type de la machine:
. Tracteur □
. Liaison Tracteur-outil □
. Liaisons d'accrochage mécanique □
. Pour les outils Portés (Liaison trois points) □
. Pour les outils Semi-portés □
. Pour les outils Trainés □
. Liaisons de transmission de puissance □
. Mécanique (Arbre de transmission à cardans) □
. Hydraulique/ Pneumatique □
. Electrique/ Electronique □
. Outil □
. Outils portés □
. Cultivateur porté
. Autre□ (spécifiez) ……
. Outils semi-portés □
. Cultivateur semi-porté
. Autre□ (spécifiez) ……
. Outils trainés □
. Remorque trainé
. Autre□ (spécifiez) ……

(spécifiez) ……
. Autre□ (spécifiez) ……
▪ Informations sur la fabrication de la machine:
Marque :…… modèle : ……Année de fabrication : |__|__|__|__|

5. Dommages

▪ Partie du corps touchée :
. Tête □
. Epaule □
. Bras□
. Avant-bras□
. Genou □
. Tronc □
. Doigt □
. Main (sans doigt) □
. Jambes et cheville □
. Hanche et cuisse □
. Coude □
. Tour de taille □
. Pieds et orteils □
. Emplacement multiple ou indéterminé □



▪ Type de blessure :
. Blessure réversible grâce à des premiers secours □
. Blessure réversible grâce à des soins médicaux □
. Blessure sans incapacité permanente (Perte de doigts, ...) □
. Blessure avec incapacité permanente (Perte d'un œil, d'un bras, …) □
. Décès □

6. Type de l'accident

▪ Conséquence de l'accident:
. renversement (par une machine mobile) □
. éjection □
. écrasement □
. coupure ou sectionnement □
. entraînement ou emprisonnement □
. happement, enroulement □
. frottement ou abrasion □
. choc □
. injection □
. cisaillement □
. glissade, trébuchement et chute □
. perforation ou piqûre□
. suffocation □
. Autre □ (spécifiez) ……

▪ Source de l'accident:

. accélération, décélération ☐	. instabilité☐	. Autre ☐ (spécifiez) ……
. pièces de forme aiguë ☐	. énergie cinétique ☐	
. rapprochement d'un élément en mouvement avec une pièce fixe ☐	. mobilité de la machine ☐	
	. éléments en mouvement ☐	
. éléments coupants ☐	. éléments en rotation ☐	
. éléments élastiques ☐	. surface rugueuse, glissante☐	
. chute d'objets☐	. arêtes vives☐	
. pesanteur ☐	. énergie accumulée ☐	
. hauteur par rapport au sol ☐	. vide☐	
. pression élevée ☐		

7. Conditions de l'accident

▪ Conditions de fonctionnement de la machine

▪ Sous-phase de la phase d'usage du système :

. Montage, installation, mise en service ☐ . Démontage, mise hors service ☐ . Transport ☐

. Maintenance ☐ . Utilisation ☐

▪ Tâche :

. Alimentation de la machine☐	. Maintenance corrective☐
. Apprentissage/programmation☐	. Manipulation de consommable☐
. Arrêt de la machine☐	. Nettoyage et entretien☐
. Arrêt de la machine en cas d'urgence☐	. Recherche de défauts/de pannes (intervention de l'opérateur) ☐
	. Redémarrage après arrêt imprévu☐
. Changement de processus/outil☐	. Réglage☐
	. Reprise du fonctionnement après bourrage ou blocage☐
. Démarrage☐	. Retrait de consommable de la machine☐
. Essais☐	. Autre ☐ (spécifiez) …….
. Maintenance préventive☐	

▪ État de la machine : *Est-ce que la machine accomplissait la fonction prévue ?* Oui☐ Non☐
si non spécifiez…….

▪ Comportement et capacités de l'opérateur

▪ Comportement de l'opérateur : *Est-ce que l'opérateur utilisait la machine en respectant la procédure et les consignes de sécurités fournis par le constructeur ?* Oui ☐ Non☐
si non spécifiez…….

▪ Capacités de l'opérateur :

. Formation (opérateur avait reçu une formation adéquate pour savoir utiliser la machine) : Oui☐Non☐

. Expérience (opérateur était avec expérience): Oui☐ Non☐

. Etat physique (opérateur était sans capacités physiques limitées) : Oui☐ Non☐

. Aptitude (opérateur était sans le stress, la fatigue, les préoccupations, etc.): Oui☐ Non☐

▪ Conditions environnementales

▪ Présence de tiers (autre personne était présentes dans l'environnement de travail) : Oui☐ Non☐

▪ Environnement fermé ou ouvert (l'environnement de travail était ouvert) : Oui☐ Non☐

▪ Milieu structuré ou naturel (l'environnement de travail était naturel): Oui☐ Non☐

8. Mesures correctives

▪ Proposition de mesures de prévention et réglementation applicable : …….
……

9. Informations sur les premiers soins apportés

▪ La victime a reçu des soins médicaux : Oui☐ Non☐ ;
si oui où: Domicile☐ Hôpital☐ ;
si en hôpital, informations sur le médecin et sur l'hôpital:
. Informations sur le médecin : Nom : ……. . Prénom : …… . N° de Téléphone : |__|__|__|__| __|__|__|__|__| __|
. Adresse d'hôpital: Ville : …….. N° et Rue : ……Code postal : |__|__|__|__| __|

10. Signature

. Contrôleur du travail ☐
. Inspecteur du travail ☐
. Autre ☐ (spécifiez) ……

Fait à ……, le (JJ/MM/AA):|__|__|/|__|__|/|__|__| Signature :

11. Annexe

▪ Photos de l'élément mis en cause dans l'accident

2.4. Présentation des cas d'applications : les liaisons tracteurs-outils

2.4.1. Les liaisons tracteurs-outils

Pour illustrer les solutions méthodologiques proposées dans nos travaux, nous considérons le cas des liaisons tracteurs-outils. Les liaisons tracteurs-outils consistent en la combinaison d'une multitude de sous-ensembles. Ces différents sous-ensembles coexistent dans un espace exigu. Ces liaisons peuvent être décomposées en deux sous-liaisons :

1. La liaison d'accrochage mécanique permettant de **porter** l'outil par le tracteur ;
2. La liaison de transmission puissance permettant de **motoriser** l'outil par l'énergie du tracteur.

Les liaisons d'accrochage mécanique sont proposées afin de répondre à la problématique d'accrochage sur un tracteur de trois types d'outils : les outils portés, semi-portés et traînés. Les outils portés ont la possibilité d'être soulevés totalement du sol. Le poids total de l'outil est alors reporté sur le tracteur. Les outils semi-portés ne peuvent pas être soulevés du sol et ne tiennent pas en équilibre seuls. Une partie de leur poids repose au sol, l'autre est reporté sur le tracteur. Les outils traînés sont ceux qui, désolidarisés du tracteur, peuvent tenir seuls en équilibre. L'énergie transmise du tracteur à l'outil peut être mécanique, hydraulique, pneumatique, électrique, et/ou électronique. L'énergie mécanique du tracteur est transmise à l'outil par l'arbre de transmission à cardans, qui est animé, côté tracteur, par la prise de force.

Ces liaisons sont à l'origine de nombreux accidents, essentiellement mécaniques. Les résultats d'une étude statistique réalisée par [Ghemraoui, 2009] à partir de données de la CCMSA sur les accidents graves rapportés entre 2000 et 2005 sont présentés à la figure 2.6. Cette analyse montre que l'arbre de transmission à cardans est l'élément le plus dangereux de la liaison tracteur outil. Le Relevage 3 points (ou liaison trois points) vient en seconde position.

Pour illustrer les avancées méthodologiques proposées dans cette recherche, nous nous intéresserons à ces deux systèmes : la Liaison Trois Points (LTP) et l'Arbre de Transmission à Cardans (ATC).

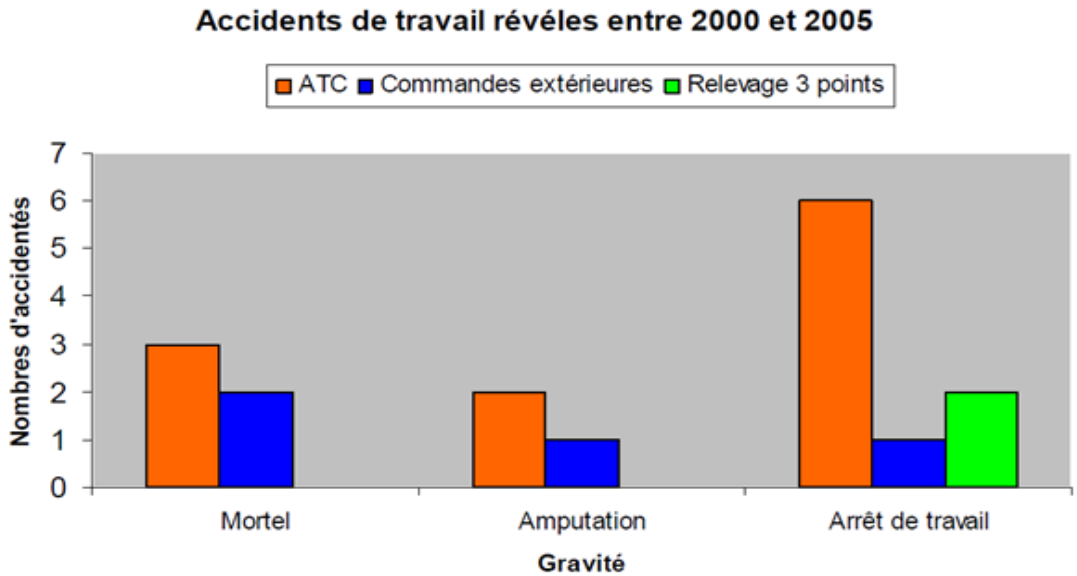
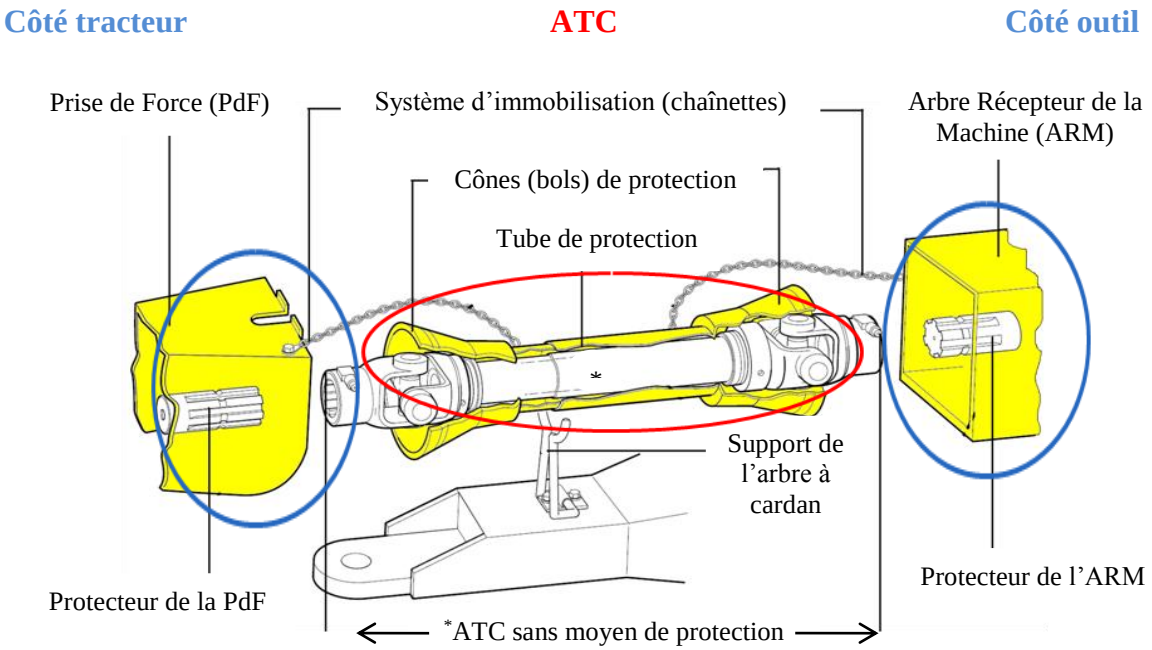


Figure 2.6. Statistiques d'accidents de travail liés à la liaison tracteur-outils [Ghemraoui, 2009].

2.4.2. L'arbre de transmission à cardans

2.4.2.1. Présentation de l'arbre de transmission à cardans

L'Arbre de Transmission à Cardans (ATC) est un dispositif amovible de transmission d'énergie mécanique {(P, C, w) avec (P) la puissance, (w) la vitesse de rotation et (C) le couple transmissible} relié au tracteur par la Prise de Force (PdF), et à l'outil par un Arbre Récepteur Machine (ARM) (figure 2.7).



Note :
- Les éléments blancs à l'intérieur de l'ovale rouge correspondent à l'ATC sans son moyen de protection ;
- Les éléments jaunes et les chaînettes à l'intérieur de ce même ovale correspondent aux moyens de protection de l'ATC.

Figure 2.7. Arbre de transmission à cardans.

Les éléments principaux sur cette figure sont [Banas et al., 2007 ; ISO 5673-1, 2005] :

- **La Prise de Force (PdF)** (arbre externe situé sur le tracteur) permettant de transmettre la puissance de rotation à un outil à l'aide d'un arbre de transmission.
- **Le protecteur de la PdF** (un bouclier) pour protéger la prise de force.
- **L'Arbre de Transmission à Cardans (ATC)** assurant la jonction entre le tracteur et l'outil et la transmission de la puissance de rotation fournie par la PdF du tracteur.
- **Les cônes (ou bols) de protection** protégeant les joints à cardans.
- **Le tube de protection** (constitué de deux parties coulissantes) qui enveloppe totalement l'arbre à cardans afin qu'aucune partie tournante ne soit accessible.
- **Le système d'immobilisation** (chaînettes) empêchant la rotation du protecteur avec l'arbre.
- **Le support de l'arbre à cardans** qui évite de laisser traîner et se détériorer l'enveloppe protectrice de l'arbre lorsque l'outil est dételé.
- **L'arbre Récepteur Machine (ARM)** (arbre externe situé sur l'outil) permettant de transmettre la puissance à un outil.

- **Le protecteur de l'ARM** (un carter) qui assure la protection coté outil.

Le périmètre de notre étude comprend (les éléments cerclés de rouge sur la figure 2.8):

Notons que dans la suite de ce manuscrit, nous appellerons l'arbre à cardan avec moyen de protection : « ATC », l'arbre à cardan sans son moyen de protection : « ATC sans moyens de protection » et le protecteur : « Moyen de protection de l'ATC ».

2.4.2.2. Statistiques d'accidents du travail liés à l'arbre de transmission à cardans

Les résultats d'une étude statistique réalisée par la CCMSA basée sur les accidents de travail entre 2000 et 2011 sont présentés à la figure 2.8. Cette étude indique le nombre d'accidents en fonction des parties du corps impactées.

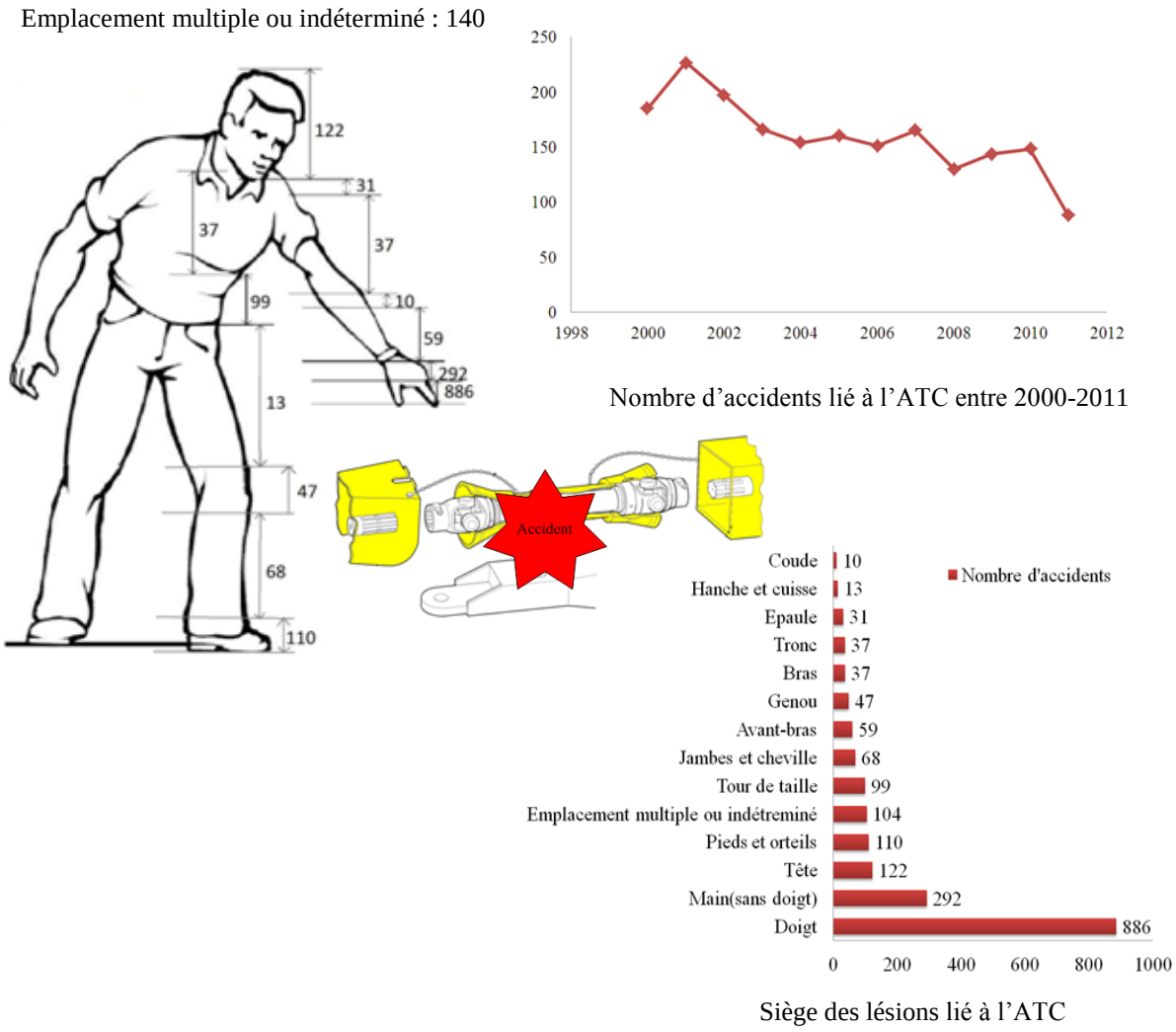


Figure 2.8. Statistiques d'accidents de travail liés à l'ATC [adapté d'une étude réalisée par la CCMSA].

Cette figure met notamment en évidence que, malgré une diminution constante du nombre d'accidents de travail lié à l'ATC, leur nombre reste élevé (1915 accidents entre 2000 et 2011). Les chiffres montrent également que les doigts, les mains, la tête, les pieds et les orteils sont les parties du corps où sont majoritairement localisées les blessures.

2.4.3. La liaison trois points

2.4.3.1. Présentation de la liaison trois points

La Liaison Trois Points (LTP), présente parfois à l'avant et de manière quasi systématique à l'arrière du tracteur, permet d'atteler un outil au tracteur. Elle permet de

soulever l'élément attelé grâce à la puissance hydraulique du tracteur. La figure 2.9 détaille les composants principaux de cette liaison.

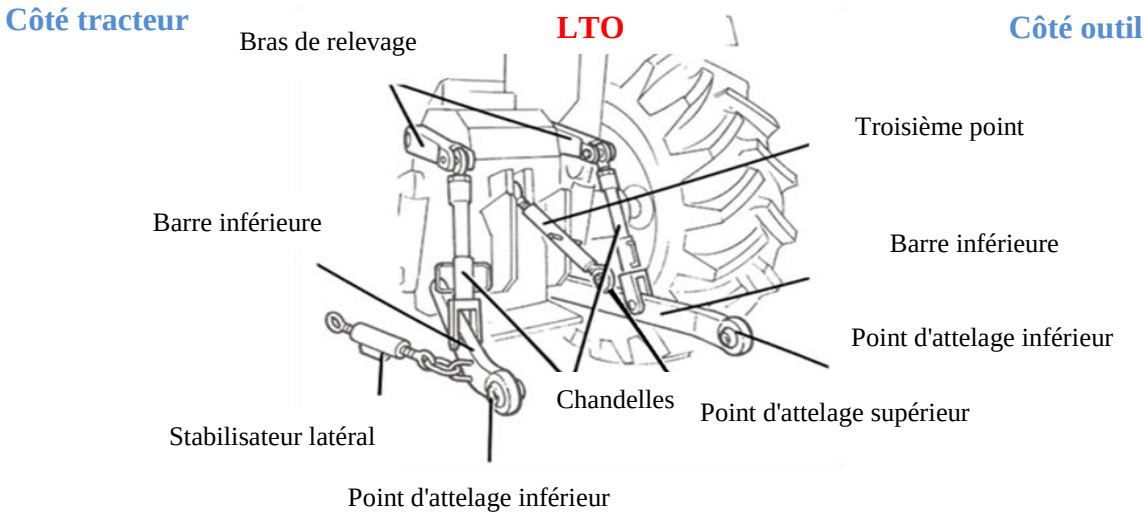


Figure 2.9. Liaison trois points.

La LTP est principalement composée de :

- **Deux barres inférieures**. L'effort du tracteur est transmis par deux « barres inférieures », portant à leur extrémité des rotules de fixation de l'outil. Ces deux barres permettent également la variation de la hauteur de l'ensemble des points par l'intermédiaire de deux chandelles reliées aux bras de relevage.
- **Le troisième point**. La barre supérieure appelée « troisième point » assure la fonction de transfert de charge sur l'essieu avant et la régulation de la profondeur de travail.
- **Deux stabilisateurs latéraux** qui permettent de rigidifier l'ensemble.
- **Deux Chandelles** qui permettent le réglage d'aplomb.

2.4.3.2. Statistiques d'accidents du travail liés à la liaison trois points

D'après une étude statistique réalisée par la CCMSA, à partir des données statistiques des accidents du travail survenus lors des opérations d'attelage et de dételage entre 2000 et 2004, le risque d'accident est avéré et en constante augmentation, avec un accroissement de leur gravité. La figure 2.10 montre le nombre d'accidents sur ces cinq années.

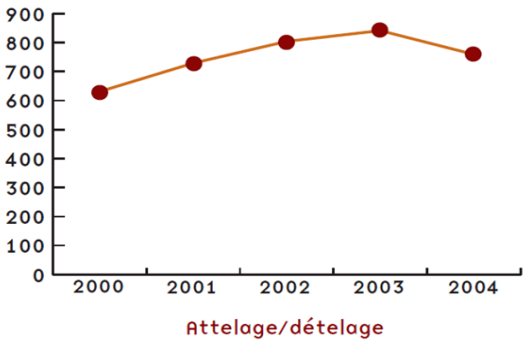


Figure 2.10. Statistiques d'accidents liés à l'attelage et au dételage [Banas, B. et la, 2006].

Cette figure met en évidence que le risque d'accident lié aux opérations d'attelage/dételage augmente alors que globalement le nombre d'accidents du travail diminue, pour les salariés.

2.4.4. Conclusion

Dans cette section, nous avons précisé le contexte applicatif de notre recherche. Il s'agit des liaisons tracteurs outils et plus précisément des liaisons trois points, et de l'arbre de transmission à cardans. Ces liaisons sont à l'origine de nombreux accidents. Notre objectif est de trouver des solutions pour la sécurisation de ces deux types de liaisons tracteurs outils.

Pour y parvenir, nous utilisons la structure type de rapport d'accident proposée précédemment (voir § 2.3) et nous remplissons les champs avec des informations provenant de rapports d'accident classiques. Ce travail est détaillé dans la section qui suit.

2.5. Application : rapports d'accident liés aux liaisons tracteurs-outils

2.5.1. Rapport d'accident lié à l'arbre de transmission à cardans

Nous avons analysé 12 rapports d'accidents mettant en cause les ATC ; accidents qui se sont produits entre 2001 et 2010. Les informations nécessaires à la mise en œuvre de la méthodologie proposée sont données aux parties 5, 6 et 7 du rapport d'accident tel que proposé ici. Ces trois parties sont détaillées ci-dessous pour un rapport d'accident analysé. Il s'agit d'un cas extrême dans le sens où ce rapport était extrêmement détaillé.

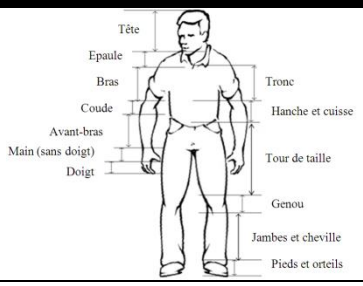
Ce rapport fait treize pages et contient deux parties : les constatations et la qualification juridique des faits. Un autre rédacteur l'aurait certainement rédigé différemment. Voici la structure type de ce rapport d'accident remplie pour les parties 5, 6 et 7 :

Tableau 2.4. Accident impliquant un arbre de transmission à cardans.

5. Dommages

▪ Partie du corps touchée :

. Tête ☐	. Jambes et cheville ☐
. Epaule ☐	. Hanche et cuisse ☐
. Bras ☑	. Coude ☐
. Avant-bras ☐	. Tour de taille ☐
. Genou ☐	. Pieds et orteils ☐
. Tronc ☐	. Emplacement multiple ou indéterminé ☐
. Doigt ☐	
. Main (sans doigt) ☐	



▪ Type de blessure :

. Blessure réversible grâce à des premiers secours ☐
. Blessure réversible grâce à des soins médicaux ☐
. Blessure sans incapacité permanente (Perte de doigts, ...) ☐
. Blessure avec incapacité permanente (Perte d'un œil, d'un bras, …) ☐
. Décès ☑

6. Type de l'accident

▪ Conséquence de l'accident:

. renversement (par une machine mobile) ☐	. choc ☐	. Autre ☐ (spécifiez) ……
. éjection ☐	. injection ☐	
. écrasement ☐	. cisaillement ☐	
. coupure ou sectionnement ☐	. glissade, trébuchement et chute ☐	
. entraînement ou emprisonnement ☐	. perforation ou piqûre ☐	
. happement, enroulement ☑	. suffocation ☐	
. frottement ou abrasion ☐		

▪ Source de l'accident:

. accélération, décélération ☐	. instabilité ☐	. Autre ☐ (spécifiez) ……
. pièces de forme aiguë ☐	. énergie cinétique ☐	
. rapprochement d'un élément en mouvement avec une pièce fixe ☐	. mobilité de la machine ☐	
	. éléments en mouvement ☐	
. éléments coupants ☐	. éléments en rotation ☑	
. éléments élastiques ☐	. surface rugueuse, glissante ☐	
. chute d'objets ☐	. arêtes vives ☐	
. pesanteur ☐	. énergie accumulée ☐	

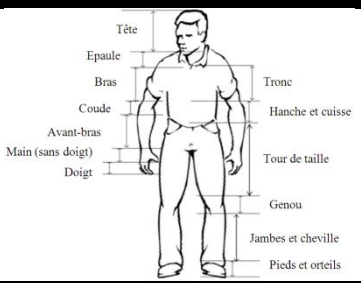
. hauteur par rapport au sol ☐ . vide☐ . pression élevée ☐	
7. Conditions de l'accident	
▪ Conditions de fonctionnement de la machine	▪ Sous-phase de la phase d'usage du système : . Montage, installation, mise en service ☐ . Démontage, mise hors service ☐ . Transport ☐ . Maintenance ☐ . Utilisation ☑
	▪ Tâche : . Alimentation de la machine☐ . Maintenance corrective☐ . Apprentissage/programmation☐ . Manipulation de consommable☐ . Arrêt de la machine☐ . Nettoyage et entretien☐ . Arrêt de la machine en cas d'urgence☐ . Recherche de défauts/de pannes (intervention de l'opérateur) ☐ . Changement de processus/outil☐ . Redémarrage après arrêt imprévu☐ . Démarrage☐ . Réglage☐ . Essais☐ . Reprise du fonctionnement après bourrage ou blocage☐ . Maintenance préventive☐ . Retrait de consommable de la machine☐ . Autre ☑ (spécifiez) …… *la victime avec l'autre personne faisaient du béton d'une bétonnière entrainée par un arbre de transmission à cardan relié à la prise de force du tracteur (la victime procédait au graissage de la couronne et (ou) du pignon de la bétonnière.*
	▪ État de la machine : *Est-ce que la machine accomplissait la fonction prévue ?* Oui☑Non☐ si non spécifiez……. *fonctionnement normal mais l'arbre de transmission dans un état de délabrement*
▪ Comportement et capacités de l'opérateur	▪ Comportement de l'opérateur : *Est-ce que l'opérateur utilisait la machine en respectant la procédure et les consignes de sécurités fournis par le constructeur ?* Oui ☐ Non☑ si non spécifiez *non respect de la consigne de sécurité (l'article R 4321-1 du code du travail qui précise la nécessité de protecteur pour les éléments mobiles de transmission d'énergie)*
▪ Conditions environnementales	▪ Capacités de l'opérateur : . Formation (opérateur avait reçu une formation adéquate pour savoir utiliser la machine) : Oui☑Non☐ . Expérience (opérateur était avec expérience): Oui☑ Non☐ . Etat physique (opérateur était sans capacités physiques limitées) : Oui☑ Non☐ . Aptitude (opérateur était sans le stress, la fatigue, les préoccupations, etc.): Oui☑ Non☐ ▪ Présence de tiers (autre personne était présentes dans l'environnement de travail) : Oui☑ Non☐ ▪ Environnement fermé ou ouvert (l'environnement de travail était ouvert) : Oui☑ Non☐ ▪ Milieu structuré ou naturel (l'environnement de travail était naturel): Oui☑ Non☐

Remarque : Nous n'avions pas d'informations sur les conditions environnementales et la capacité de l'opérateur dans le rapport d'accident. Nous avons donc complété le rapport avec des données inventées.

2.5.2. Rapport d'accident lié à la liaison trois points

Dans cette section, nous présentons les parties dommages, type d'accident et conditions de l'accident d'une structure type de rapport d'accident dont les champs ont été remplis à partir d'un rapport d'accident impliquant une LTP (tableau 2.5).

Tableau 2.5. Accident impliquant une liaison trois points.

5. Dommages		
▪ Partie du corps touchée : . Tête ☐ . Epaule ☐ . Bras ☐ . Avant-bras☐ . Genou ☐ . Tronc ☐ . Doigt ☐ . Main (sans doigt) ☐	. Jambes et cheville ☐ . Hanche et cuisse ☐ . Coude ☐ . Tour de taille ☐ . Pieds et orteils ☐ . Emplacement multiple ou indéterminé ☑	
▪ Type de blessure :		

. Blessure réversible grâce à des premiers secours ☐
. Blessure réversible grâce à des soins médicaux ☐
. Blessure sans incapacité permanente (Perte de doigts, ...) ☑
. Blessure avec incapacité permanente (Perte d'un œil, d'un bras, …) ☐
. Décès ☐

6. Type de l'accident

▪ Conséquence de l'accident:

. renversement (par une machine mobile) ☐	. choc ☐	. Autre ☐ (spécifiez) ……
. éjection ☐	. injection ☐	
. écrasement ☑	. cisaillement ☐	
. coupure ou sectionnement ☐	. glissade, trébuchement et chute ☐	
. entraînement ou emprisonnement ☐	. perforation ou piqûre ☐	
. happement, enroulement ☐	. suffocation ☐	
. frottement ou abrasion ☐		

▪ Source de l'accident:

. accélération, décélération ☐	. instabilité ☐	. Autre ☑ (spécifiez) énergie potentille
. pièces de forme aiguë ☐	. énergie cinétique ☐	
. rapprochement d'un élément en mouvement avec une pièce fixe ☐	. mobilité de la machine ☐	
	. éléments en mouvement ☐	
. éléments coupants ☐	. éléments en rotation ☐	
. éléments élastiques ☐	. surface rugueuse, glissante ☐	
. chute d'objets ☐	. arêtes vives ☐	
. pesanteur ☐	. énergie accumulée ☐	
. hauteur par rapport au sol ☐	. vide ☐	
. pression élevée ☐		

7. Conditions de l'accident

▪ Conditions de fonctionnement de la machine	▪ Sous-phase de la phase d'usage du système : . Montage, installation, mise en service ☑ . Démontage, mise hors service ☐ . Transport ☐ . Maintenance ☐ . Utilisation ☐
	▪ Tâche : . Alimentation de la machine ☐ . Maintenance corrective ☐ . Apprentissage/programmation ☐ . Manipulation de consommable ☐ . Arrêt de la machine ☐ . Nettoyage et entretien ☐ . Arrêt de la machine en cas d'urgence ☐ . Recherche de défauts/de pannes (intervention de l'opérateur) ☐ . Redémarrage après arrêt imprévu ☐ . Changement de processus/outil ☐ . Réglage ☐ . Reprise du fonctionnement après bourrage ou blocage ☐ . Démarrage ☐ . Retrait de consommable de la machine ☐ . Essais ☐ . Autre ☑ (spécifiez) attacher outil au tracteur . Maintenance préventive ☐
	▪ État de la machine : *Est-ce que la machine accomplissait la fonction prévue ?* Oui ☑ Non ☐ si non spécifiez……
▪ Comportement et capacités de l'opérateur	▪ Comportement de l'opérateur : *Est-ce que l'opérateur utilisait la machine en respectant la procédure et les consignes de sécurités fournis par le constructeur ?* Oui ☑ Non ☐ si non spécifiez
	▪ Capacités de l'opérateur : . Formation (opérateur avait reçu une formation adéquate pour savoir utiliser la machine) : Oui ☑ Non ☐ . Expérience (opérateur était avec expérience): Oui ☑ Non ☐ . Etat physique (opérateur était sans capacités physiques limitées) : Oui ☑ Non ☐ . Aptitude (opérateur était sans le stress, la fatigue, les préoccupations, etc.): Oui ☑ Non ☐
▪ Conditions environnementales	▪ Présence de tiers (autre personne était présentes dans l'environnement de travail) : Oui ☑ Non ☐ ▪ Environnement fermé ou ouvert (l'environnement de travail était ouvert) : Oui ☑ Non ☐ ▪ Milieu structuré ou naturel (l'environnement de travail était naturel): Oui ☑ Non ☐

Remarque : Nous n'avions pas d'informations sur les conditions environnementales et la capacité de l'opérateur dans le rapport d'accident. Nous avons donc complété le rapport avec des données inventées.

2.6. Conclusion

Dans ce chapitre, nous avons proposé une structure type de rapport d'accident. Elle est composée de « neuf + deux » parties :

1. Informations sur la victime ;
2. Informations sur les circonstances de l'accident ;
3. Informations sur les témoins ;
4. Informations sur le système en cause ;
5. Dommages ;
6. Type d'accident ;
7. Conditions de l'accident ;
8. Mesures correctives ;
9. Informations sur les premiers soins apportés **;**
10. Signature ; et
11. Annexe.

Le rapport contient trois parties essentielles à la poursuite de la démarche que nous proposons :

- La partie « **Dommages** » (5) qui précise la partie du corps touchée et décrit la blessure ;
- La partie « **Type d'accident** » (6) qui permet de déterminer les conséquences et la source du phénomène dangereux ;
- La partie « **Conditions de l'accident** » (7) qui décrit les conditions de fonctionnement du système, le Comportement et capacités de l'opérateur et les conditions environnementales.

Nous avons également présenté le contexte applicatif de notre recherche à savoir les liaisons tracteurs outils et plus précisément la liaison trois points et l'arbre de transmission à cardans. Enfin les parties dommages, type d'accident et conditions de l'accident de la structure type de rapport d'accident proposée ont été renseignées pour deux cas d'accident impliquant un ATC et pour deux cas impliquant une LTP. La structure proposée il permet d'accueillir ensemble des informations prévues pour ces deux cas d'applications.

Les chapitres suivants détaillent comment utiliser ces informations.

Chapitre 3. Ingénierie inverse fonctionnelle pour la sécurité

3.1. Introduction

Notre principal objectif est de proposer un processus itératif d'aide à la décision pour l'intégration de la sécurité tout au long du processus de conception en nous basant essentiellement sur l'opérationnalisation des trois cas d'emploi d'IRAD. Pour y parvenir, nous proposons de développer deux démarches complémentaires : une démarche d'ingénierie inverse fonctionnelle pour la sécurité (ou FRES pour Functional Reverse Engineering for Safety) et une démarche de réingénierie fonctionnelle pour la sécurité (ou FR2ES pour Functional REEngineering for Safety). Ce chapitre présente la première approche ; approche essentielle pour l'opérationnalisation du premier cas d'emploi d'IRAD. Elle est basée sur l'analyse du Retour d'EXpérience (REX) et plus précisément sur l'analyse d'un rapport formel d'accident.

La démarche FRES doit fournir, avant tout, une aide à l'extraction et à la formalisation des connaissances sur les accidents ainsi que sur l'aspect technique d'un système existant à partir de l'analyse d'un rapport formel d'accident. Cette démarche est basée sur trois points de vue :

- Point de vue **sécurité**, la démarche FRES permet d'extraire et de formaliser les connaissances sur les accidents en analysant des rapports formels d'accidents. Dans le chapitre 2, la partie formalisation a été traitée. Dans ce chapitre, est détaillée la partie analyse permettant de définir et comprendre les causes d'accidents. Autrement dit, la question que l'on se pose est : *Comment analyser les accidents et comment en déterminer les causes à partir du rapport d'accident ?*
- Point de vue **conception**, la démarche FRES permet d'extraire les connaissances sur la conception à partir de l'analyse d'un rapport formel d'accident. Il sera donc nécessaire de considérer les six phases du processus de conception de la méthode IRAD. L'idée est de tenter de répondre à la question suivante : *Comment extraire, formaliser et analyser les connaissances sur la conception d'un système existant afin de les réutiliser dans sa reconception ?*
- Point de vue **aide à la décision**, la démarche FRES permet de déterminer l'étape de la conception où intervenir pour limiter les risques d'accident. Basée sur un indicateur donnant le niveau de sécurité d'un système, la démarche aidera le concepteur à choisir les solutions les plus sécuritaires dans le processus de reconception sécuritaire.

Dans le chapitre 1, nous avons présenté la vue globale du processus de conception sécuritaire que nous proposons, représentée sous la forme d'un diagramme IDEF0 (figure 1.14). La fonction A0 « Concevoir de manière sécuritaire » comporte deux sous-fonctions (figure 1.17) : la sous-fonction A1 « Appliquer la démarche FRES » pour définir le processus d'ingénierie inverse fonctionnelle pour la sécurité et la sous fonction A2 « Appliquer la démarche FR2ES » pour intégrer la sécurité durant le processus de conception. Selon ce qui est présenté plus-haut, la sous-fonction A1 se décompose en trois sous-fonctions : « Extraire les connaissances sur les accidents », « Extraire les connaissances sur la conception » et « Evaluer la sécurité » (figure 3.1). À partir d'un problème de sécurité signalé dans un rapport d'accident, nous cherchons à extraire les connaissances sur les accidents et les connaissances sur la conception du système, à identifier le type de risque (C2, C4 ou C6) et à mesurer le niveau de sécurité de la partie du système impliquée dans l'accident. Dans ce chapitre, nous présentons les fonctions A11 et A12. La fonction A13, « Evaluer la sécurité », très importante dans le cadre de nos travaux, est traitée dans le chapitre suivant (chapitre 4).

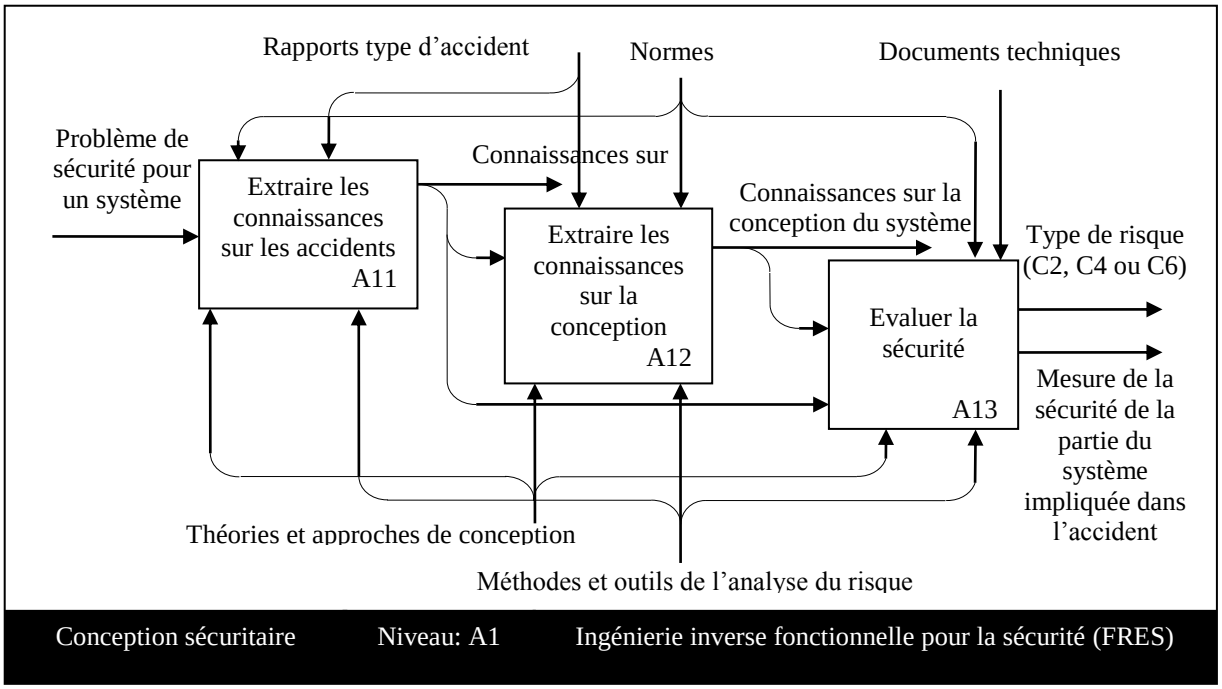


Figure 3.1. Diagramme IDEF0 niveau A1 du processus de conception sécuritaire.

Ce chapitre comporte deux sections principales. Dans un premier temps, la section 3.2 propose une approche d'extraction des connaissances sur les accidents à partir de l'analyse des rapports d'accidents. Dans un second temps, la section 3.3 propose le développement d'une approche d'extraction des connaissances de la conception de la partie du système impliquée dans l'accident. Chacune de ces deux sections comporte cinq sous sections : l'introduction, l'état de l'art, le développement de l'approche, l'application de l'approche proposée sur l'Arbre de Transmission à Cardans (ATC), une conclusion, une discussion et les perspectives. Enfin, nous clôturons ce chapitre par une conclusion.

3.2. Développement d'une approche d'extraction de connaissances sur l'accident par l'analyse des rapports d'accidents

3.2.1. Introduction

Comprendre les causes des accidents est une étape essentielle dans la conception pour la sécurité. La question importante est de savoir *Comment analyser les accidents et déterminer leurs causes ?* L'objectif de la présente partie est de montrer comment répondre à cette question. Cet objectif se base essentiellement sur l'opérationnalisation du premier cas d'emploi d'IRAD.

Cette partie est organisée en six sections. Tout d'abord, la section 3.3.2 présente un état de l'art sur les méthodes d'identification des phénomènes dangereux des deux points de vue, normatif et scientifique. La section 3.3.3 porte sur le développement de l'approche permettant l'analyse d'un rapport d'accident. Ensuite, la section 3.3.4 traite de l'évaluation de l'approche développée par son application à l'analyse des rapports d'accident mettant en cause l'Arbre de Transmission à Cardans (ATC). Finalement, la section 3.3.5 présente la conclusion et les perceptives de cette partie.

3.2.2. Etat de l'art sur l'identification des phénomènes dangereux et leurs causes

Pour quelles raisons faut-il identifier les phénomènes dangereux ? Un dommage est la conséquence d'un accident. Quand une personne est exposée à un phénomène dangereux, cela constitue une situation dangereuse. Le déclenchement d'un événement dangereux dans cette

situation peut mener à un dommage. Un dommage est la conséquence éventuelle d'un événement dangereux. En effet, les éléments entrainant un dommage sont le phénomène dangereux, la situation dangereuse et l'événement dangereux. Notre travail doit donc se focaliser sur ces éléments que nous appelons « conditions dangereuses » et les méthodes permettant leur identification et leur analyse. Cette section aborde la comparaison de quelques méthodes sélectionnées pour l'analyse des accidents et de leurs causes.

3.2.2.1. Identification des phénomènes dangereux du point de vue normatif

Selon la norme [FD ISO/TR 14121-2, 2008], la plupart des méthodes d'identification des phénomènes dangereux suivent l'une des deux approches présentées à la figure 3.2. En effet, cette figure montre la relation entre « dommage » et « phénomène dangereux ». Cette approche est basée sur la recherche de réponses à deux questions :

- *Quel phénomène dangereux pourrait causer un dommage ?* (par l'approche de haut en bas) ;
- *Dans quelles conditions le phénomène dangereux peut causer un dommage ?* (par l'approche de bas en haut).

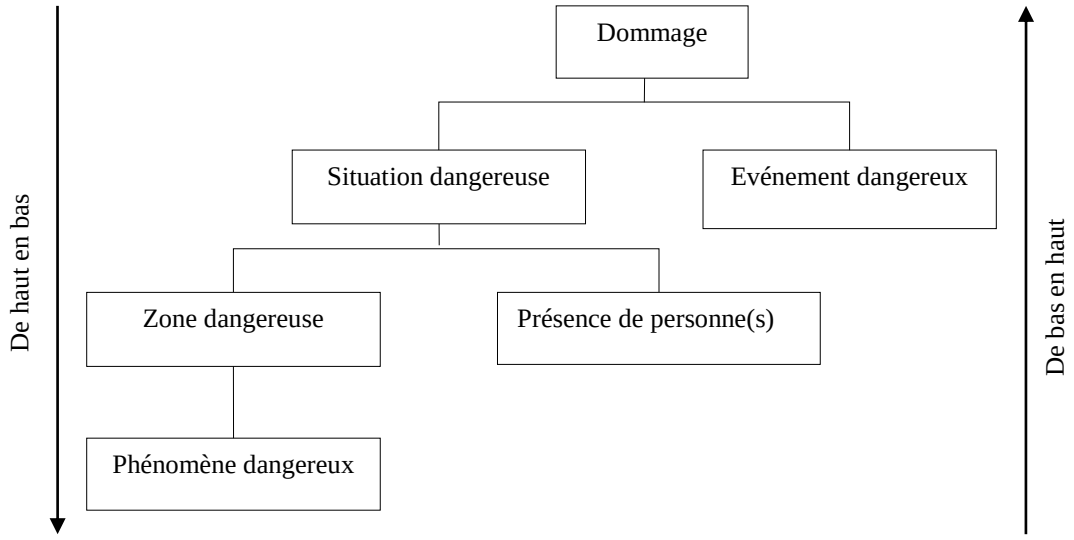


Figure 3.2. Identification structurée des phénomènes dangereux [FD ISO/TR 14121-2, 2008].

L'approche de haut en bas : Cette approche permet d'identifier le phénomène dangereux par l'analyse du dommage. L'analyse du dommage permet d'identifier la situation dangereuse puis la zone dangereuse en prenant en compte l'évènement dangereux et enfin le phénomène dangereux par la prise en compte de la présence d'une (de) personne(s).

L'approche de bas en haut : Cette approche identifie le dommage par l'analyse du phénomène dangereux. Cette approche débute par l'analyse du phénomène dangereux qui permet d'identifier la zone dangereuse. Ensuite, on examine la zone dangereuse en prenant en compte la présence de personne(s) de manière à déterminer la situation dangereuse. Enfin, l'analyse de la situation dangereuse combinée à la prise en compte des potentiels évènements dangereux permet de déterminer le dommage.

3.2.2.2. Identification des phénomènes dangereux du point de vue scientifique

De nombreuses méthodes d'analyse des phénomènes dangereux ont été développées, chacune avec leurs avantages et leurs inconvénients. L'objectif de ces méthodes d'analyse est de faire le choix entre trois mesures : la protection, la prévention ou l'atténuation. Dans la littérature, elles sont généralement classées en deux groupes [Popovi et Vasić, 2008]:

- les méthodes logiques inductives qui permettent, à partir des causes, de déduire le danger résultant ;
- les méthodes logiques déductives qui permettent, à partir du danger, de remonter vers les causes possibles.

La figure 3.3 montre les relations et les divergences entre ces deux concepts. Le tableau 3.1 permet de comparer ces deux types d'analyse.

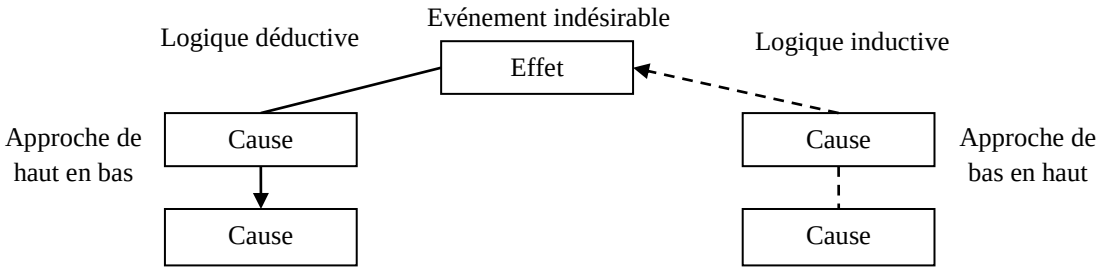


Figure 3.3. Relation entre analyses inductives et déductives [Popovi et Vasić, 2008].

Tableau 3.1. Caractéristiques des analyses inductives et déductives. Adapté de [Popovi et Vasić, 2008].

Déductive	**Inductive**
- Comment / pouvoir ? - Comment peut-il se passer … ? - Consiste à formuler une hypothèse afin d'en déduire des conséquences observables permettant d'en déterminer la validité - L'événement final est présumé et les circonstances qui pourraient provoquer cet événement final sont ensuite recherchées	- Que / si ? - Que se passe-t-il si…? - Consiste à décrire différents événements qui pourraient se transformer en accident - La défaillance d'un élément est présumée. La méthode détermine les évènements que cette défaillance pourrait provoquer

Un des éléments essentiels de nos travaux porte sur la recherche des causes d'accidents afin d'aider le concepteur à définir des exigences de sécurité pour les éliminer. Parmi l'ensemble des méthodes d'analyse de phénomènes dangereux, celles basées sur la construction d'un arbre permettent d'analyser les accidents afin de définir leurs causes ou leurs conséquences possibles. Ci-dessous, nous nous inspirons des articles de [Marhavilas et al., 2011] et de [Popovi et Vasić, 2008] pour présenter et comparer trois de ces méthodes : l'analyse par l'arbre d'événements, l'analyse par l'arbre de défaillances et l'analyse par l'arbre des causes.

Analyse par arbre d'événements : L'objectif de la méthode de l'arbre d'événements (figure 3.4) est d'« *identifier et analyser la fréquence des dangers moyennant un raisonnement inductif pour convertir différents événements initiateurs en conséquences éventuelles relatives au fonctionnement ou à la défaillance des dispositifs techniques/humains/organisationnels de sécurité* » [Mazouni, 2008]. Selon [M2OS, 2009], l'analyse par l'arbre d'événements demande de réaliser les étapes suivantes :

- Identifier l'événement initiateur ;
- Identifier les mécanismes de prévention ;
- Construire l'arbre ;
- Estimer les probabilités de chaque branche ;
- Estimer les probabilités de chaque conséquence ;
- Hiérarchiser les conséquences.

Analyse par arbre de défaillances : Cette méthode fournit une représentation graphique de l'ensemble des combinaisons d'événements pouvant aboutir à un accident. Elle

permet donc d'identifier les causes des situations dangereuses par une représentation graphique [Mazouni, 2008]. Un arbre de défaillances est constitué d'un événement sommet, d'un événement base, d'événements intermédiaires, et d'événements conditionnels. Chaque événement est représenté par un symbole. Les événements sont reliés par des portes logiques (ET/OU), comme montré à la figure 3.4. Cette méthode demande de :

- Identifier l'évènement sommet ;
- Identifier le premier niveau des sources des phénomènes dangereux ;
- Lier le premier niveau des sources de danger à un évènement sommet par des portes logiques ;
- Identifier le second niveau des sources de danger ;
- Lier le second niveau des sources de danger à un évènement sommet par portes logiques ;
- Continuer l'analyse *jusqu*'aux évènements de base dont l'analyse s'avère impossible ou sans intérêt.

Analyse par arbre des causes : L'arbre des causes est utilisé pour la représentation d'un accident sous la forme d'un arbre (figure 3.4). Cette méthode propose de décomposer chaque événement jusqu'à ce que tous les événements et conditions élémentaires cités comme ayant contribué à l'accident soient intégrés. La méthode est identique à celle de l'analyse par arbre de défaillances. Ces deux arbres ont la même représentation sauf que, dans le cas de l'arbre des causes, il n'y a pas de 'OU' et que tous les événements et les causes se représentent par des rectangles ou des ronds. Leurs objectifs sont différents. L'arbre de défaillances débute par un évènement non désiré potentiel et permet de rechercher les causes, tandis que l'arbre des causes est basé sur un évènement non désiré réel, et recherche des causes impliquées. On peut donc dire que l'arbre des causes est, en quelque sorte, une partie de l'arbre de défaillances.

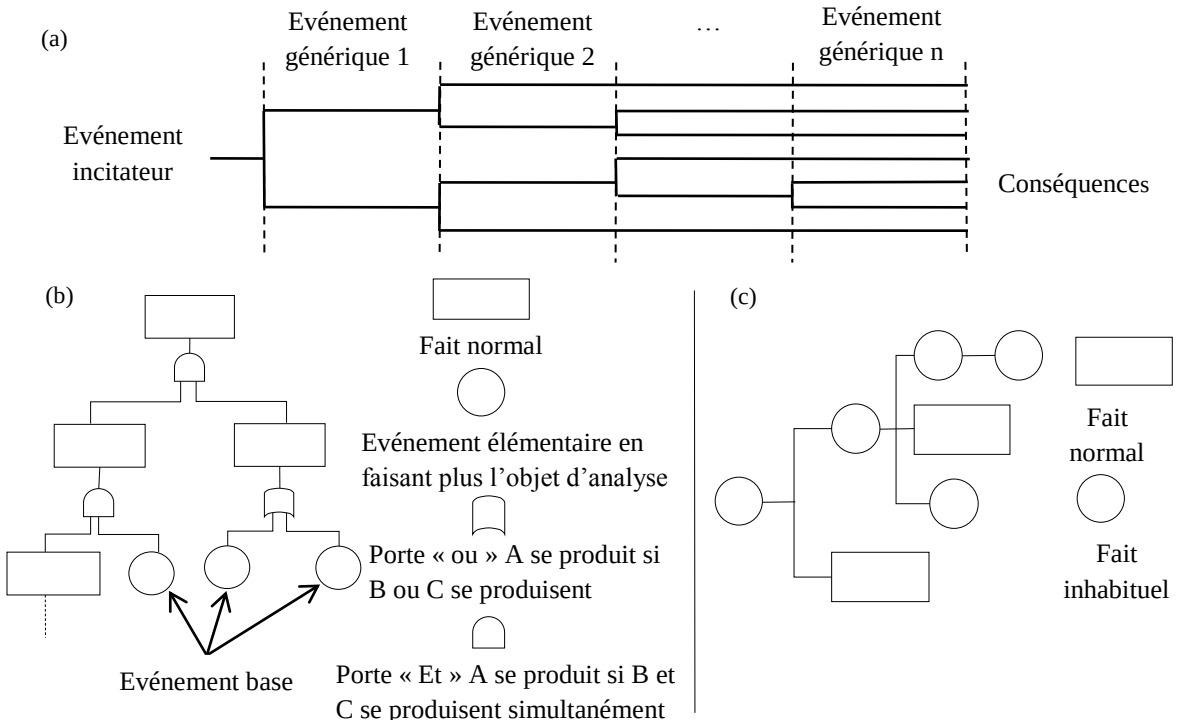


Figure 3.4. (a) l'arbre d'événements (b) l'arbre de défaillances et (c) l'arbre des causes.

3.2.2.3. Synthèse et positionnement par rapport à nos objectifs

Le tableau 3.2 résume les apports des méthodes et permet leur comparaison. L'arbre d'événements permet d'identifier les conséquences possibles d'un événement. L'arbre de défaillances est mis en œuvre afin de rechercher les causes d'un évènement non désiré potentiel. L'arbre des causes est basé sur un évènement non désiré réel. Son application permet d'analyser les causes impliquées. Parmi celles-ci et sachant que la recherche des causes des phénomènes dangereux est notre objectif premier, les méthodes de l'arbre de défaillances et de l'arbre des causes semblent les plus appropriées à notre travail. De plus, l'arbre de défaillances a l'avantage de pouvoir traiter un type d'accident contrairement à l'arbre des causes dont l'analyse se fait sur un accident en particulier.

Tableau 3.2. Synthèse des méthodes d'identification des phénomènes dangereux et de leurs causes (adaptée de [Popovi et Vasić, 2008]).

Méthode	**Inductive/ Déductive**	**Identification des phénomènes dangereux**	**Identification des causes racines**	**Objectifs**
Arbre d'Evénements	Déductive	Partiellement	Partiellement	Identifier et évaluer les conséquences possibles d'un événement initiateur selon les circonstances ou dysfonctionnements avec lesquels il se combine
Arbre de Défaillances	Déductive	Partiellement	Oui	Identifier les causes techniques ou opérationnelles à une situation
Arbre des Causes	Déductive	Partiellement	Partiellement	Réunir dans une représentation synthétique et logique tous les éléments ayant contribué à un incident avéré

3.2.3. Développement d'une approche d'extraction de connaissances sur l'accident par l'analyse des rapports d'accidents

Dans cette section, nous voulons développer une approche d'analyse d'accidents en nous basant sur la structure type des rapports d'accident développée dans le chapitre 2. Notre objectif est d'extraire des informations permettant de définir, décrire et comprendre les causes d'accident. Ces informations s'avèrent utiles afin d'améliorer la sécurité dans le processus de reconception du système ou la conception d'un système similaire.

Avant de décrire l'approche, il convient de préciser ici que selon la Directive Machines 2006/42/CE, Annexe I, 1.1.1 « personne » signifie l'opérateur, c'est-à-dire, la(les) personne(s) chargée(s) d'installer, de faire fonctionner, de régler, d'entretenir, de nettoyer, de dépanner ou de déplacer une machine [2006/42/CE]. Toute autre personne que cet opérateur (travaillant à proximité, …), est considérée comme faisant partie de l'environnement. Ainsi, dans notre travail, nous considérons que, pour chaque système, il n'y a qu'un seul opérateur.

Dans la structure type des rapports d'accident (voir chapitre 2, §2.3.4), les parties suivantes permettent de définir, décrire et comprendre les causes de l'accident :

5. Le dommage qui précise la partie du corps touchée et décrit la blessure.
6. Le type d'accident qui précise de quel type est l'accident. Un type d'accident regroupe les accidents ayant les mêmes conséquences et les mêmes sources du phénomène dangereux et qui sont causés par le même type de système ou sous-système.
7. Les conditions de l'accident qui décrivent les conditions de fonctionnement du système, du comportement et des capacités de l'opérateur et les conditions environnementales.

Il convient ensuite d'identifier les conditions dangereuses qui ont entrainé l'accident à partir de ces informations.

3.2.3.1. Identification des conditions dangereuses de l'accident par construction de l'Arbre des Causes

Dans cette étape, nous nous basons sur les informations obtenues à l'étape précédente afin de définir et décrire les causes de l'accident. Comme précisé dans le §3.2.2, nous avons opté pour l'Arbre des Causes (AdC) pour analyser et représenter chaque accident. L'AdC est basé sur un évènement non désiré réel et permet d'identifier les causes impliquées.

L'idée ici est de construire l'AdC comme précisé au §3.2.2.2 dans un premier temps puis de le comparer avec l'AdC type présenté ci-dessous (figure 3.5). Cette comparaison doit permettre d'identifier le dommage (présent au 1er niveau de l'AdC), l'évènement dangereux (présent au 2ème niveau), le phénomène dangereux (dont la source et la conséquence sont présents aux niveaux 2 et 3) et la situation dangereuse (présente au 3ème niveau).

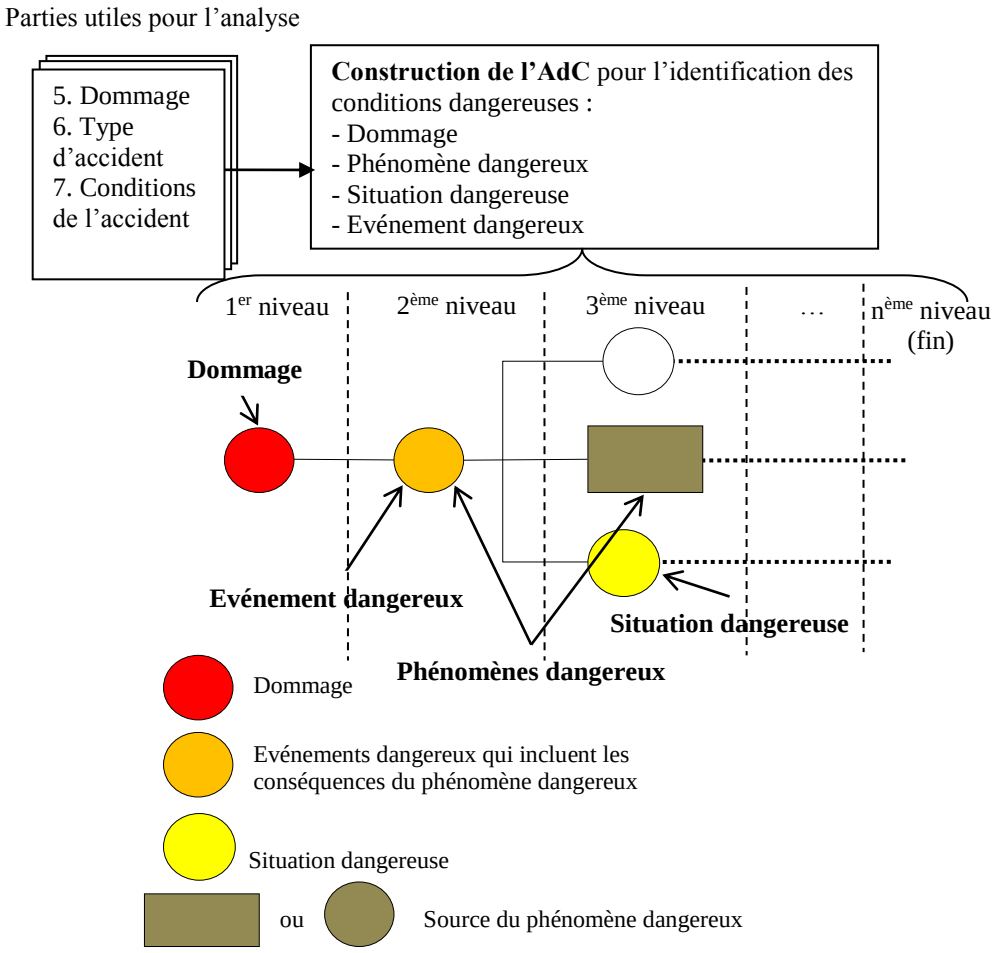


Figure 3.5. Arbre des Causes type et identification des conditions dangereuses.

3.2.3.2. Identification de toutes les causes potentielles par construction de l'Arbre de Défaillances

Les causes possibles d'un accident sont (figure 3.6.) :

- Une défaillance ou une mauvaise conception du système (conception non sécuritaire) ;
- Un facteur non prévu lié à l'humain ;
- Un facteur non prévu lié à l'environnement.

On propose ici la mise en œuvre de l'Arbre de Défaillances (AdD) de manière à regrouper toutes les causes potentielles de ce type d'accident. Comme nous l'avons cité dans l'état de l'art, l'AdC est, en quelque sorte, une branche de l'AdD. Donc, en regroupant les différents AdCs, et en cherchant, dans les documents techniques, les autres causes potentielles, nous pouvons établir l'AdD.

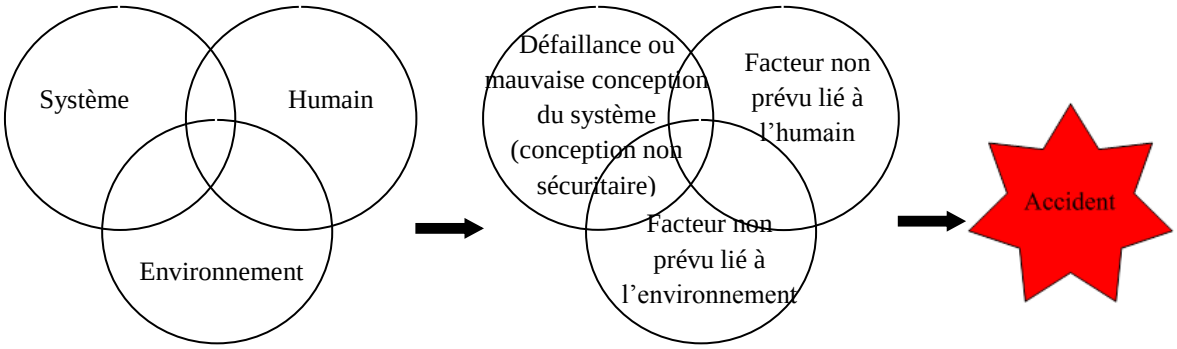


Figure 3.6. Causes d'accident.

3.2.3.3. Conclusion sur l'approche proposée pour l'analyse d'un rapport type d'accident

Dans le but d'opérationnaliser la méthode IRAD, nous avons présenté une approche d'extraction des connaissances sur l'accident basée sur l'analyse d'une structure type des rapports d'accident. Le point de départ de cette approche est l'identification d'un problème de sécurité, lié à un système, cité dans un rapport formel d'accident. En se basant sur les informations disponibles dans ses parties 5, 6 et 7, nous proposons, dans un premier temps, de construire l'Arbre des Causes (AdC) afin de définir les conditions dangereuses qui correspondent aux éléments entrainant le dommage. Ensuite, nous utilisons l'Arbre de Défaillances (AdD) afin d'identifier toutes les causes potentielles correspondant au type d'accident analysé.

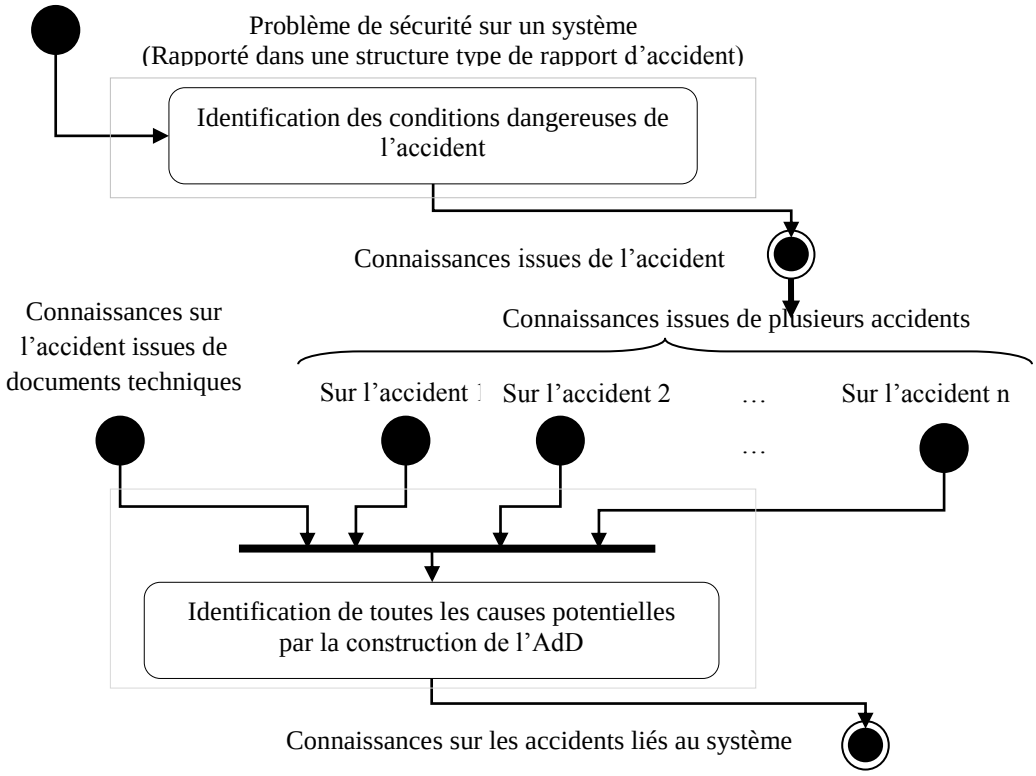


Figure 3.7. Approche d'extraction des connaissances sur les accidents basée sur l'analyse d'un rapport type d'accident.

Les résultats apportés par la mise en œuvre de l'approche sont différents types de connaissances sur les accidents, et notamment les conditions dangereuses: le phénomène dangereux, la situation dangereuse et l'événement dangereux. La figure 3.7 illustre cette approche d'analyse d'un rapport type d'accident. La section suivante a pour but la validation de cette approche en l'appliquant sur l'Arbre de Transmission à Cardans (ATC).

3.2.4. Application : extraction de connaissances issues d'un accident lié à l'ATC

Cette section a pour but de décrire l'extraction des connaissances issues d'un rapport d'accident lié à l'ATC. Ce rapport est été présenté dans le chapitre 2, §2.5.1. Nous avons identifié le dommage, le type d'accident et les conditions de l'accident impliquant l'ATC pour cet accident. Les résultats sont résumés dans le tableau ci-dessous :

Tableau 3.3. Dommage, type d'accident et conditions de l'accident impliquant l'ATC.

	Accident
Dommage	*Décès*
Type d'accident	- Conséquence d'accident: *happement* - Source d'accident: *éléments en rotation*
Conditions de l'accident	- Sous-phase de la phase d'usage du système: *Utilisation* - Tâche : *la victime avec l'autre personne faisaient du béton d'une bétonnière entrainée par un arbre de transmission à cardan relié à la prise de force du tracteur (la victime procédait au graissage de la couronne et (ou) du pignon de la bétonnière.* - État de la machine : *fonctionnement normal mais l'arbre de transmission dans un état de délabrement* - Comportement de l'opérateur : *non-respect de la consigne de sécurité (l'article R 4321-1 du code du travail qui précise la nécessité de protecteur pour les éléments mobiles de transmission d'énergie)* - Capacités de l'opérateur : *opérateur avait reçu une formation adéquate pour savoir utiliser la machine,* *il était avec expérience,* *il était sans capacités physiques limitées et sans stress, ni fatigue, ni préoccupations, etc.* - Présence de *tiers* - Environnement *ouvert* - Milieu *naturel*

3.2.4.1. Identification des conditions dangereuses de l'accident par construction de l'Arbre des Causes

Après avoir identifié le dommage, le type de l'accident et extrait les conditions de l'accident impliquant l'ATC, nous construisons l'Arbre de Causes de cet accident (figures 3.8) jusqu'au 4^{ième} niveau.

L'analyse de ce rapport montre que les accidents se traduisent par le happement de l'opérateur autour de l'ATC équipé d'un protecteur cassé lors de la sous-phase d'utilisation de la phase d'usage.

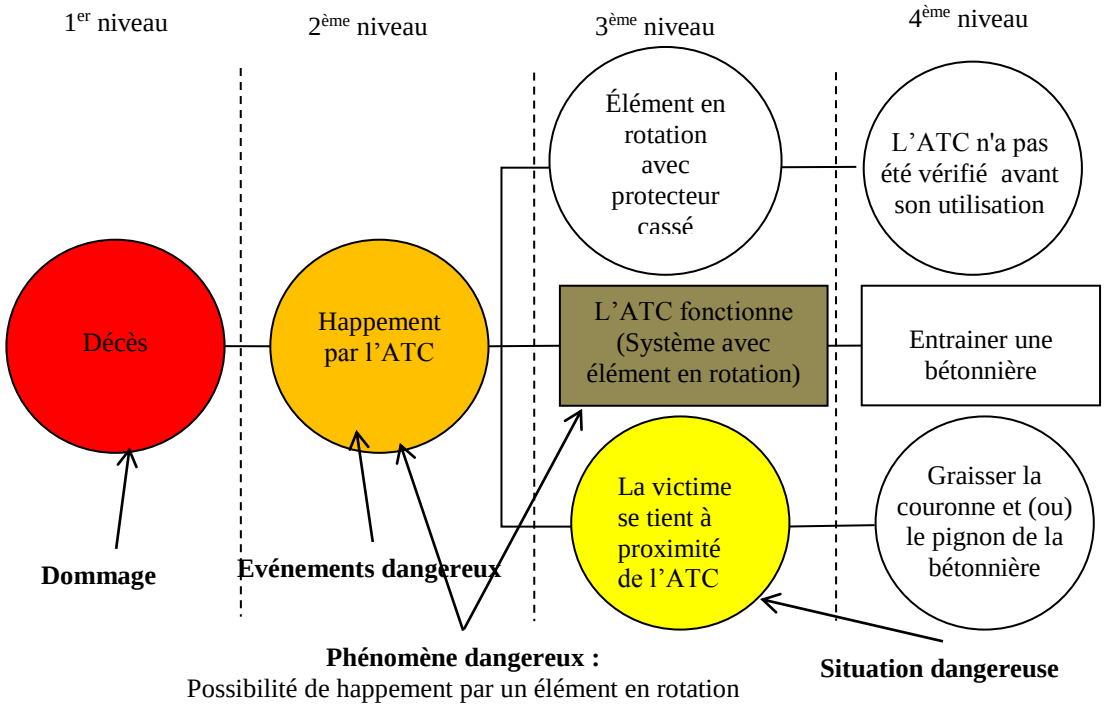


Figure 3.8. Définition des conditions dangereuses de l'ATC par l'AdC.

3.2.4.2. Identification de toutes les causes potentielles pour l'accident de happement par construction de l'AdD

Afin de construire l'Arbre de Défaillances (AdD), on passe de l'étude des rapports d'accidents à une étude d'un type d'accident : « accident de happement par l'arbre à cardan ».

L'analyse de plusieurs accidents impliquant un ATC indique que les faits « Homme se tenant à proximité de l'ATC », « ATC fonctionne », et « Absence de protecteur ou protecteur endommagé ou bien mal ajusté » peuvent causer le « happement » (figure 3.9) [Sadeghi et al., 2013a].

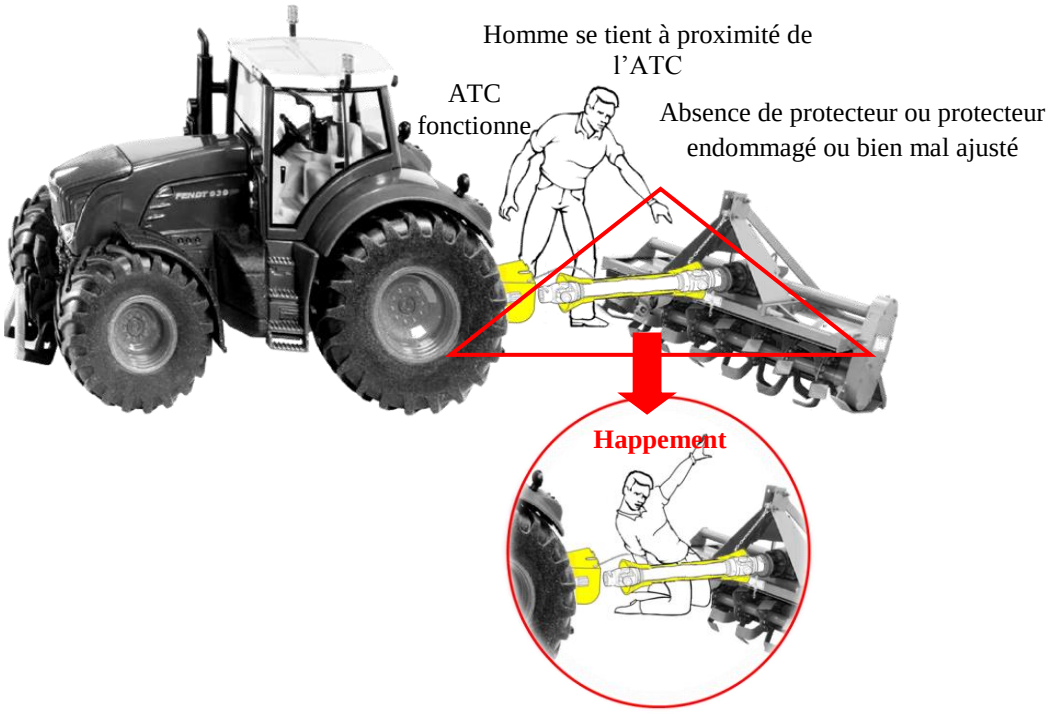


Figure 3.9. Illustration des conditions menant à l'accident avec un arbre de transmission à cardans.

Nous présentons cet AdD avec différents niveaux de détails aux figures 3.10 à 3.12. Comme l'illustre la figure 3.10, cet arbre composé des niveaux 1 et 2 reprend les résultats de l'élaboration des AdCs, c'est-à-dire qu'il montre que les événements « Homme se tient à proximité de l'arbre de transmission », « Arbre de transmission fonctionne », et « Absence de protecteur ou protecteur endommagé ou bien mal ajusté » peuvent causer le « happement ».

Pour la définition et l'élaboration des objectifs de sécurité, nous devons analyser les ramifications de l'AdD plus en profondeur. Les deux ramifications « ATC fonctionne » et « Homme se tient à proximité de l'arbre de transmission » sont liées au système sans considérations sécuritaires (présence d'un protecteur). La suite de l'analyse permet de générer d'autres déclencheurs de l'évènement. En effet, l'opérateur, l'outil et l'environnement peuvent entraîner l'accident par happement soit indépendamment soit de manière combinée.

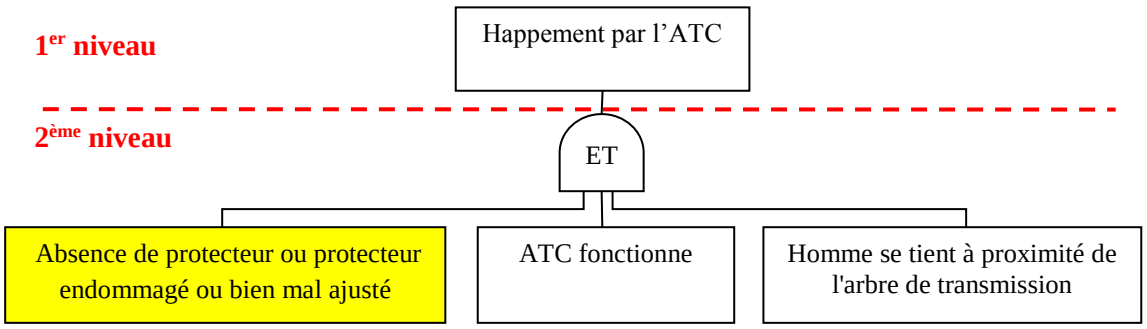


Figure 3.10. Identification des causes d'accident de l'ATC par l'AdD.

Les ATCs peuvent s'endommager ou se casser après une certaine période d'utilisation. L'expérience montre que cet endommagement ou cette casse intervient après environ 1000 heures d'utilisation. La question qui se pose est: *Pourquoi les ATCs ont tendance à se casser ou à s'endommager avec le temps?* L'AdC de la figure 3.11 présente les réponses possibles à cette question. Après avoir étudié les différents rapports d'accidents et d'autres ressources (normes, documents de la CCMSA, …), nous avons listé les raisons suivantes :

- Causes liées à la dégradation du tube de protection :
  - Taille de la transmission inadaptée ;
  - Conception trop fragile.
- Causes liées à la dégradation des bols de protection :
  - Transmission inadaptée à l'angularité maximale ;
  - Conception trop fragile ;
  - Inadaptation des bols par rapport au point d'ancrage de la transmission ainsi que par rapport aux virages serrés ;
  - Frottement, au contact et à l'impact avec les autres composants de la liaison tracteur/outil, comme les barres de traction de l'attelage trois points ;
  - Absence de graissage.
- Causes liées à la dégradation de la chainette :
  - Arrachage de la chainette ; les chaînettes sont sujettes à de nombreux accrochages avec des éléments extérieurs (branches, végétation,..) qui provoquent bien souvent leur rupture ;
  - Effort de tirage appliqué par le protecteur lors de la rotation de l'arbre de transmission à cardans.

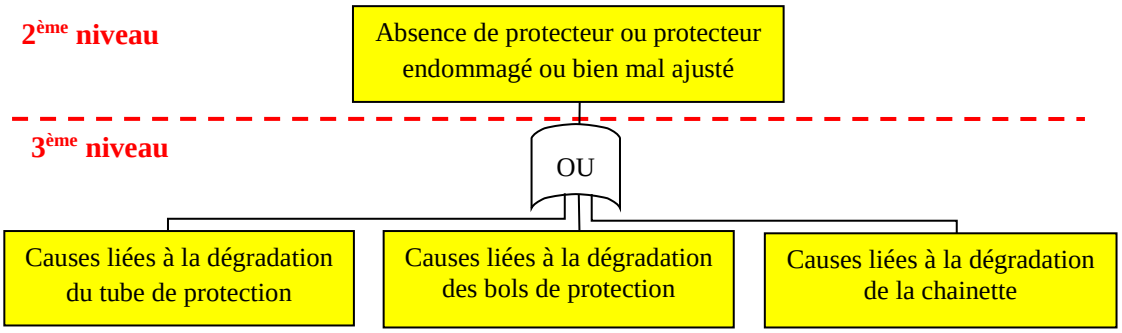


Figure 3.11. Causes d'absence, d'endommagement ou d'un mauvais ajustement du protecteur.

La deuxième question est liée à la situation dangereuse: *Pourquoi l'homme se tient à proximité de l'ATC?* L'AdC de la figure 3.12 présente les réponses possibles à cette question. En effet, l'homme se tient à proximité de l'ATC pour différentes raisons:

- Causes liées à la tâche :
  - *Exécuter une activité liée à l'ATC* ; Exemple : résoudre un problème concernant l'ATC.
  - *Exécuter une activité liée au tracteur* ; Exemples : résoudre un problème concernant le tracteur, etc.
  - *Exécuter une activité liée à l'outil ;* Exemples : résoudre un problème concernant l'outil, nettoyer l'outil, régler l'outil, graisser l'outil, vérifier le fonctionnement de l'outil.
- Causes liées à l'utilisateur ; Exemples : non-connaissance des consignes de sécurité, non-respect de ces consignes ou capacités visuelles limitées.
- Causes liées à l'environnement ; Exemples : glissement lors du déplacement vers l'outil, ramassage d'un objet se trouvant sous l'ATC.

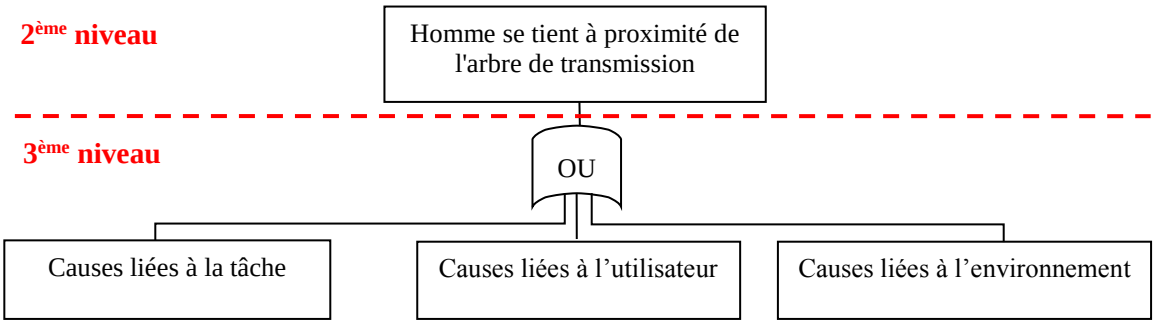


Figure 3.12. Causes de présence de l'humain à proximité de l'ATC.

Il convient de noter que nous avons essayé de regrouper les causes d'accidents « happement par l'ATC » en utilisant l'AdD. La figure 3.12 ne montre donc que les catégories des causes sans toutes les citer.

3.2.4.3. Conclusion sur l'application

Nous avons appliqué l'approche proposée sur l'Arbre de Transmission à Cardans afin de valider l'approche d'analyse des rapports formels d'accident proposée. Les résultats montrent que, pour le type d'accident « accident de happement par l'ATC », la réunion des causes suivantes peuvent entrainer le « happement »:

- homme se tient à proximité de l'arbre de transmission à cardans;
- arbre de transmission à cardans fonctionne ; et
- absence de protecteur ou protecteur endommagé ou bien mal ajusté.

Ces causes, liées à l'opérateur, à l'outil ou à l'environnement, peuvent entraîner l'accident par happement soit indépendamment soit de manière combinée. Pour chacun de ces éléments, nous avons représenté l'ensemble de causes potentielles pour ce type d'accident en utilisant l'Arbre de Défaillances (AdD). Dans la section 3.3, nous allons extraire les connaissances sur la conception de l'ATC.

3.2.5. Conclusion

Dans cette partie, nous proposons une approche permettant de définir, décrire et comprendre les causes d'accidents en nous basant sur le rapport type d'accidents présenté dans le chapitre 2. A cette fin, nous utilisons trois parties du rapport type d'accident: les parties « Dommage », « Type d'accident » et « Conditions de l'accident ». Ensuite, nous avons proposé une approche en deux étapes :

1. Déterminer les conditions dangereuses (le phénomène dangereux, la situation dangereuse et l'événement dangereux) en se basant sur la construction et l'analyse de l'Arbre des Causes (AdC) ;
2. Identifier toutes les causes potentielles en se basant sur la construction et l'analyse de l'Arbre de Défaillances (AdD).

L'approche proposée a été détaillée par une application à l'Arbre de Transmission à Cardans (ATC). L'analyse des accidents confirme que dans le cas de l'absence de protecteur ou d'un protecteur endommagé ou bien mal ajusté, ce système est très dangereux. En conséquence, et afin d'améliorer la sécurité de l'ATC, nous nous focaliserons dans le chapitre 5 à la reconception des protecteurs existants de l'ATC.

Après avoir identifiée la partie du système impliquée dans l'accident, la section suivante a pour but de décrire l'extraction de connaissances sur sa conception.

3.3. Développement d'une approche d'extraction des connaissances de la conception de la partie d'un système impliquée dans un accident

3.3.1. Introduction

Un manque identifié d'IRAD est que cette méthode ne propose pas de cheminement de l'analyse des rapports d'accidents à la construction de la matrice de conception. La section précédente a proposé une approche d'analyse de rapports d'accident formels. Le but de cette section est d'identifier et d'analyser la partie du système impliquée dans l'accident et ainsi identifier et analyser son processus de conception dans le cadre de l'opérationnalisation d'IRAD et plus précisément de l'opérationnalisation de son premier cas d'emploi. En effet, cette section tente de répondre à la question : *Comment extraire, formaliser et analyser les connaissances de conception d'un système existant afin de les réutiliser ?*

L'idée est de proposer une approche permettant de retracer, de manière hiérarchique, les choix de conception d'un système existant. Ceci doit se faire en identifiant, à partir de l'existant, les solutions de conception adoptées pour le système lors de sa conception et les exigences fonctionnelles qui ont amené ces solutions.

Dans la section qui suit (section 3.3.2), nous présentons, dans un premier temps, un état de l'art sur les approches de conception. Pour cela, nous présentons l'approche systématique et la théorie de la conception axiomatique. A la fin de cette section, une synthèse et notre positionnement sont détaillés. La section 3.3.3 porte sur le développement d'une approche d'identification et d'analyse d'un système existant du point de vue technique pour retracer son processus de conception. Ensuite, la section 3.3.4 traite de la validation de

l'approche développée par l'application à l'Arbre de Transmission à Cardans (ATC). Finalement, la section 3.4.5 présente la conclusion et les perceptives de cette partie.

3.3.2. Les approches de conception

Comme nous l'avons expliqué dans le chapitre 1, le processus de conception d'IRAD se base sur l'approche systématique décrite par Pahl et Beitz [Pahl et Beitz, 2007] et la théorie de conception axiomatique proposée par Suh [Suh, 1990]. Dans cette partie nous allons revenir sur ces deux approches.

3.3.2.1. Présentation de l'approche systématique

L'approche systématique de la conception a été proposée par Gerhard Pahl et Wolfgang Beitz en 1988. La décomposition fonctionnelle selon [Pahl et Beitz, 2007] est une décomposition de la fonction globale en sous-fonctions. Cette approche propose une représentation du processus de conception en quatre phases :

Planification et clarification de la tâche (la spécification des exigences). Cette phase a pour but la spécification des besoins dans une liste d'exigences. Elle permet d'obtenir une description des objectifs de l'étude basée sur les connexions entre les fonctionnalités du produit souhaité et les conditions de son obtention et de sa réalisation. Cette phase de conception correspond à l'établissement d'un cahier des charges décrivant les spécifications techniques et économiques à atteindre. Pour y arriver, les questions suivantes doivent trouver des réponses en collaboration avec le client: Quels objectifs la solution doit satisfaire?, Quelles sont ses propriétés?, et Quelles propriétés ne doit-t-elle pas avoir? Cette phase fait appel aux approches fonctionnelles afin de traduire les besoins du client en exigences fonctionnelles, comme le Quality Function Deployment (QFD) et débouche sur l'élaboration d'une liste d'exigences.

Conception conceptuelle (la définition du principe de solution). Cette phase a pour but de déterminer une solution de principe. L'obtention de cette solution se base sur l'analyse fonctionnelle, l'emploi d'un moyen de résolution de problèmes et l'évaluation des alternatives disponibles. Elle demande d'établir la structure fonctionnelle, de rechercher et de sélectionner les principes de solution et de combiner les principes en concepts. L'analyse de la valeur est une méthode qui permet de mettre en œuvre la conception conceptuelle donc d'établir la structure fonctionnelle, de rechercher des solutions et d'évaluer pour sélectionner les principes de solution.

Conception architecturale (la matérialisation du concept et la définition de sa structure). La finalité de cette phase est de déterminer les choix structuraux, le choix des composants, des principales dimensions du système ainsi que les formes et matériaux à utiliser. Lors de cette phase, le concepteur doit vérifier et affiner les critères techniques et économiques.

Conception détaillée (le détail du concept et la définition des plans). Cette phase est la phase de production de plans, de la spécification détaillée et de la mise en place du processus de fabrication. Elle s'achève par la production d'une documentation détaillée décrivant complètement l'objet à réaliser.

L'approche systématique proposée par Pahl et Beitz ne propose pas une structuration du produit ou de la solution à concevoir. [Scaravetti, 2004 ; Ho Kon Tiat, 2006 ; Sallaou, 2008] dans leurs thèses, présentent les approches d'analyse et de structuration d'un problème de conception. En nous inspirant de ces travaux, nous passons en revue ces approches regroupées en deux catégories.

L'analyse fonctionnelle

L'analyse fonctionnelle permet d'identifier les fonctions structurantes associées au système. Selon la norme [FD X50-153, 2009], l'analyse fonctionnelle est la décomposition du produit à concevoir à travers les fonctions qu'il doit assurer et les contraintes qu'il doit respecter. Deux niveaux dans l'analyse fonctionnelle sont identifiés :

L'analyse fonctionnelle externe a pour but d'identifier les fonctions essentielles du système. Un des outils pour l'approche fonctionnelle externe est le diagramme pieuvre (figure 3.13). Dans ce diagramme, les FS (Fonctions de Service) « *expriment l'action attendue du produit sur un élément du milieu extérieur au bénéfice d'un autre élément de ce milieu, dans une phase d'utilisation* » et les FC (Fonctions Contrainte) « *traduisent les contraintes imposées au produit par un milieu extérieur et qui ont une influence sur le choix et la définition du futur produit* » [Sallaou, 2008].

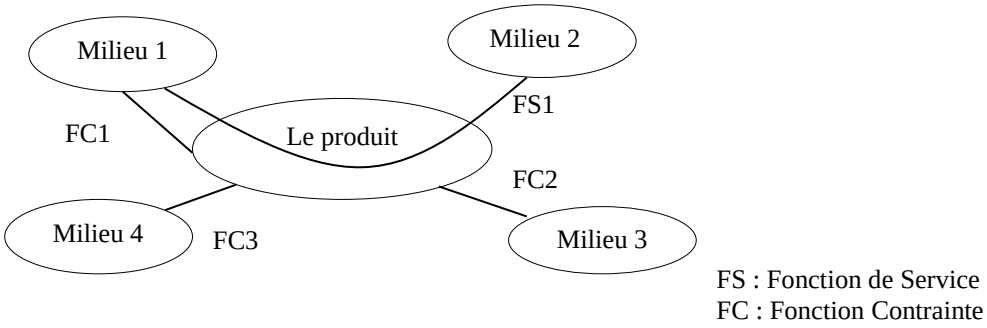


Figure 3.13. Diagramme pieuvre [Sallaou, 2008].

L'analyse fonctionnelle interne a pour finalité d'analyser les modalités de réalisation des fonctions identifiées durant l'approche externe. Un des outils utilisés dans l'analyse fonctionnelle interne est le diagramme FAST (Function Analysis System Technique). La figure 3.15 en montre la structure.

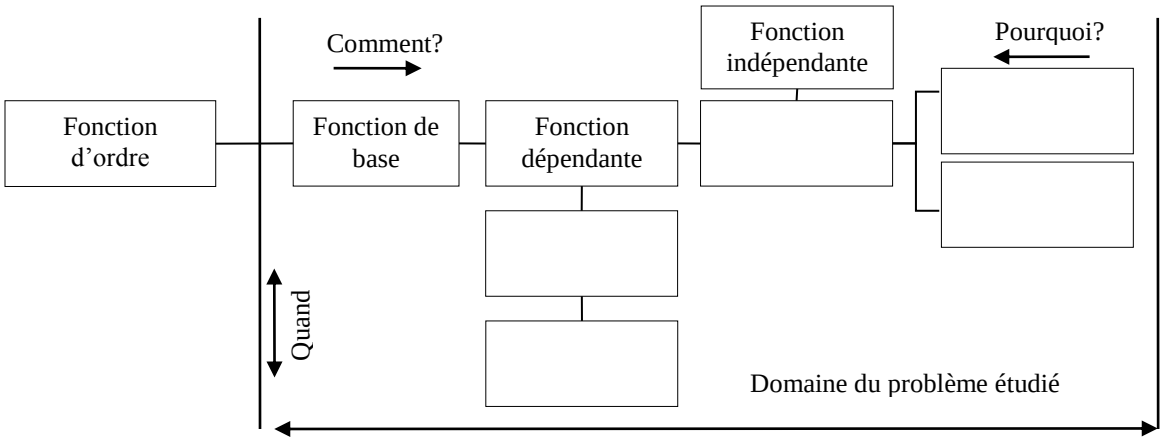


Figure 3.14. Function Analysis System Technique (FAST) [Yannou, 2008].

L'approche organique

Selon Sallaou [Sallaou, 2008] « *la définition complète d'une solution de conception passe par le choix des* ***composants*** *et les variables de définition liées à ces composants* ». Pour cette raison une décomposition organique du produit à concevoir est nécessaire. L'approche organique a pour but de décomposer structurellement un système afin de faciliter la gestion du problème de sa conception, grâce au fait que les éléments constitutifs sont répertoriés et classés [Ho Kon Tiat, 2006]. Les trois diagrammes suivants sont définis par [Sallaou, 2008] :

L'Organigramme Technique (OT): La décomposition organique permet de décomposer le produit en différentes entités qui le composent. L'OT est un graphe qui permet de décomposer le système en plusieurs niveaux. L'Organigramme Technique étendu (OTé) permet de faire apparaitre les milieux extérieurs au système, à différents niveaux, dans la constitution de l'OT (figure 3.15).

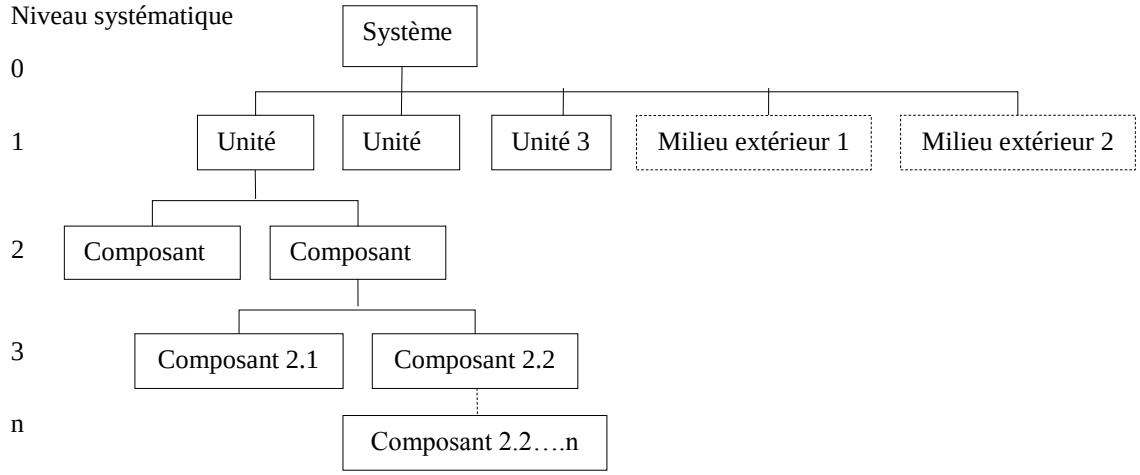


Figure 3.15. Organigramme Technique étendu (OTé) [Ho Kon Tiat, 2006].

Le Bloc Diagramme Fonctionnel (BDF): Cette représentation permet d'exploiter les informations issues des phases de décomposition fonctionnelle et de décomposition structurelle à différents niveaux systémiques (Figue 3.16). Le BDF est un outil qui représente les différents composants, les flux fonctionnels, les interactions et les composants d'interaction s'il y a lieu. Cette représentation peut être à différents niveaux systématiques [Sallaou, 2008].

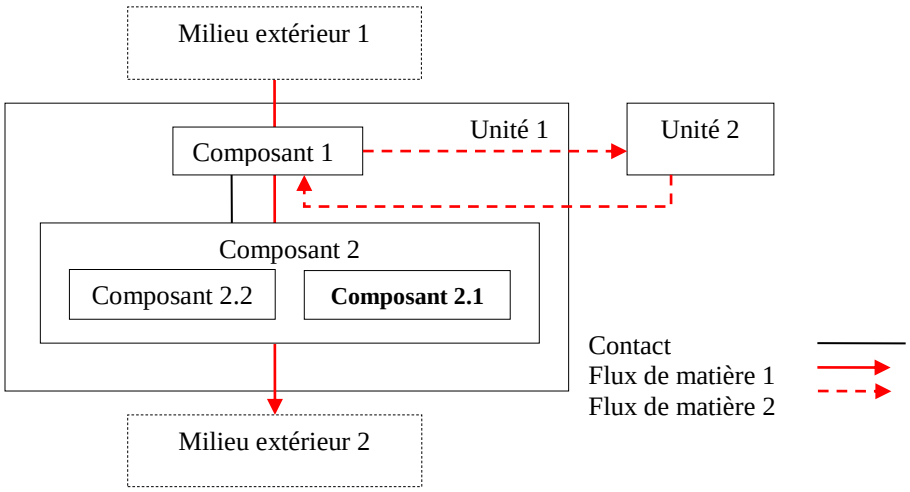


Figure 3.16. Bloc Diagramme Fonctionnel (BDF) [Ho Kon Tiat, 2006].

Le Graphe des associations Substances-Champs (GSC) : Cette représentation est une version du BDF qui permet d'intégrer les matières dans des blocs à part entière. Comme présentés à la figure 3.17, les composants, les milieux extérieurs et les matières sont identifiés à un même niveau comme étant les **substances.** Les flux transitant entre ces substances correspondent aux **champs** caractérisés par des verbes d'actions [Ho Kon Tiat, 2006]. Dans ce graphe, « *les BDFs font apparaître les éventuelles interactions qui se produisent entre les substances* » [Sallou, 2008].

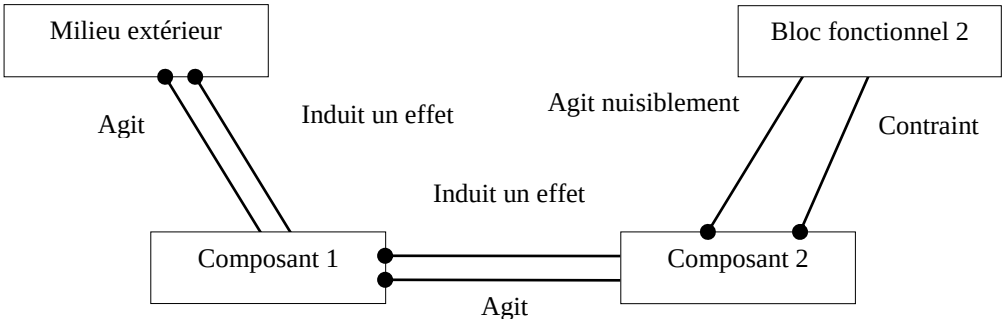


Figure 3.17. Graphe d'association Substance-Champs (GSC) [Sallaou, 2008].

La figure 3.18 issue de [Scaravetti, 2004] résume les phases d'analyse, de structuration et de formalisation des modèles pour un problème de conception architecturale. La démarche est composée de quatre approches : (1) L'analyse du besoin permettant l'expression du besoin client et des critères de qualification de la conception de son point de vue: critères technologiques, critères économiques ou critères de qualification au niveau de l'entreprise ou du marketing ; (2) L'approche fonctionnelle énumérant les situations de vie et les fonctions structurantes du produit ;(3) L'approche organique décrit la structure du produit, en utilisant un organigramme technique ;(4) L'approche physique identifie, grâce à des outils de description des flux, tous les phénomènes physiques pertinents permettant de décrire le comportement du produit.

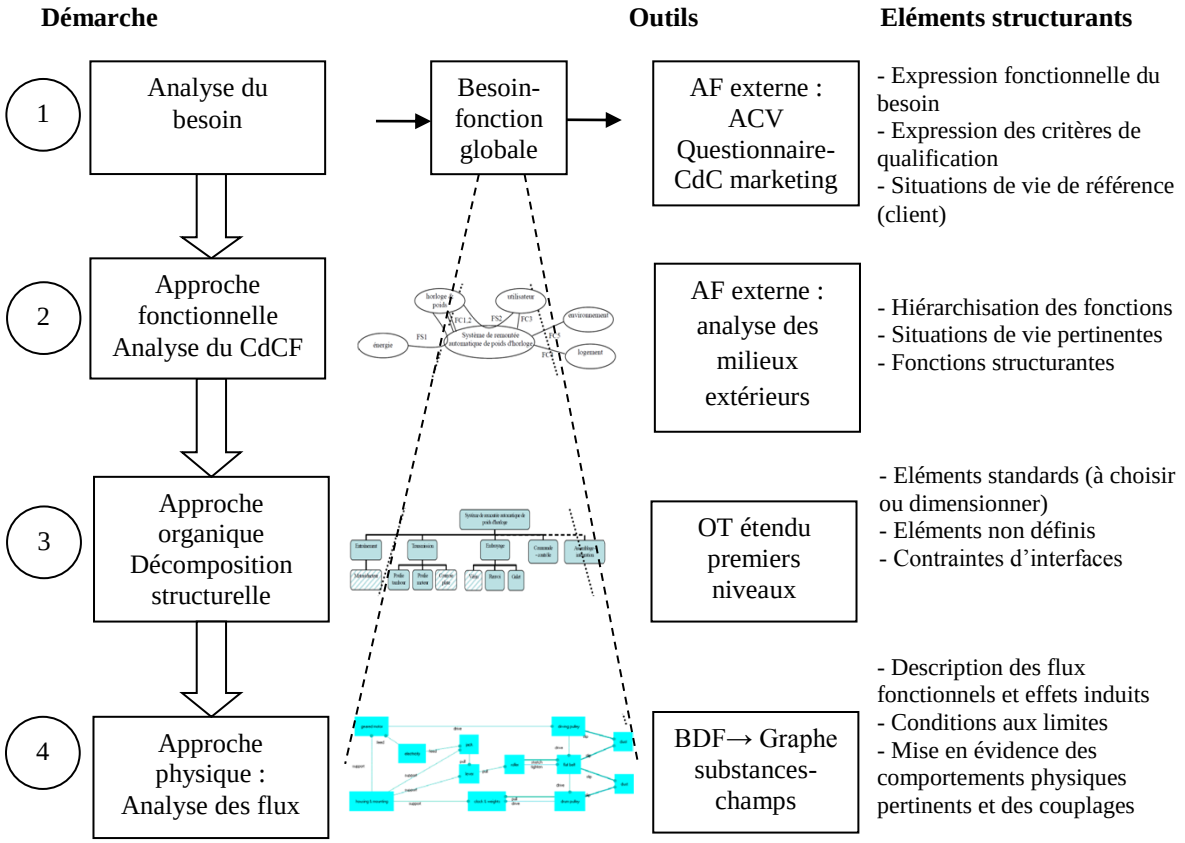


Figure 3.18. Synthèse des approches d'analyse et structuration du problème de conception [Scaravetti, 2004].

3.3.2.2. Présentation de la conception axiomatique

La conception axiomatique (ou AD pour Axiomatic Design) a été proposée par Suh du MIT [Suh, 1990 ; Suh, 2001 ; et Suh, 2005]. Cette théorie consiste à respecter des règles (des axiomes), afin d'obtenir une conception correcte. La conception axiomatique est basée sur les concepts principaux suivants: la conception en tant que processus de mappage entre quatre domaines; la décomposition hiérarchique, les lois de la conception sous la forme d'axiomes et la matrice de conception représentant les dépendances fonctionnelles. Une introduction de ces quatre concepts principaux est développée ci-dessous. Elle est basée sur les travaux de Suh.

Le mappage : Selon Suh, la conception suit un cheminement itératif et séquentiel entre "Ce que l'on cherche à accomplir" et "Comment l'accomplir". Donc, l'AD définit quatre domaines pour décrire le processus de conception : les domaines client, fonctionnel, physique et processus. Les besoins des clients, les exigences fonctionnelles, les paramètres de conception et les variables du processus forment les vecteurs caractéristiques de chaque domaine (figure 3.19).

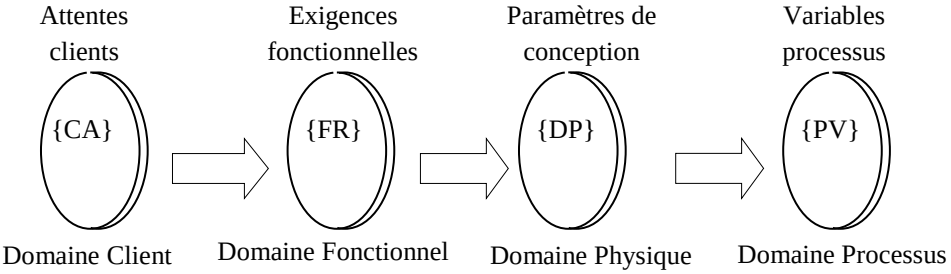


Figure 3.19. La Conception Axiomatique selon [Suh, 1990].

Décomposition hiérarchique : Le mappage est un processus itératif entre les différents domaines. Les attentes client sont exprimées sous forme de fonctionnalités dans le domaine fonctionnel par la mise en œuvre de méthodes comme le Quality Function Deployment (QFD). Les exigences fonctionnelles, les paramètres de conception ainsi que les variables de processus doivent être décomposées hiérarchiquement jusqu'à l'obtention de tous les détails de la conception. Mais cette décomposition ne peut pas être faite tout en restant dans le même domaine. Des allers-retours, « zigzaging », entre les domaines sont nécessaires pour réaliser cette décomposition (figure 3.20). A chaque niveau hiérarchique de la conception, les exigences fonctionnelles associées à ce niveau constituent le vecteur FR (pour Functional Requirement) dans le domaine fonctionnel. Les paramètres de la conception (ou DP pour Design Parameters) du domaine physique associés à ce même niveau hiérarchique expriment le vecteur DP. Dans notre travail de recherche, nous nous intéressons plus particulièrement aux deuxième et troisième domaines de l'approche de la conception axiomatique (domaines fonctionnel et physique).

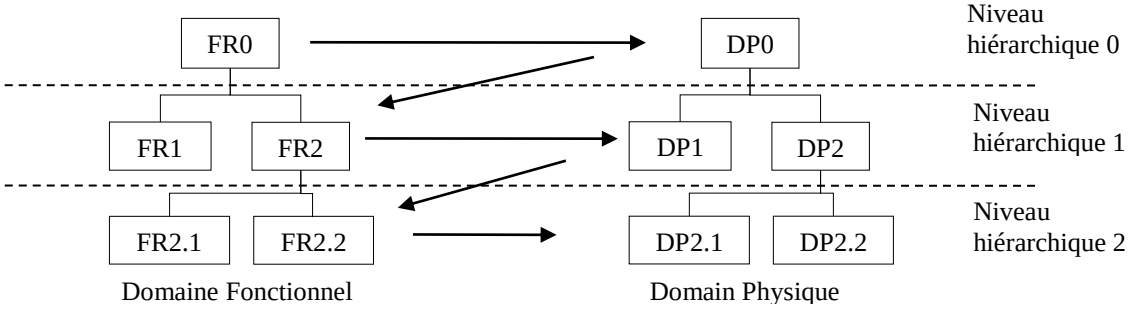


Figure 3.20. Décomposition hiérarchique d'une conception.

Matrice de conception : Le mappage entre FR et DP est exprimé sous forme mathématique, en fonction des vecteurs caractéristiques qui définissent les objectifs de la conception et les solutions de conception: {FR} = [A] {DP}

Dans cette équation, [A] est la matrice de conception.

Axiomes de conception : Les axiomes permettent la détermination de la qualité de la conception. Dans cette partie, nous décrivons les deux axiomes de transition du domaine fonctionnel au domaine physique.

- **L'axiome 1 (axiome d'indépendance)** propose de maintenir l'indépendance des exigences fonctionnelles (FR). Selon la forme de la matrice de conception, on peut vérifier l'indépendance des exigences. Les trois types de conception correspondent à des matrices de conception différentes :
  - Conception non couplée : Si la matrice de conception est diagonale (tous les $A_{ij} = 0$ et les A_{ii} sont non nuls), l'axiome d'indépendance est respecté. Dans ce type de conception, chaque FR est satisfait indépendamment par un DP. Ce type de conception est une conception optimale ;
  - Conception découplée : Si la matrice de conception est triangulaire (inférieure ou supérieure), l'axiome d'indépendance est respecté. Dans ce type de conception, l'indépendance des FR ne peut être garantie que si les paramètres de conception sont définis par une séquence bien définie. Ce type de conception est une conception acceptable ;
  - Conception couplée : Si la matrice de conception n'est ni diagonale, ni triangulaire, la conception est dite couplée.

  Selon cet axiome, une conception idéale comprend autant de paramètres de conception que d'exigences.
- **L'axiome 2 (axiome du minimum d'informations)** propose de minimiser l'information contenue dans une conception sachant que la meilleure conception est celle contenant le minimum d'informations.

  Le calcul de la quantité d'informations contenues dans une conception est facilité par l'utilisation des fonctions « étendue de conception » et « étendue du système ». L'étendue de conception est indiquée pour chaque FR par le concepteur, alors que l'étendue du système résulte de la performance réelle de la conception. Pour parvenir à une conception robuste, Suh [Suh, 2001] a proposé d'éliminer les biais et de réduire la variance du système. Le terme de biais est défini comme la différence entre la moyenne d'un FR de l'étendue du système et la valeur cible définie par le client. Le chevauchement entre l'étendue de conception et l'étendue du système est appelé l'étendue commune (figure 3.21).

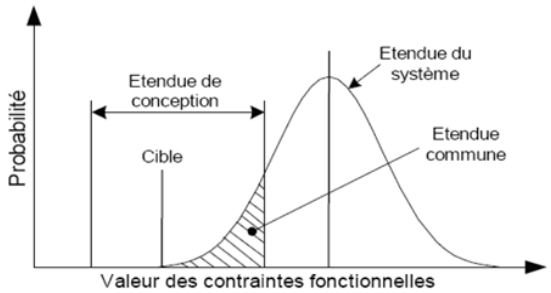


Figure 3.21. Axiome du minimum d'informations.

Ainsi, la robustesse de la conception est améliorée en satisfaisant le second axiome de la conception axiomatique.

3.3.2.3. Synthèse et positionnement par rapport à nos objectifs

L'approche systématique vis-à-vis de nos objectifs. Dans le cadre de nos travaux, l'objectif principal est d'intégrer la sécurité au plut tôt dans le processus de la conception. Il est donc nécessaire de détailler les caractéristiques influençant potentiellement la sécurité du système conçu à chacune des phases de conception. L'approche systématique développée par [Pahl et Beitz, 2007] décrit les actions à réaliser à chaque phase mais ne formalise pas les démarches de réalisation de ces actions. Nous proposons d'utiliser cette approche et de répondre à la question : *Comment exprimer et structurer les solutions techniques à chaque phase de la conception ?* Intégrer les principes de l'approche de la conception axiomatique devrait nous permettre de répondre à cette question.

Après avoir présenté les approches de l'analyse et la structuration du problème de conception, nous revenons sur nos problèmes et objectifs. Dans nos travaux, et plus précisément dans le cadre de l'ingénierie inverse fonctionnelle pour la sécurité, notre objectif est de représenter les connaissances sur le système existant. L'idée est d'identifier les composants techniques, les composants de sécurité du système et les relations entre ces composants. Ci-dessous sont listées les questions auxquelles nous devons répondre dans ce cadre.

- *Comment les composants du système fonctionnent-t-ils ensemble ?*
- *Quels sont les composants du système et les relations entre eux permettant de parvenir à un bon fonctionnement du système ?*
- *Quelle est l'objectif de chaque composant ?*

L'analyse fonctionnelle et l'approche organique détaillées dans cette partie sont des outils propices à répondre à ces questions.

La conception axiomatique vis-à-vis de nos objectifs. Dans le cadre de l'ingénierie inverse fonctionnelle pour la sécurité, notre objectif est d'identifier les paramètres de la conception et leurs liens avec chaque composant et ensuite de définir l'exigence fonctionnelle associée. La question qui se pose est donc: *Comment formuler les FRs et DPs à partir d'un système existant ?* Une fois les FRs et DPs identifiés, il faut analyser la conception. La matrice de conception de l'AD semble être un outil intéressant permettant d'y parvenir. Restent deux questions auxquelles nous devons répondre : *Comment remplir la matrice de conception?* et *Comment lire une matrice de conception ?*

Dans la section suivante, et en s'appuyant sur les conclusions présentées dans les sections précédentes, nous allons développer l'approche de conception inverse.

3.3.3. Développement d'une approche d'extraction des connaissances sur la conception du système

La section 3.2.3 a proposé une approche d'analyse de rapports types d'accident. Cette approche permet d'identifier la partie du système impliquée dans l'accident. Dans cette section, nous allons développer une approche de conception inverse en nous basant sur l'approche systématique et la théorie de la conception axiomatique. On s'attachera ici à répondre plus précisément aux questions posées dans la section précédente. Au regard des différents constats brièvement présentés ci-dessus, il a été choisi de proposer les étapes suivantes afin d'identifier et d'analyser le système du point de vue technique et de définir son processus de conception [Sadeghi et al., 2013a].

Les systèmes étudiés sont des systèmes complexes. Il faut donc, autant que faire se peut, limiter le périmètre d'étude. Dans la mesure du possible, il est nécessaire de se limiter à « la partie du système impliquée dans l'accident » ; celle-ci ayant été identifiée lors de

l'analyse du rapport type de l'accident. Pour plus de clarté dans la suite de ce manuscrit, nous appellerons système la partie ayant été identifiée comme partie du système impliquée dans l'accident.

3.3.3.1. Compréhension du système par l'abstraction

Comment les composants du système fonctionne-t-il ensemble ? L'abstraction du système doit permettre de définir le fonctionnement du système afin d'en comprendre le fonctionnement. On peut ici s'aider d'informations sur le système provenant de documents techniques (guide d'utilisation, fiches de données de sécurité, …), des normes, etc.

3.3.3.2. Analyse du système par l'approche organique

Quels sont les composants du système et les relations entre eux permettant de parvenir à un bon fonctionnement du système ? Il convient ici de représenter les composants du système (techniques et de sécurité) et de mettre en évidence les flux existants (contact, énergie, information et matière) entre ces composants et l'environnement. Le Bloc Diagramme Fonctionnel (BDF) permet d'identifier la fonction principale du système ainsi que les fonctions contraintes et auxiliaires. Le flux qui relie deux éléments du milieu en passant par les composantes du système retrace la fonction principale. Le flux qui relie un élément extérieur avec des composants du système représente une contrainte. Le flux qui relie des composants du système entre eux, retrace une fonction technique. Nous représentons donc ici les composants du système et les relations qui les lient.

A quel niveau de la conception est intervenu chaque composant ? La description hiérarchique du système permet de répondre à cette question. Cette description peut être formalisée en utilisant le diagramme Organigramme Technique étendu (OTé). Le système est identifié au niveau 0 du diagramme, ses unités au niveau 1 et ses composants aux niveaux inférieurs.

3.3.3.3. Définition des DPs et FRs

Le modèle du processus de la conception que nous avons adopté dans nos travaux est basé sur la confrontation d'une analyse fonctionnelle, d'une analyse organique et de la théorie de la conception axiomatique. Un des principes de cette théorie est la décomposition hiérarchique des exigences fonctionnelles (FRs) et des paramètres de conception (DPs). Notre approche d'ingénierie inverse doit permettre de définir les exigences fonctionnelles à partir des composants en passant par la définition des paramètres de conception. L'OTé apparait intéressant pour réaliser le premier mappage entre les composants du système et les DPs et le BDF pour réaliser le second entre les DPs et les FRs.

Rappelons que les objectifs de conception sont définis en termes d'exigences fonctionnelles. Une exigence s'exprime sous la forme « verbe + complément » et que les DPs, variables clés qui caractérisent l'entité physique créée par le processus de conception afin de remplir les FRs, se formalise sous la forme d'un nom a minima. Ces points sont synthétisés dans le tableau ci-dessous (tableau 3.4).

Tableau 3.4. Guide pour l'identification des DPs et FRs [Sadeghi et al., 2013a].

	DPs : solutions	**FRs : objectifs**
Répondre à	A quoi cela ressemble-t-il ?	Quelle est sa fonction?
Commencer par	Un nom	Un verbe
Présenter	Une solution de conception	Un objectif de conception

3.3.3.4. Analyse de la conception par la matrice de conception

Comment peut-on remplir la matrice de conception? A un niveau hiérarchique donné de la conception, les exigences fonctionnelles constituent le vecteur des FRs. De la même manière, les paramètres de la conception constituent le vecteur des DPs. La relation entre les deux vecteurs à chaque niveau hiérarchique correspond à la matrice de conception caractérisant le système. Chaque lien entre un DP et un FR est caractérisé dans cette matrice par une croix.

Contrainte de remplissage : Dans la mesure du possible, isoler dans la matrice les FRs liés à la sécurité des autres FRs et isoler les DPs liés à la sécurité des autres DPs.

Comment peut-on lire la matrice de conception ? Après avoir rempli la matrice de conception, il est nécessaire de l'analyser. Cette analyse se limite ici à l'identification des couplages. Ces couplages seront utilisés pour la reconception du système dans la démarche FR2ES.

3.3.3.5 Conclusion sur l'approche proposée pour extraire les connaissances sur la conception

Dans cette section, nous avons présenté une approche permettant d'extraire les connaissances sur la conception de la partie du système impliquée dans l'accident. Elle est basée sur la confortation d'une analyse fonctionnelle, d'une analyse organique et de la conception axiomatique en quatre étapes (figure 3.22) :

1. **La compréhension du système par l'abstraction** en se basant sur les connaissances obtenues sur le système suite à l'analyse des rapports d'accidents et issues des documents techniques, normes, etc. ;
2. **L'analyse du système par l'approche organique** qui se décompose en deux sous-étapes : représenter les composants du système et les relations qui les lient à l'aide du Bloc Diagramme Fonctionnel (BDF) et décomposer hiérarchiquement le système en utilisant l'Organigramme Technique étendu (OTé) ;
3. **La définition des DPs et FRs** en se basant sur le BDF et l'OTé réalisés à l'étape précédente ;
4. **L'analyse de la conception du système à l'aide de la matrice de conception** qui débute par la construction de la matrice et se termine par son analyse d'un point de vue technique.

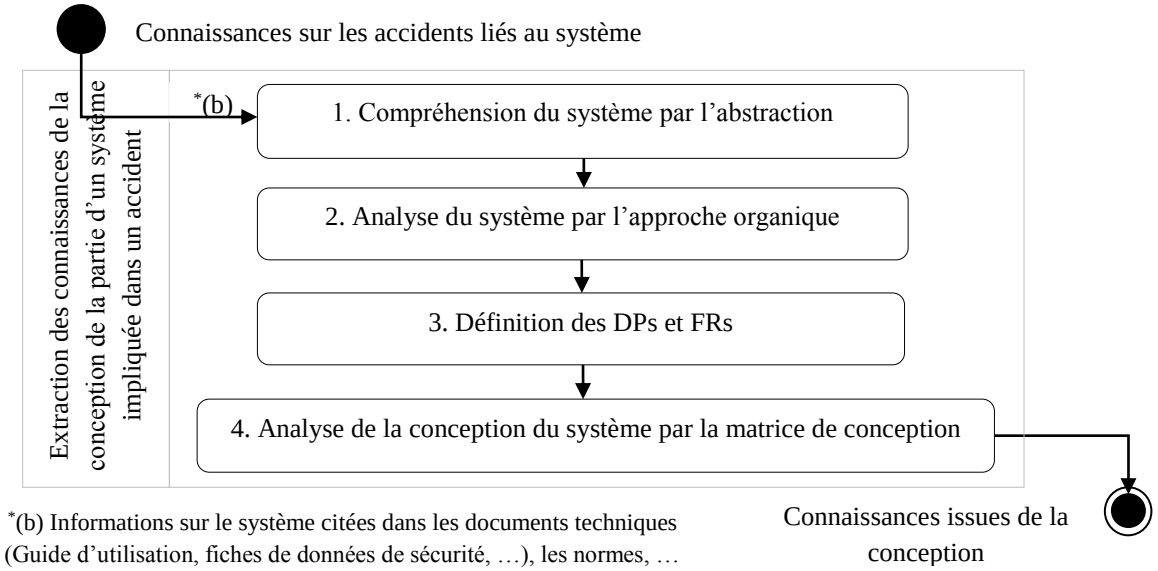


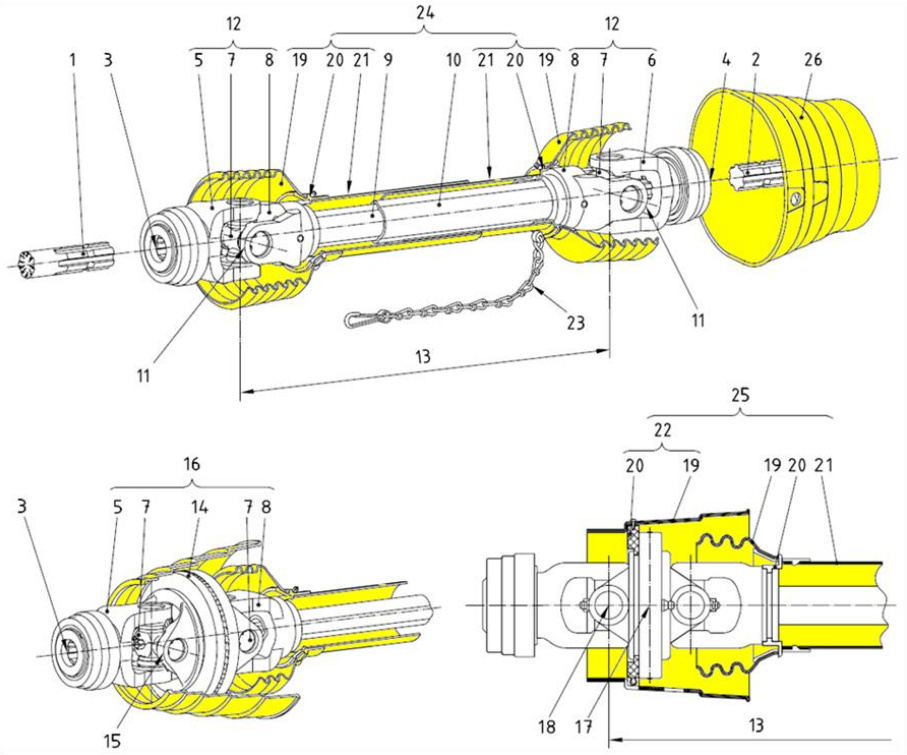
Figure 3.22. Approche d'extraction des connaissances de la conception.

Dans la section suivante, nous appliquons cette approche à l'Arbre de Transmission à Cardans (ATC).

3.3.4. Application : extraction des connaissances sur la conception de l'arbre de transmission à cardans

3.3.4.1. Compréhension de l'ATC par abstraction

Une description de ce système a été réalisé au chapitre 2 (§2.4.2). Les ATCs agricoles sont normalisés [ISO 5673-1, 2005; ISO 5673-2, 2005; NF EN ISO 5674, 2009; NF EN 12965 + A2, 2009]. Leurs dimensions, leur vitesse de rotation et leurs moyens de protection ont été définis afin d'éliminer ou de réduire les risques de happement. Nous avons trouvé ces informations dans diverses documents (normes, livres spécialisés [Banas, et al, 2007], notices d'utilisation, etc.). Les composants de l'ATC sont illustrés à la figure 2.7 du chapitre 2 (§2.4.2). Le figure 3.23 montre les détaille des composantes de l'ATC.



1 arbre de transmission à cardans de prise de force (p.d.f.)
2 arbre récepteur de la machine (a.r.m.)
3 alésage de la mâchoire correspondant à la p.d.f.
4 alésage de la mâchoire correspondant à l'a.r.m.
5 mâchoire de cardan correspondant à la p.d.f.
6 mâchoire de cardan correspondant à l'a.r.m.
7 croisillon d'assemblage du joint de cardan
8 mâchoire de cardan mâle
9 profil coulissant mâle
10 profil coulissant femelle
11 extrémité de la mâchoire intérieure du joint de cardan
12 joint de cardan
13 longueur minimale et maximale de l'arbre de transmission à cardans de p.d.f.
14 double joint de cardan
15 extrémité du double joint de cardan
16 joint de cardan à grand angle
17 centre de l'articulation du joint de cardan à grand angle
18 centre du joint extérieur
19 cône de protection
20 palier du protecteur
21 tube de protection
22 protecteur séparé du joint de cardan à grand angle
23 dispositif d'immobilisation (à titre d'exemple)
24 protecteur d'arbre de transmission à cardans de p.d.f.
25 protecteur d'arbre grand angle de transmission à cardans de prise de force
26 protecteur de l'a.r.m.

Figure 3.23. Les composantes de l'ATC avec moyen de protection [ISO 5673-1, 2005] (les deux figures bas présentent cas particulière du joint à cardans double).

La figure 3.24 montre l'abstraction de l'ATC. Le repère R_0 (O_0 | x_0, y_0, z_0) est lié à la prise de force, les repères R_1 (O_1 | x_1, y_1, z_1) et R_2 (O_2 | x_2, y_2, z_2) au joint de cardan côté tracteur. T1 est l'élément télescopique, R_3 (O_3 | x_3, y_3, z_3) et R_4 (O_4 | x_4, y_4, z_4) les repères liés au joint de cardan côté outil, et R_5 (O_5 | x_5, y_5, z_5) le repère lié à l'ARM (Arbre Récepteur Machine) côté outil.

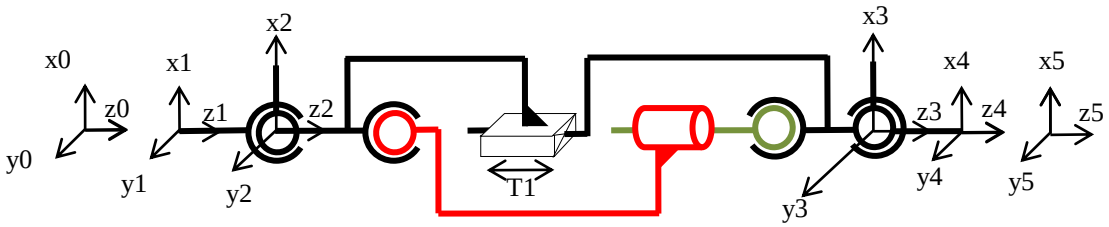


Figure 3.24. Abstraction de l'arbre de transmission à cardans.

3.3.4.2. Analyse de l'ATC par l'approche organique

Nous nous intéressons ici au tracteur, à l'outil et à l'opérateur qui correspondent aux facteurs entrant dans la fonction globale. L'ATC est composé de deux unités principales : l' « ATC sans moyen de protection » et le « Moyen de protection de l'ATC ». L'« ATC sans moyen de protection » est composé de trois sous-ensembles : une « mâchoire extérieure côté PdF », un « arbre de transmission à cardans » et une « mâchoire extérieure côté ARM ». Le sous-ensemble « arbre de transmission à cardans » est composé d'un « joint de cardan coté tracteur », d'un « système télescopique et d'un « joint de cardan coté outil ». Nous ne détaillons pas les autres composants. Le « Moyen de protection de l'ATC » comporte quatre sous-ensembles : un « système d'immobilisation », un « cône de protection (côté PdF) », un « tube de protection » et un « cône de protection (coté ARM) ».

Nous construisons ensuite le BDF (figure 3.25). Sur ce diagramme, le flux d'énergie en bleu correspond à la fonction principale et la ligne en pointillés correspondant au contact entre le tracteur, l'ATC, le protecteur et l'outil. Les composants de sécurité sont représentés sur fond jaune.

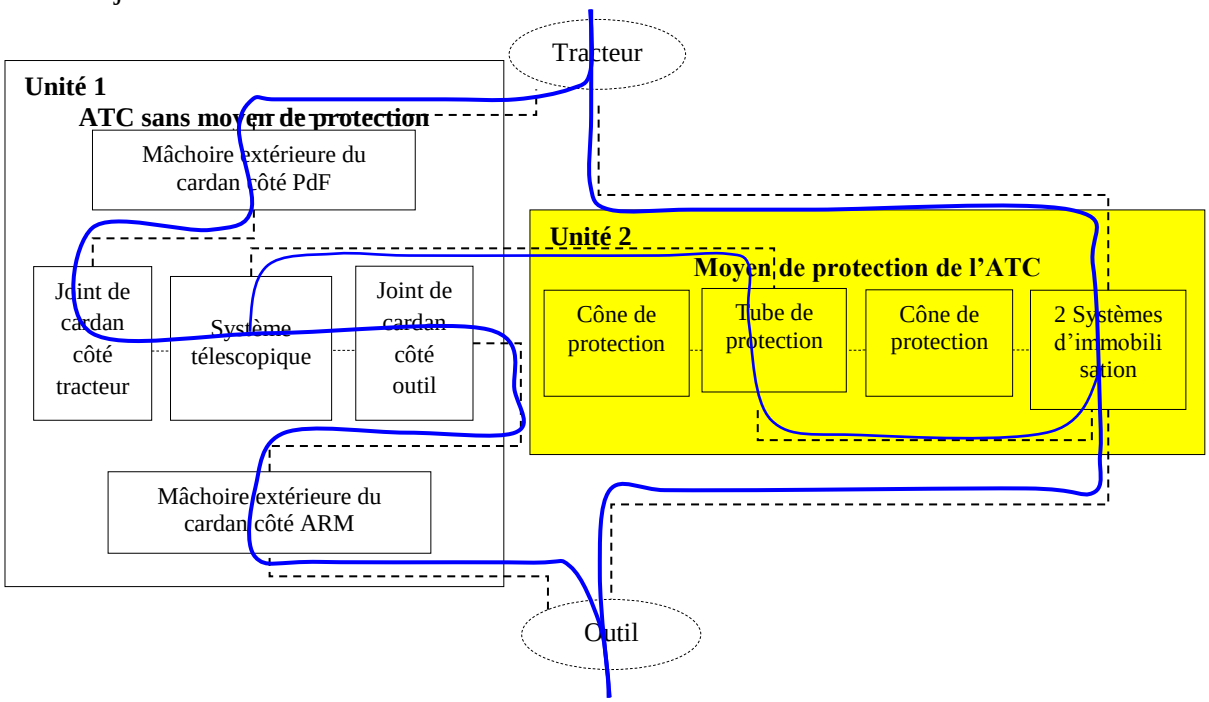


Figure 3.25. Bloc Diagramme Fonctionnel de l'ATC.

La figure 3.26 montre la décomposition structurelle de l'ATC. Nous retrouvons l'ATC au niveau 0. Ses deux unités, l' « ATC sans moyen de protection » et le « Moyen de protection de l'ATC » apparaissent au niveau 1. Au niveau 2, nous retrouvons les composants de l'ATC sans moyen de protection et les composants du moyen de protection. Enfin, au niveau 3, sont listés les composants de l'arbre de transmission à cardans.

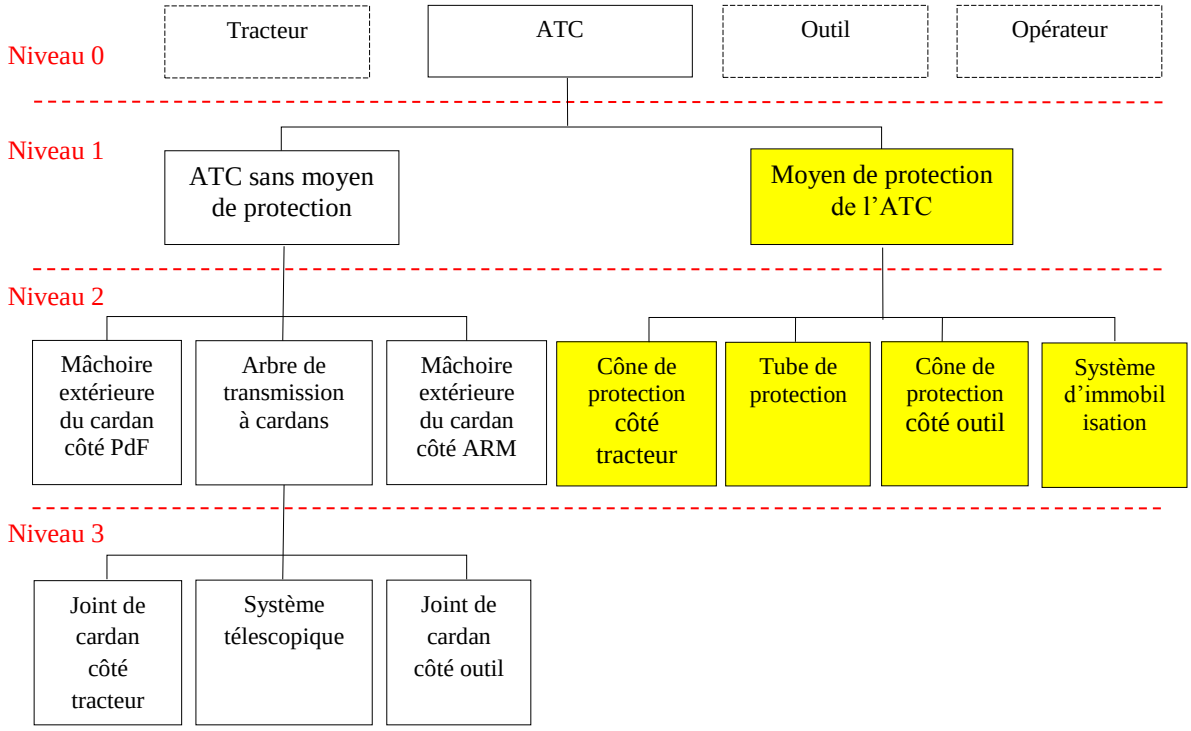


Figure 3.26. Organigramme Technique étendu de l'ATC.

3.3.4.3. Définition des DPs et FRs

Pour définir les DPs liés aux composants de l'ATC, nous nous basons sur l'OTé de l'ATC (figure 3.26) et le guide d'identification des DPs et FRs (§3.3.3.3 - tableau 3.4). Nous définissons les FRs à partir des DPs et du BDF de l'ATC (figure 3.25). Dissocier les FRs et DPs liés à la sécurité se fait ici naturellement puisqu'ils sont déjà séparés au niveau de l'OTé et du BDF.

L'ATC peut être défini comme un « système de transmission de puissance protégé » (DP0). La fonction principale de l'ATC est FR0 « assurer la motorisation de l'outil par l'énergie du tracteur en sécurité ».

L'ATC sans moyen de protection est un « système avec éléments en rotation» (DP1) et le moyen de protection de l'ATC est un « système de protection » (DP2). Les deux sous-fonctions de FR0 sont donc «FR1 : Motoriser l'outil par l'énergie du tracteur » et «FR2 : Rendre le système tournant sécuritaire ».

Nous décomposons le DP1 en deux paramètres de conceptions DP11 et DP12, auxquels nous avons affectés les exigences fonctionnelles FR11 et FR12. Le DP2 se décompose en quatre paramètres de conceptions DP21 à DP24 et les exigences fonctionnelles correspondantes sont les FR21 à FR24.

Ensuite, nous décomposons le DP11 en six paramètres de conceptions DP111 à DP116, auxquels nous avons affectés les exigences fonctionnelles FR111 à FR116.

La figure 3.27 résume les DPs et FRs identifiés jusqu'ici :

0	DP	Système de transmission de puissance protégée	
1	DP	Système avec éléments en rotation	
1.1	DP	Système de positionnement	
1.1.1	DP	Joint à cardan côté outil	
1.1.2	DP	Joint à cardan côté tracteur	
1.1.3	DP	-	
1.1.4	DP	Arbre télescopique	
1.1.5	DP	Joint fixé côté tracteur	
1.1.6	DP	Joint fixé côté outil	
1.2	DP	Système de transmission de puissance	
2	DP	Système de protection	
2.1	DP	Bol de protection côté tracteur	
2.2	DP	Tube de protection de l'arbre	
2.3	DP	Bol de protection côté outil	
2.4	DP	Chainette anti rotation	
0	FR	Assurer la motorisation de l'outil par l'énergie du tracteur en sécurité	
1	FR	Motoriser l'outil par l'énergie du tracteur	
1.1	FR	Autoriser les mouvements entre deux arbres	
1.1.1	FR	Autoriser la rotation autour des 2 axes perpendiculaires à l'axe de l'ATC	
1.1.2	FR	Autoriser la rotation autour de l'axe principal de l'ATC	
1.1.3	FR	Autoriser la translation autour des 2 axes perpendiculaires à l'axe de l'ATC	
1.1.4	FR	Autoriser la translation sur l'axe principal de l'ATC	
1.1.5	FR	Connecter le système à la prise de force	
1.1.6	FR	Connecter le système à l'arbre récepteur	
1.2	FR	Transmettre la puissance du tracteur à l'outil	
2	FR	Rendre le système tournant sécuritaire	
2.1	FR	Couvrir le joint de cardan côté tracteur	
2.2	FR	Couvrir l'arbre télescopique	
2.3	FR	Couvrir le joint de cardan côté outil	
2.4	FR	Empêcher la rotation des éléments couvrants	

Figure 3.27. DPs et FRs de l'ATC.

3.3.4.4. Analyse de la conception de l'ATC par la matrice de conception

La matrice de conception relative à la décomposition hiérarchique présentée à la Figure 3.27 est montrée à la figure 3.28.

Dans cette matrice, une dépendance entre une FR et un DP est identifiée par une « × » sur fond bleu. Dans le cas où il n'y a pas de DP pour répondre à une FR la valeur « 0 » est placée dans un carré vert, sauf lorsqu'elle se trouve sur la diagonale. Dans ce cas, la case n'est pas colorée. Notons que les couleurs utilisées n'ont pas de signification particulière. Elles permettent uniquement à différentier les cas. Nous avons rempli cette matrice comme suit :

- Le Système avec éléments en rotation (DP1) répond à Motoriser l'outil par l'énergie du tracteur (FR1) ;
- Le Système de protection (DP2) répond à Rendre le système tournant sécuritaire (FR2) ;
- Le Système de positionnement (DP11) répond à Autoriser les mouvements entre deux arbres (FR11) et Transmettre la puissance du tracteur à l'outil (FR12) ;
- Le Système de transmission de puissance (DP12) répond à Transmettre la puissance du tracteur à l'outil (FR12),
- Le Bol de protection côté tracteur (DP21) répond à Couvrir le joint à cardan côté tracteur (FR21) et Empêcher la rotation des éléments couvrants (FR24) ;

- Le Tube de protection de l'arbre (DP22) répond à Couvrir l'arbre télescopique (FR22) et à Empêcher la rotation des éléments couvrants (FR24) ;
- Le Bol de protection côté outil (DP23) répond à Couvrir le joint de cardan côté outil (FR23) et à Empêcher la rotation des éléments couvrants (FR24) ;
- La Chainette anti rotation (DP24) répond à Couvrir le joint à cardan côté tracteur (FR21), Couvrir l'arbre télescopique (FR22), Couvrir le joint à cardan côté outil (FR23) et à Empêcher la rotation des éléments couvrants (FR24) ;
- Le Joint à cardan côté outil (DP111) répond à Autoriser la rotation autour des 2 axes perpendiculaires à l'axe de l'ATC (FR111), Autoriser la translation autour des 2 axes perpendiculaires à l'axe de l'ATC (FR113) et Autoriser la translation sur l'axe principal de l'ATC (FR114) ;
- Le Joint à cardan côté tracteur (DP112) répond à Autoriser la rotation autour des 2 axes perpendiculaires à l'axe de l'ATC (FR111), Autoriser la translation autour des 2 axes perpendiculaires à l'axe de l'ATC (FR113) et Autoriser la translation sur l'axe principal de l'ATC (FR114) ;
- Il n'y a pas de solution de conception pour réaliser l'alignement entre le cardan et la prise de force. Le DP113 ne répond à aucun FR ;
- L'Arbre télescopique (DP114) répond à Autoriser la translation autour des 2 axes perpendiculaires à l'axe de l'ATC (FR113) et Autoriser la translation sur l'axe principal de l'ATC (FR114) ;
- Le Joint fixé côté tracteur (DP115) répond à Connecter le système à la prise de force (FR115) ;
- Le Joint fixé côté outil (DP116) répond à Connecter le système à l'arbre récepteur (FR116).

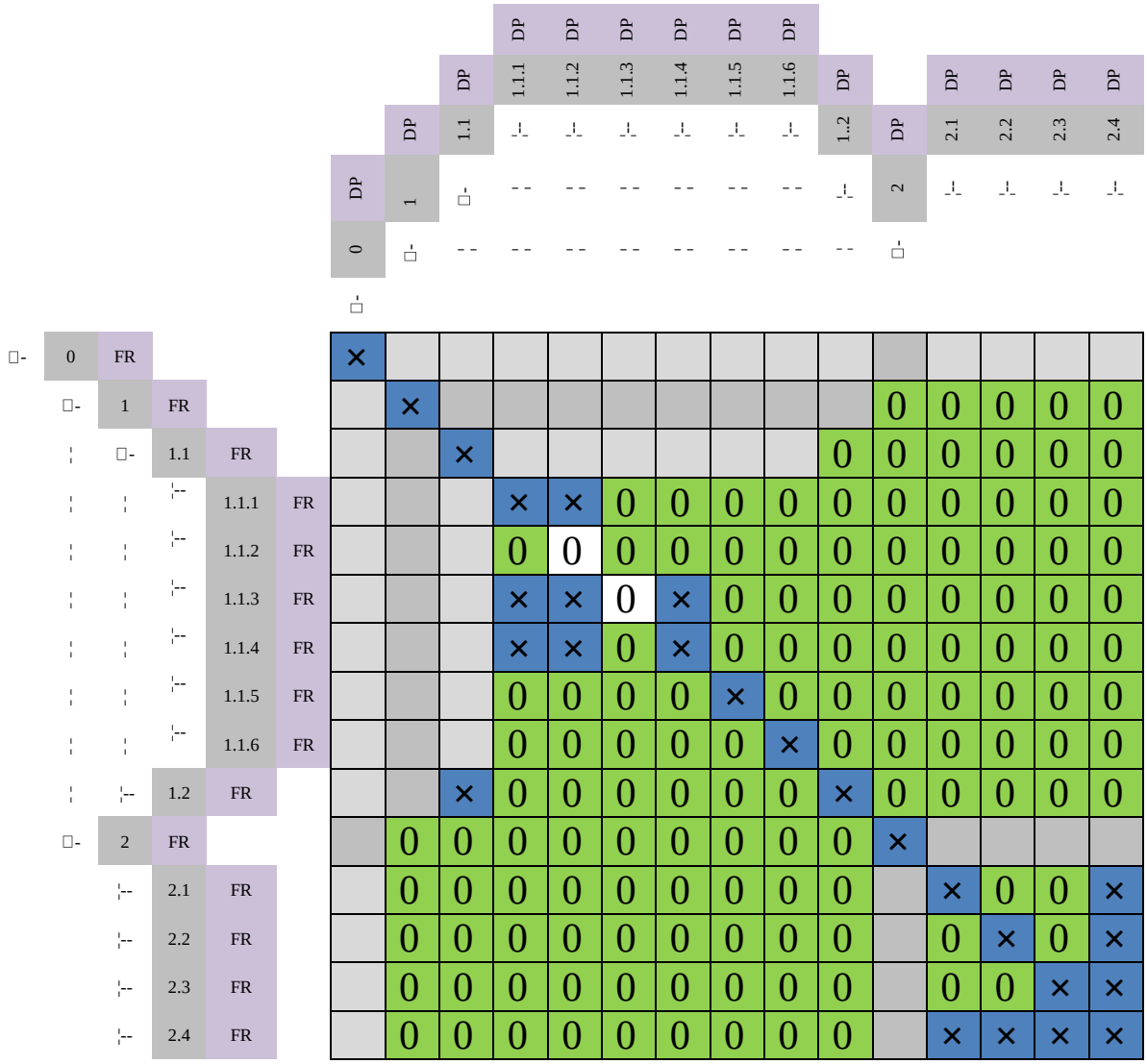


Figure 3.28. Matrice de conception de l'ATC.

3.3.4.5. Conclusion sur l'application

Dans les paragraphes précédents, nous avons appliqué notre approche afin d'obtenir des connaissances sur la conception. Ainsi, les composants de l'ATC et les relations qui les lient ont été identifiés. L'ATC a également été décomposé hiérarchiquement. Les DPs et FRs ont ensuite été définis. Ainsi 14 DPs et 15 FRs ont été identifiés. L'analyse des liens entre chacun d'eux a permis de construire la matrice de conception qui a révélé 13 couplages.

Ce travail permet de définir les fonctions contraintes synthétisées par le diagramme pieuvre (figure 3.29) :

Cs1 : S'adapter au tracteur ;
Cs2 : S'adapter à l'outil ;
Cs3 : S'adapter et ne pas causer de dommage à l'opérateur pendant toutes les sous phases de la phase d'utilisation ;
Cs4 : Respecter la réglementation;
Cs5 : Tenir compte des normes de sécurité ;
Cs6 : S'adapter aux conditions environnementales ;

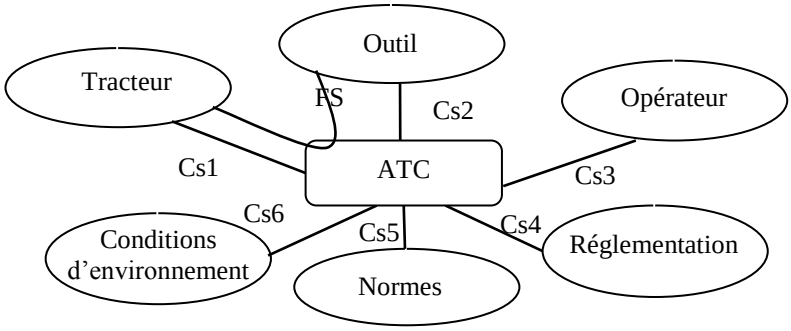


Figure 3.29. Diagramme pieuvre de l'arbre de transmission à cardans.

3.3.5. Conclusion

Dans cette section, nous avons développé une approche permettant d'identifier et d'analyser la partie du système impliquée dans un accident. Cette approche a été développée dans le cadre de l'opérationnalisation de la méthode IRAD, et plus précisément dans le cadre de l'opérationnalisation de son premier cas d'emploi. Elle est basée sur la confortation d'une analyse fonctionnelle, d'une analyse organique et de la conception axiomatique et comporte quatre étapes : (1) La compréhension du système par l'abstraction ; (2) L'analyse du système par l'approche organique ; (3) La définition des DPs et FRs ; et (4) L'analyse de la conception du système par la matrice de conception.

Nous avons appliqué cette approche sur l'Arbre de Transmission à Cardans (ATC). Elle a permis d'identifier l'ensemble des DPs et FRs ainsi que de construire la matrice de conception et donc d'identifier des couplages.

3.4. Conclusion

Dans ce chapitre, dans le cadre d'opérationnalisation de la méthode IRAD, nous avons présenté une partie de l'approche FRES. La deuxième partie de l'approche concerne l'évaluation de la sécurité. Elle est présentée dans le chapitre suivant. Le développement de la première approche, l'approche d'extraction des connaissances sur les accidents, est basée sur trois parties d'un rapport formel d'accident (Dommage, Type d'accident et conditions de l'accident). L'application de cette approche sur l'Arbre de Transmission à Cardans indique que les faits « Homme se tenant à proximité de l'ATC », « ATC fonctionne », et « Absence de protecteur ou protecteur endommagé ou bien mal ajusté » peuvent causer le « happement ».

La deuxième approche, l'approche d'extraction des connaissances sur la conception, a été développée en se basant sur la confortation d'une analyse fonctionnelle, d'une analyse organique et de la conception axiomatique. L'application de cette approche à l'ATC a permis de définir les différentes composantes de ce système et les relations qui les lient. Ainsi 14 DPs et 15 FRs ont été identifiés.

Les connaissances obtenues à partir de la mise en œuvre de la démarche FRES vont être utilisées pour l'évaluation de la sécurité du système. La démarche associée est présentée au chapitre suivant. Elles le seront également dans le cadre de la reconception sécuritaire. Cette autre démarche, appelée FR2ES, est présentée au chapitre 5.

Chapitre 4. Evaluation de et pour la sécurité

4.1. Introduction

Dans le chapitre précédent, nous avons présenté les deux premières étapes de notre approche d'ingénierie inverse fonctionnelle pour la sécurité (FRES) : l'extraction des connaissances sur un accident en se basant sur un rapport d'accident et l'extraction des connaissances sur la conception d'un système impliqué dans un accident guidée par la conception axiomatique. Dans ce chapitre, nous nous intéressons à la troisième étape de l'approche. Elle concerne l'évaluation de la sécurité d'un système. Cette évaluation permettra ensuite d'estimer le niveau de sécurité d'un système impliqué dans un accident.

Cette étape pourra également être mise en œuvre dans le cadre de la réingénierie fonctionnelle pour la sécurité et donc lors de l'application de l'approche FR2ES. Dans ce contexte, elle permettra de comparer les différentes alternatives de solutions de conception du point de vue sécurité et d'aider à la prise de décision.

Ainsi, l'intérêt de l'évaluation la sécurité peut être vue selon trois points de vue différents :

- Point de vue **sécurité**, l'évaluation de la sécurité permet d'identifier les risques et d'évaluer le niveau de sécurité de la partie du système impliqué dans l'accident. En effet, pour la partie du système impliquée dans l'accident, il faut répondre à deux questions: *Comment pouvons-nous identifier les risques et les ventiler selon les trois phases de la conception ?* et *Comment pouvons-nous mesurer son niveau de sécurité ?*
- Point de vue **conception**, l'évaluation de la sécurité traduit les caractéristiques et les aspects techniques du système en niveau de sécurité. Cette évaluation permet l'identification des paramètres techniques à optimiser afin d'obtenir un système sécuritaire.
- Point de vue **aide à la décision**, l'évaluation de la sécurité fournit un indicateur qui aide le concepteur à identifier et à choisir les solutions les plus sécuritaires parmi les différentes alternatives de solutions possibles tout au long du processus de conception.

Comme le montre la figure 4.1, nous proposons de décomposer la fonction A13 « Evaluer la sécurité » en deux sous-fonctions: A131 « Identifier et ventiler les risques selon les phases de conception » et A132 « Mesurer la sécurité ».

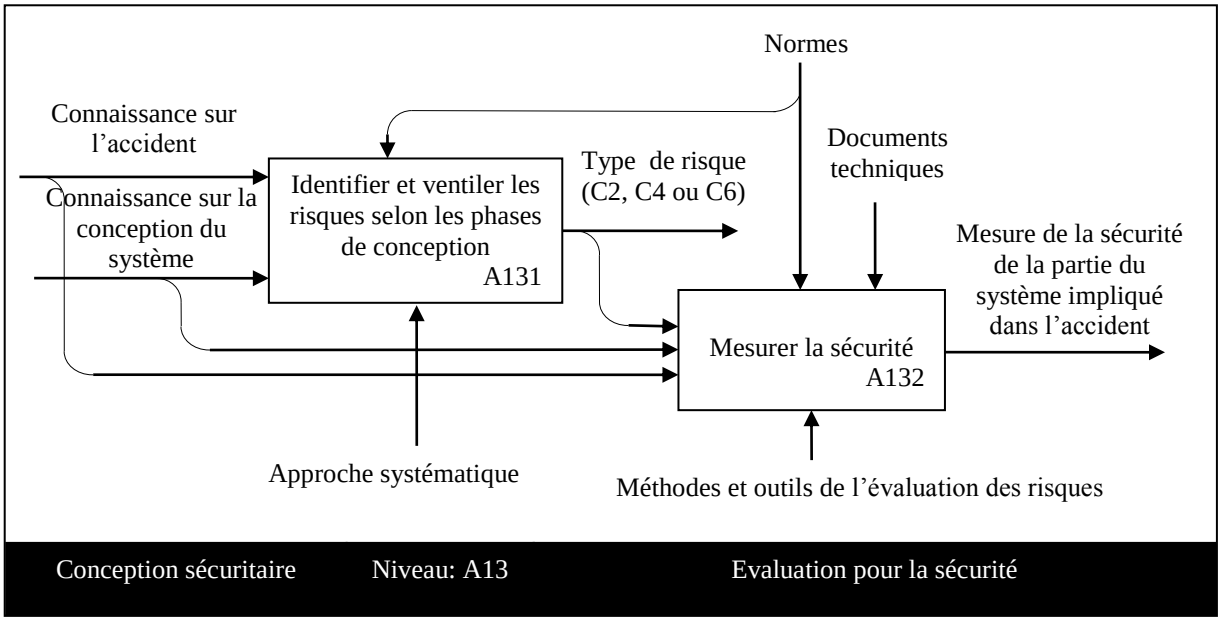


Figure 4.1. Diagramme IDEF0 niveau A13 du processus de conception sécuritaire.

Ce chapitre comporte deux sections principales. La section 4.2 propose une approche d'identification et de ventilation du risque selon les phases de la conception et la section 4.3 définit un indicateur de sécurité pour la prise de décision dans le processus de conception d'un système. Comme pour le chapitre 3, chacune de ces deux sections comporte cinq sous sections : l'introduction, l'état de l'art, le développement de l'approche, l'application de l'approche proposée à l'arbre de transmission à cardans, une conclusion, une discussion et les perspectives.

4.2. Développement d'une approche d'identification et de ventilation des risques selon les phases de la conception

4.2.1. Introduction

Comme nous l'avons mentionné précédemment, cette thèse vise à opérationnaliser la méthode IRAD. Dans le cadre de cette opérationnalisation, un des problèmes est de répondre à la question suivante: *Comment peut-on formuler les risques et les ventiler dans les trois phases du processus de conception?* L'objectif est d'identifier les risques liés à l'utilisation du système et de les ventiler selon les trois contextes de risque d'IRAD: **(C2)** les risques d'accident identifiés au niveau conceptuel ; **(C4)** les risques ergonomiques identifiés au niveau architectural ; **(C6)** les risques résiduels identifié au niveau détaillé.

La section 4.2.2 dresse un état de l'art sur la classification des risques dans les documents normatifs et scientifiques. Les classifications des trois phases de conception proposées dans le chapitre 3, nous conduisent à proposer une démarche d'identification et de ventilation de risque dans la section 4.2.3. La section 4.2.4 traite de l'utilisation de cette approche sur l'arbre de transmission à cardans. Enfin, nous concluons cette partie par une synthèse et les perspectives de recherche.

4.2.2. Etat de l'art sur la classification des risques

Ghemraoui a proposé les principes généraux de la ventilation des risques selon les trois phases de conception. Nous nous appuyons sur cette proposition ainsi que sur les normes relatives à la sécurité en conception pour opérationnaliser cette ventilation [Ghemraoui, 2009].

La première question qui se pose est : *Pourquoi faut-il ventiler les risques ?* Notre objectif est d'intégrer la sécurité au plus tôt dans la conception. Selon Bernard et Hasan [Bernard et Hasan, 2002], généralement, la sécurité intervient soit très tôt et retarde le concepteur, soit très tard et conduit à des modifications complexes et coûteuses. Cette constatation montre clairement la nécessité d'une démarche permettant une ventilation optimale des risques dans le processus de conception, c'est-à-dire introduire chaque exigence de sécurité au bon moment lors du processus de conception.

La deuxième question à laquelle il faut répondre est : *Comment peut-on classer les solutions techniques et déterminer la relation entre les risques et solutions?* Nous cherchons à trouver les règles qui ventilent les risques dans les trois contextes (C2, C4 et C6) proposés par IRAD. Chaque risque a pour origine un phénomène dangereux. Nous proposons donc de nous focaliser sur les origines des phénomènes dangereux. La classification des phénomènes dangereux n'est pas normalisée.

Dans la suite de cette partie, nous présentons la classification proposée dans le cadre de la méthode IRAD. Nous présentons ensuite les classifications des phénomènes dangereux existantes des points de vue normatif et scientifique. Enfin, nous concluons cette partie par une synthèse et un positionnement par rapport à nos objectifs.

4.2.2.1. IRAD et la ventilation des risques selon les trois phases de conception

Ghemraoui a proposé de ventiler les risques dans les trois contextes (C2, C4 et C6) relatifs aux trois phases physiques de la conception [Ghemraoui, 2009]. Nous détaillons ici les trois contextes utilisés et proposons de les modifier afin de les rendre plus facilement opérationnels.

Risque d'accident (C2) : ce risque est identifié au niveau conceptuel, donc lié à une solution de conception proposée au niveau de la conception **conceptuelle**. [Ghemraoui, 2009] considère qu'un phénomène dangereux est toujours généré par une source d'énergie et que la nature du risque qui en découle est dépendante de la nature de l'énergie considérée. Les origines des phénomènes dangereux liés aux risques C2 peuvent être par exemple un élément en rotation, l'effet du vide, etc.

Risque ergonomique (C4) : ce risque est identifié au niveau architectural, donc lié à une solution de conception proposée au niveau de la conception **architecturale**. Ce risque est relatif à la violation des limites humaines d'un point de vue ergonomique c'est-à-dire lié à la tâche. Les origines des phénomènes dangereux liés aux risques C4 peuvent être par exemple une posture, une vibration causée par un défaut d'alignement des pièces en mouvement, etc. Elles peuvent être également liées à l'éclairage local, liées à une activité répétitive ou encore à un effort. Les événements dangereux peuvent être l'inconfort causé par la vibration, des postures douloureuses et fatigantes, le stress, une perte de visibilité directe de la zone de travail, une manipulation répétitive à fréquence élevée, un effort excessif. Le risque C4 ne couvre pas seulement l'aspect ergonomie, mais aussi les aspects liés au non fiabilité technique.

L'ergonomie est considérée comme une discipline ayant pour objectif d'adapter la situation de travail en cherchant l'efficience du travail, mais surtout d'assurer la santé/sécurité des opérateurs [Neboit et al, 1990]. La norme [NF EN ISO 15535, 2013] définit le concept de l'anthropométrie comme l'étude et la mesure des dimensions physiques et de la masse du corps humain et de ses parties constitutives. Pour ces raisons, nous considérons qu'il est nécessaire de redéfinir le risque C4 comme **risque anthropométrique ou de non fiabilité technique**.

Risque résiduel (C6) : ce risque est identifié au niveau détaillé, donc lié à une solution de conception proposée au niveau de la conception **détaillée**. Ce type de risque reste relatif à la conception mais induit des effets minimes par rapport aux risques relatifs aux autres choix effectués au cours de la conception. Les origines des phénomènes dangereux liés aux risques C6 peuvent être, par exemple, liées à une texture de surface. Ces risques sont étroitement liés à l'usage fait du système. Pour cette raison, nous redéfinissons le risque C6 comme **risque d'usage**.

IRAD classe donc tous les risques sous trois contextes, mais ne propose pas de solution pour ventiler un risque donné dans l'un d'entre-eux. Notre objectif est ici de proposer une approche pour résoudre ce manquement d'IRAD.

4.2.2.2. La classification des risques du point de vue normatif

Selon la norme [NF EN ISO 12100, 2010], le phénomène dangereux est la source potentielle du dommage. Le phénomène dangereux peut provenir de la façon dont la machine est conçue et/ou de la manière dont elle est utilisée. L'annexe B de cette norme regroupe les phénomènes dangereux en 10 groupes en fonction de leur type:

- Phénomènes dangereux mécaniques ;
- Phénomènes dangereux électriques ;

- Phénomènes dangereux thermiques ;
- Phénomènes dangereux engendrés par le bruit ;
- Phénomènes dangereux engendrés par les vibrations ;
- Phénomènes dangereux engendrés par les rayonnements ;
- Phénomènes dangereux engendrés par des matériaux et des produits ;
- Phénomènes dangereux engendrés par le non-respect des principes ergonomiques ;
- Phénomènes dangereux associés à l'environnement dans lequel la machine est utilisée ;
- Combinaison de phénomènes dangereux.

Cette norme exprime que chaque phénomène dangereux peut être caractérisé par son origine (éléments coupants, éléments élastiques, …) et par la nature du dommage potentiel (choc électrique, coupure, …). Elle présente également des exemples d'origines et de conséquences possibles de phénomènes dangereux. Le tableau 4.1 présente des exemples d'origines et de conséquences possibles de phénomènes dangereux mécaniques.

Tableau 4.1. Exemples de phénomènes dangereux mécaniques [NF EN ISO 12100, 2010].

Origines	Conséquences possibles
– accélération, décélération; – pièces de forme aiguë; – rapprochement d'un élément en mouvement avec une pièce fixe; – éléments coupants; – éléments élastiques; – chute d'objets; – pesanteur; – hauteur par rapport au sol; – pression élevée; – instabilité; – énergie cinétique; – mobilité de la machine; – éléments en mouvement; – éléments en rotation; – surface rugueuse, glissante; – arêtes vives – énergie accumulée; – vide.	– renversement (par une machine mobile); – éjection; – écrasement; – coupure ou sectionnement; – entraînement ou emprisonnement; – happement, enroulement; – frottement ou abrasion; – choc; – injection; – cisaillement; – glissade, trébuchement et chute; – perforation ou piqûre; – suffocation.

4.2.2.3. La classification des risques du point de vue scientifique

D'une manière générale, un phénomène dangereux mécanique peut se produire lorsqu'une partie du corps humain entre en contact avec un élément mobile ou stationnaire de la machine ou lorsqu'une partie de la machine, de la pièce à usiner ou des fluides de travail sont éjectés de la machine [Caputo et al., 2013]. En partant de ce postulat, classer des phénomènes dangereux demande de répondre aux deux questions suivantes :

- *Quel est le principe de fonctionnement des éléments mobiles de la machine ?* et
- *Pour quelles raisons le corps d'une personne peut entrer en contact avec ces éléments mobiles ?*

Il existe différents travaux scientifiques de classification des risques et des phénomènes dangereux. L'INRS[4] [INRS, 2006] s'est inspiré de la norme NF EN ISO 12100, et a proposé la classification des risques mécaniques suivante :

- risque d'écrasement ;
- risque de cisaillement ;
- risque de coupure ou de sectionnement ;
- risque de happement, d'enroulement ;
- risque d'entrainement ou d'engagement ;
- risque de chocs ;
- risque de perforation ou de piqûre ;
- risque d'abrasion ;
- risque d'éjection de fluides sous haute pression ;
- risque de projection de pièces, outils, poussières, etc.

Les auteurs [INRS, 2006] ont également listé les principaux facteurs à prendre en compte concernant les éléments mécaniques, outils, pièces pouvant être à l'origine de risques mécaniques :

- leur forme : éléments coupants, arrête vives, etc. ;
- leur disposition relative pour les pièces en mouvement ;
- leur masse et leur stabilité (chute) ;
- leur masse et leur vitesse (énergie cinétique) ;
- leur accélération ;
- leur résistance mécanique (rupture, éclatement, flexion) ;
- leur énergie potentielle (ressorts, éléments élastiques, gaz et liquides sous pression).

Le CSST[5] et l'IRSST[6] [CSST et IRSST, 2008] ont utilisé le terme de « phénomènes mécaniques dangereux » qu'ils ont séparé en deux classes :

- Les phénomènes associés à des pièces et à des outils :
    - pièces et outils en mouvement ;
    - disposition relative des pièces et des outils en mouvement ;
    - angles rentrants (des rouleaux, des convoyeurs, etc.) ;
    - résistance mécanique inadéquate ;
    - formes dangereuses (tranchante, pointue, rugueuse, etc.).
- Les phénomènes associés à la gravité terrestre :
    - masse et stabilité (chute d'éléments ou d'un travailleur sous l'effet de leur poids).

Les auteurs présentent également les conséquences possibles de quelques exemples de phénomènes dangereux et listent trois facteurs à prendre en compte pour ces phénomènes:

- Masse, vitesse (énergie cinétique des éléments en mouvement contrôlé ou non contrôlé) ;
- Accélération, force ;
- Énergie potentielle, soit l'accumulation d'énergie à l'intérieur de la machine engendré par :

[4] *INRS :* Institut National de Recherche et de Sécurité
[5] *CSST* : Commission de la santé et de la sécurité du travail (commission québécoise)
[6] *IRSST :* Institut de recherche Robert-Sauvé en santé et en sécurité du travail (institut québécois)

- des éléments élastiques (ressorts, etc.) ;
- des gaz/des liquides sous pression (hydraulique, pneumatique, etc.) ;
- l'effet du vide/d'une pression.

4.2.2.4. Synthèse et positionnement par rapport à nos objectifs

La norme [NF EN ISO 12100, 2010] exprime chaque phénomène dangereux par son origine et par la nature du dommage potentiel sur l'homme. Ici nous faisons deux critiques sur la proposition de la norme :

1. La classification des origines de ces phénomènes n'est pas homogène. L'origine peut être :
   - un objet : par exemple un élément élastique ou un élément coupant ;
   - un paramètre physique : par exemple une accélération, une décélération ou une énergie cinétique ;
   - une forme : par exemple une pièce de forme aiguë, une surface rugueuse, glissante ou une arête vive ;
   - etc.
2. Elle ne montre pas les liens entre origines et conséquences (quelles origines entrainent telle ou telle conséquence).

Il faut également noter que cette norme ne se veut pas exhaustive en termes de phénomènes dangereux. La classification proposée ne couvre donc pas la totalité des origines et conséquences possibles.

La classification des risques mécaniques proposée par l'INRS [INRS, 2006] a été réalisée, tout comme la norme [NF EN ISO 12100, 2010], selon leurs conséquences possibles mais celle-ci en est différente. Les auteurs ont essayé d'y reclasser les origines, mais comme pour la classification proposée dans la norme, celle-ci n'est pas homogène.

La classification proposée par le CSST et l'IRSST [CSST et IRSST, 2008] est en partie basée sur la norme [NF EN ISO 12100, 2010]. Dans cette classification, les auteurs ont essayé de regrouper les origines par catégorie et d'identifier les conséquences pour chaque origine. Ce travail a pour avantage par rapport à la norme de faire le lien entre origines et conséquences des phénomènes dangereux. Cependant, et comme pour la classification proposée dans la norme, elle reste non homogène et non exhaustive.

Comme indiqué dans le §4.2.2.1, la méthode IRAD a l'avantage de proposer de ventiler les risques selon trois contextes (C2, C4 et C6) relatifs aux trois phases de la conception mais ne propose pas de méthode pour les ventiler. La norme [NF EN ISO 12100, 2010] fait état dans les méthodes de classification des risques. La preuve en est qu'elle est utilisée comme base dans les travaux scientifiques traitant de ce sujet. Nous proposons donc de combiner IRAD et la norme afin de proposer un mécanisme générique de classification des risques.

4.2.3. Développement d'une approche d'identification et de ventilation du risque

La ventilation du risque en fonction des phases de la conception demande, dans l'ordre :

- d'identifier la source du phénomène dangereux en faisant le lien entre la source des phénomènes dangereux et les conséquences possibles tel que défini dans la **norme** (par exemple « happement » et « élément en rotation ») ;

- de définir la solution de conception en fonction de la source du phénomène dangereux, (par exemple la solution de conception « élément en rotation » et « énergie mécanique ») ;
- de déterminer le lien entre chaque solution de conception et les phases de conception liées aux risques de types C2, C4 et C6 (par exemple la solution de conception « énergie mécanique » et la phase de conception conceptuelle P2 est liée à un risque de type C2).

Le mot « origine », utilisé dans la norme [NF EN ISO 12100, 2010] dans l'expression « Origine des phénomènes dangereux », indique soit le mouvement ou les caractéristiques d'un élément (« élément tournant », « chute d'objet », etc.) soit un paramètre physique (« énergie cinétique », « accélération », etc.). Dans la suite de ce document, nous décrirons les origines des phénomènes dangereux par leurs paramètres physiques. Pour cette raison, nous préférons adopter le terme « source » que celui d'« origine ». Nous nous basons également sur la synthèse réalisée ci-dessus afin de développer notre approche d'identification et de ventilation des risques dans les trois phases de la conception.

4.2.3.1. Identification de la source du phénomène dangereux

La première étape de la démarche consiste à identifier les sources des phénomènes dangereux. Celle-ci a déjà été décrite auparavant dans ce manuscrit.

Ainsi, dans le chapitre 3, nous avons proposé une approche d'ingénierie inverse fonctionnelle pour la sécurité (FRES) afin d'extraire des connaissances sur l'accident et des connaissances sur la conception de la partie du système impliquée dans l'accident. Dans le §3.2.3.2, nous proposons d'établir un ADC à partir des informations obtenues sur l'accident.

La lecture des différents niveaux de l'AdC permet de déterminer les conditions dangereuses (événement dangereux, situation dangereux et phénomène dangereux). A ce niveau, la source et la conséquence de l'ensemble des phénomènes dangereux sont identifiées ; la source du phénomène dangereux se trouvant au 3ème niveau.

4.2.3.2. Ventilation du risque

Une fois la source du phénomène dangereux identifiée, le lien entre celle-ci et une des trois phases de conception doit être établi. Dans le chapitre 3, après avoir présenté l'approche systématique développée par [Pahl et Beitz, 2007], nous avons fait une synthèse sur les caractéristiques influant sur la sécurité du système à chaque phase de la conception. Selon cette synthèse :

- **La phase de conception conceptuelle** est liée au principe de la solution. A cette phase, on s'intéresse en particulier aux caractéristiques énergétiques utilisée dans le principe de la solution retenue ;
- **La phase de conception architecturale** est liée à la structure de la solution. On s'intéresse donc ici aux caractéristiques spatiale et temporale, dimensionnelles, géométriques;
- **La phase de conception détaillée** est liée aux détails de la solution. Cette phase s'intéresse aux caractéristiques de forme des composants.

Nous nous basons sur la liste des sources des phénomènes dangereux mécaniques proposés dans la norme [NF EN ISO 12100, 2010] afin de trouver ce lien. Notre proposition est résumée dans le tableau 4.2. Tout d'abord, pour chaque source de phénomènes dangereux (tableau 4.2 - colonne 1), nous identifions le paramètre physique associé (tableau 4.2 - colonne 2). A partir des paramètres physiques identifiés, nous définissons une classification

plus générale (tableau 4.2 - colonne 3). Enfin, en comparant avec le processus de conception de la méthode IRAD, nous faisons le lien entre cette classification et les phases de conception (tableau 4.2 - colonne 4 et 5). Ainsi chaque source de phénomène dangereux est associée à une phase de la conception.

Tableau 4.2. Lien entre sources des phénomènes dangereux mécaniques et phase de la conception.

source des phénomènes dangereux mécaniques, 1er classification [NF EN ISO 12100, 2010]	**Paramètre physique associé**	**2ème classification**	**3ème classification**	**Phase de la conception**
énergie cinétique	énergie	énergies mécaniques	énergies	P2 lié au risque C2
accélération, décélération	accélération			
éléments en mouvement	vitesse			
éléments en rotation	vitesse			
rapprochement d'un élément en mouvement avec une pièce fixe	vitesse			
énergie accumulée	énergie			
éléments élastiques	énergie			
instabilité	énergie			
chute d'objets	accélération de la gravité			
mobilité de la machine	vitesse			
pression élevée	pression	énergies hydraulique et pneumatique		
vide	pression			
rapprochement d'un élément en mouvement avec une pièce fixe	distance	caractéristiques dimensionnelles	caractéristiques dimensionnelles et géométriques	P4 lié au risque C4
hauteur par rapport au sol	distance			
éléments coupants	angle	caractéristiques géométriques et formes fonctionnelles		
pièces de forme aiguë	angle			
pesanteur	poids			
surface rugueuse, glissante	rugosité	textures de surface	caractéristiques de forme	P6 lié au risque C6
arêtes vives	angle	formes non fonctionnelles		

La figure 4.2 ci-dessous illustre les caractéristiques de chaque phase de conception en lien avec les risques afin d'aider à la ventilation du risque (risque C2, C4 ou C6).

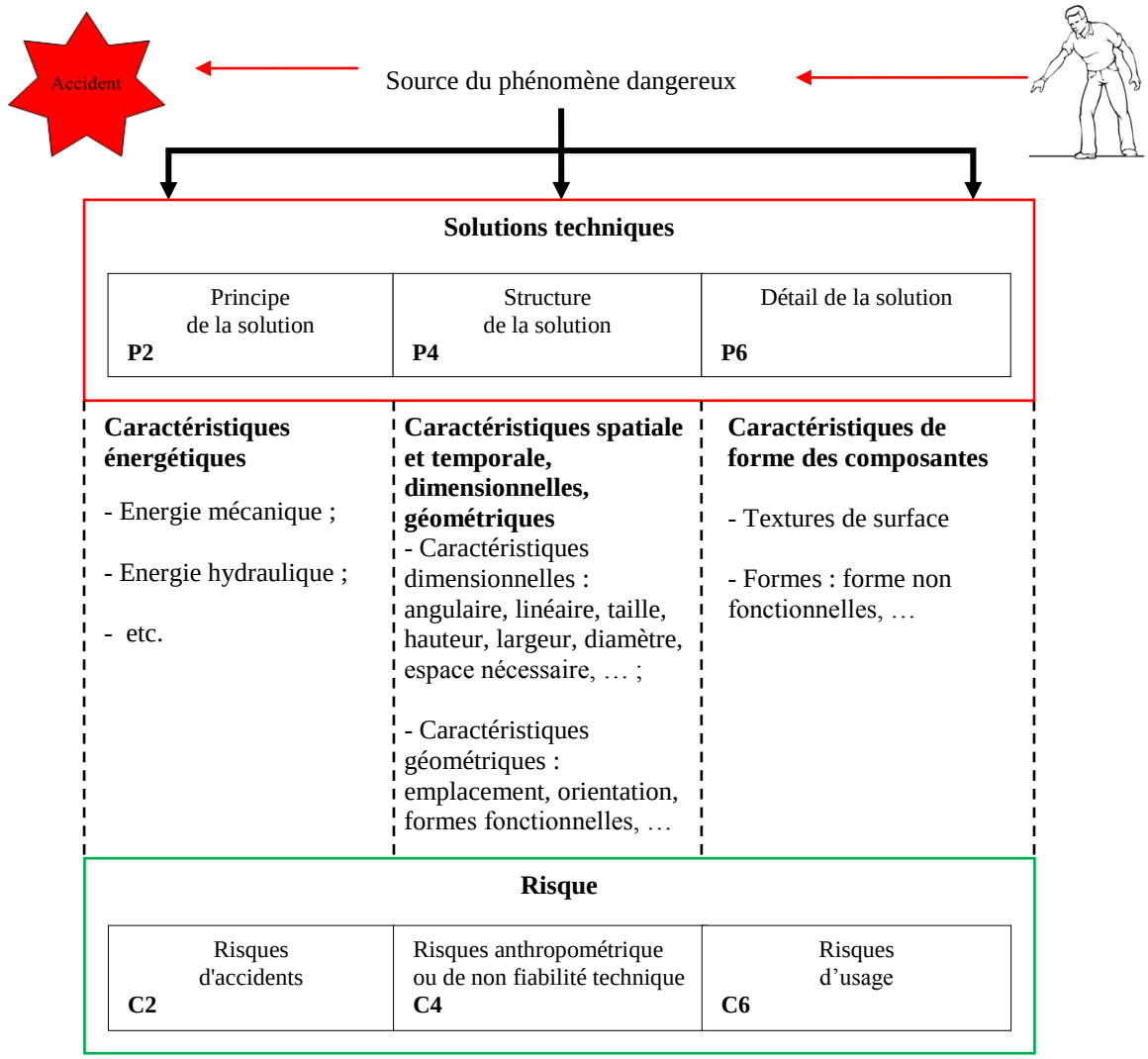


Figure 4.2. Exemples des caractéristiques liées à chaque phase de conception et types de risque associés.

4.2.3.3. Démarche d'identification et de ventilation du risque

Ventiler le risque selon les trois phases de conception demande de se poser une 1ère question : *Est-ce que la source du phénomène dangereux est liée à une énergie ?*

- Si la réponse à cette question est Oui, le risque est du type risque d'accident (C2).
- Si la réponse est Non, il convient de se poser une 2ème question : *Est-ce que la source du phénomène dangereux est liée à des caractéristiques dimensionnelles et géométriques?*
    - Si la réponse de cette question est Oui, le risque est du type risque anthropométrique ou de non fiabilité technique (C4).
    - Si la réponse est Non, il faut se poser la 3ème et dernière question : *Est-ce que la source du phénomène dangereux est liée à des caractéristiques de forme?*
        - Si la réponse à cette question est Oui, le risque est du type risque d'usage (C6).
        - Dans le cas contraire, il faut reconsidérer le phénomène dangereux et en ré-identifier la source.

La figure 4.3 décrit l'approche proposée. Son point de départ est les connaissances sur les accidents et sur la conception du système ; connaissances obtenues par la mise en œuvre

de la démarche FRES développée dans le chapitre précédent (chapitre 3). Les résultats obtenus sont l'identification de la source des phénomènes dangereux, la définition du type de risque associé et donc la phase de conception impactée.

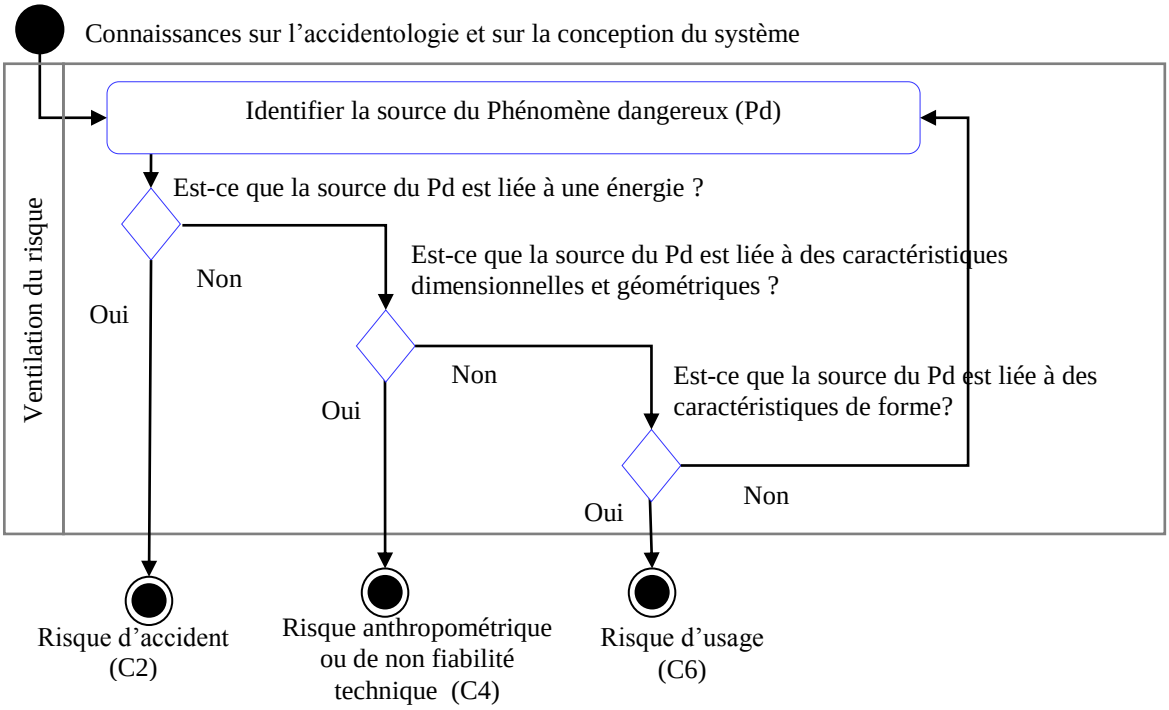


Figure 4.3. Ventilation des risques selon les trois phases de conception.

Dans la section suivante, nous évaluons cette approche par son application au cas de l'Arbre de Transmission à Cardans (ATC).

4.2.4. Application : identification et ventilation des risques liés à l'ATC

4.2.4.1. Identification de la source du phénomène dangereux lié à l'ATC

La mise en œuvre de la démarche FRES au cas de l'ATC (2ème partie du chapitre 3) a montré que les faits « Homme se tenant à proximité de l'ATC », « ATC fonctionne », et « Absence de protecteur ou protecteur endommagé ou mal ajusté » peuvent causer le « Happement par l'ATC ». L'AdC détaillé au §3.2.4.2 montre que la conséquence du phénomène dangereux est le « happement » et sa source un « élément en rotation ».

4.2.4.2. Ventilation du risque lié à l'ATC

La première étape consiste à répondre à la question : *Est-ce que la source du phénomène dangereux est liée à une énergie* ? Selon la classification des sources des phénomènes dangereux mécaniques et leur lien avec les phases de la conception présentée au §4.2.3.2 (tableau 4.2), « élément en rotation » est lié à l'énergie. La réponse à la question est donc positive.

Nous pouvons donc en conclure que le risque lié à ce phénomène dangereux est un risque d'accident (C2). Il faut noter que dans notre cas, c'est le système de protection de l'ATC qui est défectueux. Par conséquent, nous considérerons 2 systèmes par la suite: le système ATC sans moyen de protection d'un côté et le moyen de protection de l'ATC de l'autre.

4.2.4.3. Conclusions sur l'application

Dans cette section, nous avons appliqué la démarche d'identification et de ventilation du risque selon les trois phases de la conception au cas des accidents mettant en cause l'ATC.

La démarche a pu être appliquée dans son intégralité et a permis de déterminer le type de risque à partir de la source du phénomène dangereux identifiée. Ainsi, le risque lié à l'ATC est un risque défini au niveau de la conception conceptuelle, c'est-à-dire un risque d'accident (C2).

4.2.5. Conclusion

La finalité de cette partie était de proposer une approche d'identification et de ventilation des risques dans le cadre de l'opérationnalisation de la méthode IRAD. Pour cela, nous avons présenté un état de l'art sur les travaux effectués pour la classification des risques des points de vue normatif et scientifique. Ensuite, sur la base de ces travaux, nous avons proposé une approche permettant d'identifier et de ventiler les risques. L'approche proposée est basée (1) sur l'analyse des connaissances des accidents et de la conception du système, (2) sur les trois contextes C2, C4 et C6 de la méthode IRAD et (3) sur les travaux normatif portant sur la classification des sources des phénomènes dangereux. Un point pouvant être amélioré dans le futur est la liste des sources des phénomènes dangereux utilisée. Celle-ci correspond à celle donnée dans la norme [NF EN ISO 12100, 2010]. Elle permet de traiter la majorité des cas mais reste non exhaustive.

Cette approche a ensuite été appliquée au cas de l'ATC. Cette étape a montré l'applicabilité de la démarche et a produit le résultat principal suivant : le risque lié à l'ATC est un risque d'accident (risque type C2).

Connaissant le type de risque lié au phénomène dangereux identifié, il convient maintenant d'en déduire les objectifs de sécurité et les niveaux d'intervention envisageables lors du processus de conception afin d'améliorer la sécurité du système. Mais améliorer objectivement la sécurité demande de pouvoir la mesurer. Par conséquent, avant de traiter le problème de la définition des objectifs de sécurité, nous proposons de définir un indicateur de sécurité permettant de mesurer la qualité d'une solution de conception d'un point de vue sécuritaire.

4.3. Proposition d'un indicateur de sécurité pour l'évaluation du niveau de sécurité d'un système

4.3.1. Introduction

Comme nous l'avons exprimé précédemment, l'objectif général de cette thèse est de proposer un processus itératif d'aide à la décision pour l'intégration de la sécurité dans les trois phases de conception. Les questions qui se posent ici sont : *Qu'est-ce qu'une conception sécuritaire? Et comment objectiver ce concept ?* En d'autres termes, il convient ici de répondre à la question : *comment peut-on mesurer la sécurité ?*

Cette section du chapitre 4 est structurée de la manière suivante : La section 4.3.2 est consacrée à l'état de l'art concernant la problématique de l'évaluation et de la mesure de la sécurité et du risque des points de vue normatif et scientifique. Les principes, les objectifs et la nécessité de construire un indicateur de sécurité adapté au processus de conception sont détaillés dans la section 4.3.3. La démarche générale qui a été suivie pour la définition d'un indicateur de sécurité est ensuite présentée dans la section 4.3.4. Cette démarche se base sur la définition de la sécurité et des conditions dangereuses (des éléments entrainant un dommage). Enfin, l'applicabilité de l'approche est montrée dans la section 4.3.5 sur l'Arbre de Transmission à Cardans (ATC). La section 4.3.6 clôt cette partie par une conclusion.

4.3.2. Etat de l'art sur l'évaluation, la mesure de la sécurité et du risque

L'évaluation du risque, qu'est-ce que c'est ? L'évaluation du risque, pour faire quoi ? Le terme d'évaluation du risque est défini dans la norme [NF EN ISO 12100, 2010] comme un « jugement destiné à établir, à partir de l'analyse du risque, si les objectifs de réduction du risque ont été atteints ». Cette évaluation du risque s'intègre dans un processus d'appréciation du risque, lui-même inclus dans un processus de réduction du risque. L'issue de ce processus fait suite à une comparaison de risques ayant pour résultat une réduction du risque de manière adéquate.

Cette norme précise également qu'« *au cours du processus d'évaluation du risque, les risques inhérents à la machine ou à des parties de la machine peuvent être comparés à ceux d'une machine ou de parties de la machine similaires* », sous réserve que les conditions suivantes soient remplies : machine similaire conforme à la norme pertinente de type C, phénomènes dangereux, éléments de risques, spécifications techniques et conditions d'utilisations, utilisation normale, mauvais usage raisonnablement prévisible, conception et construction des deux machines comparables.

Les trois étapes nécessaires à une évaluation du risque sont : une collecte d'informations sur le risque; une appréciation critique (un jugement de valeur) pour le risque ; et des propositions qui contribuent à une prise de décision afin d'éliminer ou de réduire le risque.

Dans cette section, nous présentons un état de l'art sur l'évaluation, la mesure de la sécurité et du risque basé sur les documents normatifs et les travaux scientifiques. Elle se conclut par une synthèse sur l'évaluation et la mesure de la sécurité et du risque.

4.3.2.1. L'évaluation et la mesure de la sécurité et du risque du point du vue normatif

Comme nous l'avons déjà cité précédemment, selon la norme [NF EN ISO 12100, 2010], le risque associé à une situation dangereuse particulière dépend de la gravité du dommage et de la probabilité d'occurrence de ce dommage. Le tableau 4.3 ci-dessous reprend les mots liés au risque et leur définition selon les normes.

Tableau 4.3. Les différents concepts relatifs au risque.

Terme français	**Traduction anglaise**	**Définition**
Estimation du risque	Risk estimation	Définition de la gravité probable d'un dommage et de la probabilité de ce dommage
Analyse du risque	Risk analysis	Combinaison de la détermination des limites de la machine, de l'identification des phénomènes dangereux et de l'estimation du risque
Évaluation du risque	Risk evaluation	Jugement destiné à établir, à partir de l'analyse du risque, si les objectifs de réduction du risque ont été atteints
Appréciation du risque	Risk assessment	Processus global d'analyse et d'évaluation du risque
Réduction du risque	Risk reduction	Réduction du risque répondant au moins aux exigences légales, l'état de la technique du moment étant pris en considération

L'estimation de la gravité du dommage et de la probabilité d'occurrence de ce dommage doit se faire par la prise en compte de nombreux facteurs. Ces facteurs sont résumés dans le tableau 4.4 ci-dessous.

Selon cette norme, [NF EN ISO 12100, 2010], les aspects à considérer pendant l'estimation du risque sont : les personnes exposées ; le type, la fréquence et la durée d'exposition ; le rapport entre l'exposition et les effets ; les facteurs humains ; l'applicabilité des mesures de prévention ; la possibilité de neutralisation ou de contournement des mesures de prévention ; la capacité à maintenir les mesures de prévention ; et les informations pour l'utilisation.

Tableau 4.4. Estimation de la gravité et de la probabilité d'occurrence d'un dommage.

Risque		**Les facteurs à prendre en compte lors de l'estimation**
Gravité du dommage		- la gravité des lésions ou de l'atteinte à la santé - l'étendue du dommage
Probabilité d'occurrence d'un dommage	**Exposition des personnes au phénomène dangereux**	- le besoin d'accès à la zone dangereuse - la nature de l'accès - le temps passé dans la zone dangereuse - le nombre de personnes devant pouvoir y accéder - la fréquence d'accès
	Occurrence d'un événement dangereux	- les données de fiabilité et autres données statistiques - l'historique d'accidents - l'historique des atteintes à la santé - la comparaison de risques
	Possibilité d'éviter ou de limiter le dommage	- les différentes personnes susceptibles d'être exposées au(x) phénomène(s) dangereux - le laps de temps permettant une réaction - la conscience du risque - l'habileté humaine d'éviter ou de limiter le dommage - l'expérience et la connaissance pratique

Selon la norme [FD ISO/TR 14121-2, 2008], la plupart des outils d'estimation du risque disponibles utilisent l'une des méthodes suivantes : matrice des risques, graphe des risques, évaluation numérique, estimation quantifiée du risque, outils hybrides. Le tableau 4.5 résume ces outils et présente quelques-uns de leurs avantages et inconvénients.

Tableau 4.5. Outils d'estimation du risque.

Outil		**Définition**	**Avantages**	**Inconvénients**
Estimation qualitative du risque	**Matrice des risques**	est un tableau à plusieurs dimensions permettant de combiner n'importe quel type de gravité du dommage avec la probabilité d'occurrence de ce dommage	- simple d'utilisation	- dépend de l'avis d'expert
	Graphe des risques	se base sur un arbre décisionnel. Chaque nœud du graphe représente un paramètre du risque et chaque branche partant d'un nœud représente une classe du paramètre	- illustre le taux de réduction du risque fourni par une mesure de protection et le paramètre qu'elle influence	- devient encombré et illisible s'il comprend plus de deux branches pour plus d'un paramètre du risque

	Evaluation numérique	a de deux à quatre paramètres scindés en plusieurs classes, de la même manière que les matrices de risques ou les graphes de risques	- les systèmes de cotations permettent de pondérer les paramètres de façon simple et explicite	- l'utilisation de nombres peut fournir une impression d'objectivité en ce qui concerne le niveau de risque, même si l'attribution de valeurs pour chaque élément de risque est fortement subjective
Estimation quantifiée du risque		consiste en un calcul mathématique, aussi précis que possible avec les données disponibles, de la probabilité d'un résultat spécifique se produisant pendant une durée spécifique	- permet de comparer le risque calculé avec des critères ayant trait à un chiffre réel de décès par an ou de statistiques d'accidents	- demande beaucoup de ressources et nécessite des compétences considérables pour être menée avec succès ; - nécessite un modèle détaillé et complet de la chaîne d'événements conduisant au résultat défini et dépend de la qualité des données relatives aux événements de base ; - peut être subjective et sujette à des erreurs.
Outils hybrides		combine deux des approches d'estimation du risque. Il s'agit communément de graphes de risque contenant soit des matrices, soit des systèmes de score pour l'un des éléments à risque.	- incorporer un certain degré de quantification dans n'importe quelle approche qualitative	

Cette synthèse montre que, dans la proposition de la norme, les résultats dépendent de l'avis d'experts. Le niveau de sécurité d'un système obtenu de cette façon est donc expert-dépendante.

4.3.2.2. L'évaluation et la mesure de la sécurité et du risque du point de vue scientifique

Cette partie présente un état de l'art sur l'évaluation et la mesure de la sécurité issu des travaux scientifiques.

D'après [Øien, 2011a], dans le domaine de la sécurité et jusque dans les années 80, les termes les plus souvent utilisés étaient indice, taux et mesure. Depuis, le terme d'indicateur est communément utilisé.

Qu'est-ce qu'un indicateur ? D'après [Hellevik, 1999 cité dans Øien, 2011a], un indicateur est la définition mesurable/opérationnelle d'une variable théorique. Il s'agit d'une variable opérationnelle. [Øien, 2011a] propose de combiner ces deux définitions et parvient à la définition suivante : un indicateur est une variable mesurable/opérationnelle qui peut être utilisée pour décrire les conditions d'un phénomène ou un aspect de la réalité.

Dans le domaine de la sécurité, on trouve deux types d'indicateurs : les indicateurs de risque [Øien, 2001a ; Øien, 2001b] et les indicateurs de sécurité [Coulibaly et al., 2008 ; Øien et al., 2011a ; Øien et al., 2011b]. Ces deux types d'indicateurs sont souvent utilisés indifféremment les uns des autres. [Øien et al., 2011a] explique les différences qui les caractérisent. Selon ces auteurs, un indicateur de risque doit être inclus dans un modèle de risque (tel qu'un modèle probabiliste des risques) de manière à pouvoir déterminer les effets sur le risque d'un changement de la valeur de l'indicateur, alors qu'un indicateur de sécurité peut être élaboré à partir de différentes approches comme une approche basée sur la performance en terme de sécurité ou une approche basée sur les incidents.

Øien propose deux types d'indicateurs de risque dans ces travaux: Un indicateur de risque technique [Øien, 2001a] et un indicateur de risque organisationnel [Øien, 2001b]. Dans [Øien, 2001a], Øien présente une méthode générale pour la mise en place d'indicateurs de

risque technique. Cette méthode est basée sur l'analyse quantitative des risques (QRA : Quantitative Risk Analysis). Pour cela, il propose un facteur d'influence de risque (RIF : Risk Influencing Factor) qu'il définit comme un aspect d'un système ou d'une activité affectant le niveau de risque d'un système/d'une activité. Selon lui, l'indicateur est une représentation mesurable du RIF. Pour cela, Øien liste les facteurs d'influence de risque (RIF_i) et pour chaque facteur, il identifie l'indicateur de risque (X_i) et calcule son effet sur le risque en utilisant l'équation suivante :

$$\begin{cases} \dfrac{\Delta R\ (0,t)}{R(0)} \approx \sum_{i=1}^{n} \left\{ \left[\dfrac{X_i(t) - X_i\ (0)}{X_i(0)} \right] K_i \right\} \quad et \quad K_i = \dfrac{\dfrac{\Delta R_{i,N}(0,t)}{R(t)}}{\dfrac{\Delta \theta_{i,N}(0,t)}{\theta_i(t)}} \\ avec: \\ \Delta R\ (0,t): mesure\ relative\ du\ changement\ du\ risque\ sur\ une\ période\ de\ temps\ (de\ 0\ à\ t) \\ R(0): mesure\ de\ risque\ à\ t = 0 \\ X_i(0): indicateur\ de\ risque\ du\ ième\ paramètre\ à\ t = 0 \\ X_i(t): indicateur\ de\ risque\ du\ ième\ paramètre\ à\ l'instant\ t \\ K_i: constante\ pour\ le\ ième\ paramètre\ de\ 0\ à\ t \\ \theta_i(t): paramètre\ du\ risque \\ \Delta\theta_{i,N}(0,t): valeur\ du\ paramètre\ du\ risque\ du\ ième\ paramètre\ de\ 0\ à\ t \end{cases} \qquad Equation\ (4-1)$$

Cet indicateur est essentiellement basé sur l'analyse quantitative des risques et sur ses facteurs d'influence. Il permet de mesurer les changements du niveau de risque mais ne permet pas de mesurer un niveau de risque absolu.

[Øien, 2001b] traite de la définition d'un indicateur de risque organisationnel. Il y propose d'établir cet indicateur en utilisant l'équation suivante :

$$\begin{cases} \dfrac{\Delta R\ (0,t)}{R(0)} = K_\lambda \left(\dfrac{E(\lambda(t)\ |OF(t), \neq Obs(t))}{E(\lambda)_0} - 1 \right) \\ avec: \\ K_\lambda: facteur\ de\ sensibilité\ normalisée\ pour\ le\ paramètre\ de\ fréquence\ de\ fuite \\ E(\lambda)_0: valeur\ attendue\ du\ paramètre\ de\ fréquence\ de\ fuite \\ OF(t): Informations\ sur\ les\ nouveaux\ états \\ \neq Obs(t): nombre\ de\ fuites\ observées \end{cases} \qquad Equation\ (4-2)$$

[Coulibaly et al. 2008] ont proposé des indicateurs pour la prédiction de la maintenabilité et de la sécurité dans les premières phases de la conception de produits mécanisés. L'indicateur relatif à la sécurité s'exprime par la multiplication de deux valeurs : le facteur de risque (FRis) et l'indice de risque (IRis).

$$I_S: \begin{cases} I_S = FRis\ \times IRis \\ avec: \\ FRis: facteur\ de\ risque \\ IRis: indice\ de\ risque \end{cases} \qquad Equation\ (4-3)$$

Le facteur de risque (FRis) est une valeur binaire qui indique l'existence d'un risque ou non. Ils proposent d'évaluer cette valeur grâce à l'équation suivante :

$$FR_{iS}: \begin{cases} FR_{iS} = Ph \times Zo\ \times HIn \\ avec: \\ Ph: Présence\ d'un\ phénomène\ dangereux \\ Zo: Présence\ d'une\ zone\ dangereuse \\ HIn: Intervention\ de\ l'homme\ dans\ la\ zone\ identifiée \end{cases} \qquad Equation\ (4-4)$$

Selon cette équation, si Fris=0, le système ne présente pas de risque. Mais si FRis=1, le concepteur doit tenter de modifier l'un de ces paramètres : Ph, Zo ou HIn afin d'annuler la

valeur de cet indicateur. Dans le cas où c'est impossible, le concepteur doit déterminer l'indice de risque (IRis) afin de quantifier le risque et vérifier qu'il est acceptable ou non. IRis est une valeur numérique (mesurable). Cette valeur est exprimée par l'équation suivante :

$$IR_{iS}: \begin{cases} IR_{iS} = Gr \times Ex \times Pr \times Av & Equation\ (4-5) \\ avec: \\ Gr: Gravité\ du\ risque \\ Ex: Durée\ et\ fréquence\ d'exposition \\ Pr: Probabilité\ de\ l'évenement\ dangereux \\ Av: Probabilité\ d'éviter\ le\ phénémone\ dangereux\ et\ l'accident\ ou\ l'incident \end{cases}$$

Les valeurs numériques de Gr, Ex, Pr et Av sont estimées par des experts, en se fixant sur des échelles de valeurs selon les niveaux. Une fois qu'I_S est déterminé, le concepteur doit alors comparer sa valeur avec les valeurs de références proposées par son entreprise ou la comparer avec les solutions alternatives.

4.3.2.3. Synthèse sur l'évaluation, la mesure de la sécurité et du risque

Dans le chapitre 3, nous avons présenté les conditions dangereuses correspondant aux causes du dommage. Nous considérons qu'il faut prendre en compte ces conditions pour mesurer le niveau de sécurité d'un système. Nous avons également pointé, à partir de l'analyse des différents rapports d'accident, le fait qu'un accident peut être causé par une défaillance ou une mauvaise conception (conception non sécuritaire), par un facteur non prévu lié à l'humain ou lié à l'environnement. Ces différents facteurs doivent donc être considérés lors de la mesure de la sécurité. De plus, la mesure de la sécurité doit se faire dès la conception conceptuelle. L'aspect conception du système est donc un élément clé. Les questions auxquelles nous devons répondre ici sont :

- *Existe-il un indicateur de sécurité développé antérieurement répondant à nos besoins ?*
- *Dans le cas où celui-ci n'existe pas, pouvons-nous adapter un des indicateurs présentés dans l'état de l'art pour répondre à notre besoin ou faut-il en développer un nouveau ?*

L'état de l'art présenté ci-dessus montre que les conditions dangereuses, l'aspect de conception du système et la qualité de la conception ne sont pas pris en compte dans le développement des indicateurs existants.

L'indicateur de sécurité répondant au mieux à notre besoin est celui présenté dans [Coulibaly et al., 2008]. Cet indicateur a été développé pour être appliqué pendant la conception. Les conditions dangereuses y sont également intégrées. Cependant, il ne répond pas à l'intégralité du cahier des charges que nous nous sommes fixé:

- Cet indicateur ne peut s'appliquer que dans la phase de conception architecturale. Or, dans nos travaux, nous avons besoin de mesurer la sécurité dès la conception conceptuelle.
- Il se base sur l'estimation d'un expert pour la détermination de différentes valeurs numériques rentrantes dans son expression comme la gravité, la probabilité d'occurrence de l'événement dangereux, etc. Or, nous cherchons à éviter au maximum à avoir recours à un expert afin d'avoir un indicateur le plus objectif possible.
- Bien que [Coulibaly et al., 2008] précisent que la probabilité de l'événement dangereux est fonction de la fiabilité de l'humain et la fiabilité intrinsèque du système, ils ne proposent pas de lien entre leurs indicateurs de maintenabilité et de sécurité ni des indications pour calculer la fiabilité de l'humain. La méthode IRAD souligne le

lien entre la sécurité et le couplage entre les exigences fonctionnelles du système. Nous considérons que la probabilité d'occurrence de l'événement dangereux n'est pas simplement fonction de la fiabilité du système mais également fonction de sa qualité de conception en général.

- Dans [Coulibaly et al., 2008], la présence d'un protecteur ou d'un système de protection n'est pas spécifiquement traitée. Dans notre cas, nous considérons les moyens de protection comme un système à part entière et nous souhaitons pouvoir évaluer le niveau de sécurité du système avec et sans protecteur.

Nous avons donc fait le choix de nous baser sur l'indicateur de sécurité proposé par [Coulibaly et al.2008] en l'adaptant afin de répondre aux critiques faites ci-dessus.

4.3.3. Définition d'un indicateur de sécurité, I_S

Comme défini dans le chapitre 1 de ce manuscrit, la sécurité est « l'absence de **danger** ou de conditions de créer un **risque**». Cette formulation est la base de la définition de l'indicateur de sécurité proposé ici :

$$I_S : \begin{cases} I_S = f_1(P_D, N_R) \\ avec: \\ P_D : Présence\ de\ Danger \\ N_R : Niveau\ de\ Risque \end{cases} \qquad Equation\ (4-6)$$

Cet indicateur de sécurité est donc dépendant de deux paramètres, la Présence de Danger, P_D, caractérisant la présence ou l'absence de danger et un Niveau de Risque, N_R. L'avantage de cette formulation de la sécurité et de cette définition est qu'elle ne fait pas intervenir directement la notion de risque en tant que telle (où la probabilité d'occurrence de l'événement dangereux est souvent difficile à estimer et où la gravité du dommage probable varie selon l'expert) mais plus précisément la notion de conditions dangereuses entrainant un dommage (le phénomène dangereux, la situation dangereuse et l'événement dangereux). Dans la section qui suit, nous décrivons les caractéristiques et le mode de calcul des deux paramètres P_D et N_R.

Nous souhaitons que la valeur finale d'I_S soit sans dimension. En conséquence, les valeurs prises par l'ensemble des paramètres utilisés dans le calcul seront comprises entre 0 et 1. La valeur de l'I_S sera comprise entre 0 et 1 et, plus cette valeur sera élevée, plus le système sera sécuritaire.

4.3.4. Caractéristiques de l'indicateur de sécurité, I_S

4.3.4.1. Présence de Danger, P_D

Comme cela a été précisé dans le chapitre 3, le phénomène dangereux est la source potentielle du dommage. L'événement dangereux est l'événement susceptible de causer un dommage et la situation dangereuse est le contexte dans lequel une personne est exposée à au moins un phénomène dangereux. Ceci se traduit par l'équation suivante :

$$P_D : \begin{cases} P_D = f_2(P_{Pd}, P_{Sd}, P_{Ed}) \\ avec: \\ P_{Pd}: Présence\ d'un\ Phénomène\ dangereux \\ P_{Sd}: Présence\ d'une\ Situation\ dangereuse \\ P_{Ed}: Présence\ d'un\ Evénement\ dangereux \end{cases} \qquad Equation\ (4-7)$$

Le P_D, est une valeur binaire. Il vaut 1 si la solution évaluée comporte, au moins, un phénomène dangereux, une situation dangereuse et un événement dangereux. Nous pouvons expliquer la relation entre P_D, P_{Pd}, P_{Sd}, et P_{Ed} comme suit :

- S'il n'y a pas de phénomène dangereux, on ne peut pas avoir de situation dangereuse et $P_D = 0$;
- S'il y a un phénomène dangereux, on peut avoir une situation dangereuse ou non. S'il n'y a pas de situation dangereuse, $P_D = 0$. S'il existe une situation dangereuse, nous considérons que l'accident est toujours probable. Dans ce cas, un événement dangereux est possible et $P_D = 1$.

Reconcevoir de façon plus sécuritaire un système demande d'une part d'identifier le niveau de sécurité apporté par le système et ensuite celui apporté par le système équipé de ses moyens de protection. Ainsi, il est ensuite possible d'agir sur le système, ses moyens de protection ou sur les deux. Dans notre travail, nous considérons que les moyens de protection, les solutions de protection ajoutées pour améliorer la sécurité du système, sont des systèmes à part entière. Dans la suite, nous utilisons le mot « système » pour l'ensemble «système sans moyens de protection » et « moyens de protection ». Le tableau 4.6 détaille l'ensemble des combinaisons des valeurs possibles des trois indices P_{Pd}, P_{Sd} et P_{Ed} et les valeurs de P_D pour chacune de ces combinaisons pour un système sans moyen de protection.

Tableau 4.6. Valeurs prises par la Présence de Danger pour un système sans moyen protection (P_{Dssmp}).

P_{Pd}	P_{Sd}	P_{Ed}	P_{Dssmp}
0	0	0	0
1	0	0	0
1	1	1	1

Nous pouvons exprimer le résultat précédent par l'équation booléenne suivante :

$$P_{Dssmp}: \{P_{Dssmp} = P_{Pd} \,\&\, P_{Sd} \,\&\, P_{Ed} \qquad Equation\ (4-8)$$

Concernant la Présence de Danger pour le moyen de protection (P_{Dmp}), deux cas sont possibles :

- **La Présence de Danger pour le système sans moyen de protection est égale à 1 ($P_{Dssmp} = 1$)**. Le risque provient du système sans moyen de protection. Dans ce cas, quelles que soient les conditions dangereuses pour le moyen de protection, la P_{Dmp} est considérée égale à 1 (voir tableau 4.7.a).
- **La Présence de Danger pour le système sans moyen de protection est égale à 0 ($P_{Dssmp} = 0$)**. Le système sans moyen de protection ne présente pas de risque. Comme nous l'avons décrit au-dessus, nous considérons le moyen de protection comme un système à part entière. La table de vérité est dans ce cas identique à la table de vérité du système sans moyen de protection (voir tableau 4.7.b).

Tableau 4.7. Valeurs prises par la Présence de Danger pour le moyen protection (P_{Dmp}) (a) dans le cas où $P_{Dssmp} = 1$ et (b) dans cas où $P_{Dssmp} = 0$.

(a) $P_{Dssmp} = 1$

P_{Pd}	P_{Sd}	P_{Ed}	P_{Dmp}
0	0	0	1
1	0	0	1
1	1	1	1

(b) $P_{Dssmp} = 0$

I_{PPd}	I_{PSd}	I_{PEd}	P_{Dmp}
0	0	0	0
1	0	0	0
1	1	1	1

Nous pouvons exprimer ce résultat par l'équation booléenne suivante :

$$P_{Dmp}: \left\{P_{Dmp} = P_{Dssmp} \mid (P_{Pd} \,\&\, P_{Sd} \,\&\, P_{Ed})\right. \qquad Equation\ (4-9)$$

4.3.4.2. Niveau de Risque, N_R

Dans la section précédente, la présence de danger a été établie à partir des éléments entrainant un dommage. De la même manière, le niveau de risque est lié à ce dommage et donc au phénomène dangereux, à la situation dangereuse et à l'évènement dangereux. Le Niveau de Risque (N_R) peut s'exprimer sous la forme suivante :

$$N_R : \begin{cases} N_R = f_3(N_{RPd}, N_{RSd}, N_{REd}) \\ avec: \\ N_{RPd} : Niveau\ de\ Risque\ lié\ au\ Phénomène\ dangereux \\ N_{RSd} : Niveau\ de\ Risque\ lié\ à\ la\ Situation\ dangereuse \\ N_{REd} : Niveau\ de\ Risque\ lié\ à\ l'Evénément\ dangereux \end{cases} \qquad Equation\ (4-10)$$

L'évaluation du niveau de risque, N_R, nécessite donc l'évaluation des niveaux de risque liés au phénomène dangereux, à la situation dangereuse et à l'évènement dangereux, respectivement N_{RPd}, N_{RSd} et N_{REd}.

Niveau de Risque lié au Phénomène dangereux, N_{RPd}

L'impact d'un phénomène dangereux sur le niveau de risque est lié à la notion d'incompatibilité entre les paramètres du système, en lien avec ce phénomène, et les caractéristiques de l'humain. Pour un phénomène dangereux donné, nous proposons d'évaluer cette incompatibilité en comparant la valeur du paramètre par rapport à un seuil correspondant à la valeur limite maximale de ce paramètre pouvant être supportée par l'humain. Le Niveau de Risque lié au Phénomène dangereux (N_{RPd}) sera exprimée comme suit :

$$N_{RPd} : \begin{cases} N_{RPd} = 1 - \dfrac{V_{seuil}}{V} & si \quad V > V_{seuil} \\ N_{RPd} = 0 & si \quad V \leq V_{seuil} \\ avec: \\ V : Valeur\ liée\ au\ phénomène\ dangereux\ caractérisant\ le\ système\ étudié \\ V_{seuil} : Valeur\ seuil\ coorespondante\ supportée\ par\ l'humain \end{cases} \qquad Equation\ (4-11)$$

Nous considérons qu'il existe trois niveaux de risque à déterminer ; chacun d'eux étant lié à une phase de la conception. Nous détaillons les modes de calcul des Niveaux de Risque lié au Phénomène dangereux pour chaque phase de la conception dans les sections suivantes.

. N_{RPd} en lien avec les risques d'accident (C2)

L'impact du phénomène dangereux en lien avec les risques d'accident (C2) sur le niveau de risque est basé sur la valeur de l'énergie dégagée par le phénomène dangereux. Nous nommons ce niveau d'énergie E. L'humain peut supporter de l'énergie jusqu'à un certain niveau selon son type. Nous nommons cette valeur maximale de l'énergie supportée par l'humain, E_{seuil}. L'incompatibilité entre les caractéristiques physiques du système et les caractéristiques de l'humain s'exprime donc sous la forme : E_{seuil}/E. Le N_{RPd} en lien avec les risques d'accident peut s'exprimer comme suit :

$$N_{RPd}\ en\ lien\ avec\ C2 : \begin{cases} N_{RPd} = 1 - \dfrac{E_{seuil}}{E} & si \quad E > E_{seuil} \\ N_{RPd} = 0 & si \quad E \leq E_{seuil} \\ avec: \\ E : valeur\ de\ l'énergie\ dégagée\ par\ le\ phénomènedangereux \\ E_{seuil} : valeur\ maximale\ de\ l'énergie\ supportée\ par\ l'humain \end{cases} \qquad Equation\ (4-12)$$

Il convient cependant de souligner que les valeurs seuils des énergies supportées par l'humain ne sont pas disponibles dans les normes. Quelques articles parus dans le domaine de la biomécanique [Kleiven, 2007 ; LaPlaca et al., 2007] proposent de telles valeurs.

. N_{RPd} en lien avec les risques anthropométriques et de non fiabilité technique (C4)

Selon la norme [NF EN 614-1+A1:2009] pour la conception des machines, il est nécessaire de prendre en compte les caractéristiques ergonomiques suivantes:

- les dimensions corporelles, les postures, les mouvements du corps et la force physique des personnes ;
- les capacités mentales ;
- l'influence de l'environnement physique du travail sur les personnes.

L'analyse ergonomique à réaliser doit non seulement s'attacher aux principes ergonomiques (morphologie de l'humain, force physique, posture et mouvement), mais aussi aux cinq sens de l'humain. Nous devons, en conséquence, considérer les phénomènes dangereux engendrés par le bruit, les vibrations, les rayonnements, etc. Nous proposons de classer les phénomènes dangereux liés à l'ergonomie en quatre catégories:

- Phénomènes dangereux engendrés par le bruit [NF EN ISO 9612, 2009 ; NF EN ISO 11688-1, 2009 ; NF EN ISO 11688-2, 2004] ;
- Phénomènes dangereux engendrés par les vibrations [NF EN 1299+A1, 2009] ;
- Phénomènes dangereux engendrés par les rayonnements [NF EN 12198-1, 2008] ;
- Phénomènes dangereux engendrés par le non-respect des principes ergonomiques :
  - Morphologie de l'humain [NF EN 1005-2+A1, 2008; NF EN 1005-3+A1, 2008] ;
  - Force physique [NF ISO 11228-2, 2007] ;
  - Posture et mouvement [NF EN 1005-4, 2008].

Pour chaque catégorie, nous citons les références normatives précisant les valeurs seuils. Nous nommons X la valeur de bruit, de vibration, de rayonnement ou de non-respect des principes ergonomiques engendrée par le système. L'humain peut supporter une valeur seuil pour chaque catégorie. Nous le nommons X_{seuil}. Par conséquent, le niveau de risque lié au phénomène dangereux en lien avec les risques anthropométriques et de non fiabilité technique peut s'exprimer de la manière suivante :

$$N_{RPd}\ en\ lien\ avec\ C4: \begin{cases} N_{RPd} = 1 - \dfrac{X_{seuil}}{X} & si \quad X > X_{seuil} \\ N_{RPd} = 0 & si \quad X \leq X_{seuil} \\ avec \\ X: valeur\ de\ bruit, de\ vibration, \dots issue\ du\ système \\ X_{seuil}: valeur\ maximale\ de\ bruit, de\ vibration, \dots supportée\ par l'humain \end{cases} \qquad Equation\ (4-13)$$

. N_{RPd} en lien avec les risques d'usage (C6)

Les risques d'usage sont liés aux caractéristiques de forme et aux propriétés des matériaux. L'expression du N_{RPd} en lien avec ce type de risque est identique à celle en lien avec les risques anthropométriques et de non fiabilité technique.

$$N_{RPd}\ en\ lien\ avec\ C6: \begin{cases} N_{RPd} = 1 - \dfrac{Y_{seuil}}{Y} & si \quad Y > Y_{seuil} \\ N_{RPd} = 0 & si \quad Y \leq Y_{seuil} \\ avec : \\ Y: valeur\ issue\ du\ système \\ Y_{seuil}: valeur\ maximale\ supportée\ par\ l'humain \end{cases} \qquad Equation\ (4-14)$$

Niveau de Risque lié à la Situation dangereuse, N_{RSd}

Les situations dangereuses sont les circonstances dans lesquelles une personne est exposée à, au moins, un phénomène dangereux. L'exposition d'une personne résulte souvent de la réalisation d'une tâche sur la machine. Le Niveau de Risque lié à la Situation dangereuse (N_{RSd}) est égal au rapport entre le temps d'exposition de l'opérateur au phénomène dangereux pendant un cycle de travail complet (T) et la durée du cycle de travail (T_{ref}).

$$N_{RSd} : \begin{cases} N_{RSd} = T / T_{ref} \\ avec: \\ T : temps\ d'exposition\ de\ la\ persone \\ T_{ref} : durée\ du\ cycle\ de\ travail \end{cases} \qquad Equation\ (4-15)$$

Le cycle de travail sera défini en fonction de la phase de travail concernée. En phase d'utilisation normale de la machine, le temps d'utilisation sera soit égal au nombre d'heures de travail par jour, si le travail sur la machine est quotidien et continu, soit égal au nombre d'heures de fonctionnement de (ou de travail sur) la machine dans une journée. En phase de maintenance, de nettoyage, d'entretien, …, la durée du cycle sera la durée totale de la phase.

Niveau de Risque lié à l'Evénement dangereux, N_{REd}

Comme nous l'avons mentionné précédemment, l'Evénement dangereux (Ed) est l'événement susceptible de causer un dommage. Dans le chapitre 3, section « Analyse du rapport formel d'accident », nous avons vu qu'un accident peut être causé par le système, par l'humain, par l'environnement ou par une combinaison de ces facteurs. L'Ed est donc fonction de Facteurs liés au système (F_{Rs}), à l'humain (F_{Rh}) et à l'environnement (F_{Re}). Le Niveau de Risque lié à l'Evénement dangereux (N_{REd}) peut donc s'exprimer de la façon suivante :

$$N_{REd} : \begin{cases} N_{REd} = f_4(F_{Rs}, F_{Rh}, F_{Re}) \\ avec: \\ F_{Rs} : Facteurs\ de\ Risque\ liés\ au\ système \\ F_{Rh} : Facteurs\ de\ Risque\ liés\ à\ l'humain \\ F_{Re} : Facteurs\ de\ Risque\ liés\ l'environnement \end{cases} \qquad Equation\ (4-16)$$

La suite de ce paragraphe présente le calcul de Facteurs de Risque liés au système (F_{Rs}), à l'humain (F_{Rh}) et à l'environnement (F_{Re}).

Facteurs de Risque liés au système, F_{Rs}

Pour calculer le Facteur de Risque lié au système (F_{Rs}), il faut en évaluer la conception. Pour réaliser cette évaluation, nous proposons de nous baser sur la satisfaction des deux axiomes de la conception axiomatique. Ainsi, le facteur de risque lié au système est fonction de la Qualité de la conception (Q_c) et du Niveau de fiabilité (N_f) du système:

$$F_{Rs} : \begin{cases} F_{Rs} = f_5(Q_c, N_f) \\ avec: \\ Q_c : Qualité\ de\ la\ conception \\ N_f : Niveau\ de\ fiabilité \end{cases} \qquad Equation\ (4-17)$$

Obtenir F_{Rs} nécessite donc évaluer Q_c et N_f. Comme pour l'ensemble des facteurs détaillés jusqu'ici, ce facteur aura une valeur comprise entre 0 et 1.

Qualité de conception (Q_c): Selon la conception axiomatique, une bonne conception est une conception sans couplage entre les exigences fonctionnelles. De plus, selon la méthode IRAD, une conception couplée est une conception non sécuritaire. Nous proposons que la Qualité de la conception, Q_c, soit exprimée sous la forme d'une valeur binaire, de la façon suivante :

$$Q_c : \begin{cases} Q_c = 1\ si\ \exists\ couplage \\ Q_c = 0\ si\ \nexists\ couplage \end{cases} \qquad Equation\ (4-18)$$

Niveau de fiabilité (N_f): Dans la Norme [NF EN ISO 12100, 2010], la fiabilité a été définie comme l'aptitude d'une machine, ou de ses composants ou équipements, à accomplir sans défaillance une fonction requise, dans des conditions données et pendant un laps de temps donné. La fiabilité correspond donc ici à un non-fonctionnement du système ou une partie du système dans des conditions données pendant un temps donné. Selon la norme [NF EN ISO13849-1, 2008], pour mesurer la fiabilité, il faut disposer d'informations sur la durée de vie. Celles-ci peuvent être issues d'historiques ou le fruit d'une expérience sur le système. Donc le Niveau de fiabilité (N_f) peut s'exprimer en fonction de la durée de vie avant défaillance et la durée de vie souhaitée :

$$N_f : \begin{cases} N_f = 0 & si \;\; Dvad > Dvs \\ N_f = 1 - \dfrac{Dvad}{Dvs} & si \;\; Dvad \leq Dvs \\ Dvad : Durée\ de\ vie\ avant\ défaillance \\ Dvs : Durée\ de\ vie\ souhaitée \end{cases} \qquad Equation\ (4-19)$$

Il convient de noter que le couplage dans le système peut être identifié dès la phase de la conception conceptuelle. La qualité de la conception, Qc, peut donc être évaluée dès la première phase de la conception. Le niveau de fiabilité, Nf, quant à lui, ne peut être évalué une fois que les composants du système conçus ont été sélectionnés donc à partir de la phase de la conception architecturale. Pour évaluer le niveau de sécurité d'un système dès la phase de sa conception conceptuelle, nous considérons que, à cette phase, le niveau de fiabilité est optimale et donc que Nf = 0. Le niveau de sécurité, représenté par l'indicateur Is, aura une valeur plus précise avec l'avancement de la conception.

Sachant que nous souhaitons obtenir une valeur comprise entre 0 et 1, nous proposons de définir le facteur de risque lié au système de la façon suivante :

$$F_{Rs} : \begin{cases} F_{Rs} = \dfrac{(\alpha_1 Q_c + \alpha_2 N_f)}{\alpha_1 + \alpha_2} \\ \alpha_1 : coefficient\ de\ pondération\ Q_c \\ \alpha_2 : coefficient\ de\ pondération\ \ de\ \ N_f \end{cases} \qquad Equation\ (4-20)$$

Nous considérons que $\alpha_1 > \alpha_2$, la qualité de la conception (Q_c) ayant plus d'influence sur le système car pouvant être évaluée dès la phase de conception conceptuelle.

Facteur de Risque lié à l'humain, F_{Rh}

Les facteurs humains doivent être pris en compte dans la mesure de l'E_d. Les facteurs de risque liés aux humains incluent plusieurs caractéristiques tels que la formation, l'expérience, l'état physique, les aspects liés au stress, aux capacités mentales c'est-à-dire la capacité de l'opérateur à contrôler la machine et à exécuter les tâches requises [NF EN ISO 12100, 2010]. Nous considérons pour la suite quatre classes de facteurs humains :

- **F_{Rh1}: la formation.** Ce facteur vaut 1 si l'opérateur n'a pas reçu une formation adéquate pour savoir utiliser le système. Il vaut 0 dans le cas contraire.
- **F_{Rh2}: l'expérience.** Pour une personne sans expérience, ce facteur prend la valeur 1. Pour une personne expérimentée, ce facteur vaut 0.
- **F_{Rh3}: l'état physique.** Pour un opérateur aux capacités physiques limitées, ce facteur vaut 1 et 0 sinon.
- **F_{Rh4}: l'attitude.** Nous considérons ici le stress, la fatigue, les préoccupations, etc. de l'opérateur. Si celui-ci à une mauvaise attitude, ce facteur prend la valeur 1 sinon la valeur 0.

Il faut noter qu'il est possible d'ajouter d'autres facteurs et que chacun d'eux peut être pondéré. Le Facteur de Risque lié à l'humain peut se formuler de la manière suivante :

$$F_{Rh}: \begin{cases} F_{Rh} = \dfrac{\sum_{i=1}^{n} \beta_i F_{Rhi}}{\sum_{i=1}^{n} \beta_i} \\ avec: \\ n: \ nombre\ des\ facteurs\ considérés \\ F_{Rhi} : i^{ème}\ facteur; \ \forall\ i\ ,\ F_{Rhi} = 0,1 \\ \beta_i : coefficient\ de\ pondération\ pour\ le\ i^{ème}\ facteur \end{cases} \qquad Equation\ (4-21)$$

Facteur de Risque lié à l'environnement, F_{Re}

Selon la norme [NF EN ISO 12100, 2010], l'environnement de travail est l'ensemble des facteurs physiques, chimiques, biologiques, organisationnels, sociaux et culturels qui entourent un travailleur. Le nombre de facteurs est donc important. Afin d'en simplifier le calcul, nous avons regroupé une liste non exhaustive de ces facteurs environnementaux en trois classes :

- **F_{Re1}: présence d'autres personnes**. On considère que F_{Re1}=1 si d'autre personne sont présentes dans l'environnement de travail sinon F_{Re1}=0.
- **F_{Re2}: environnement fermé ou ouvert**. On considère que F_{Re2}=1 si l'environnement de travail est ouvert sinon F_{Re2}=0.
- **F_{Re3}: milieu structuré ou naturel**. On considère que F_{Re3}=1 si l'environnement de travail est naturel sinon F_{Re3}=0.

Nous considérons donc ici comme prépondérant le fait que l'environnement du système est mieux maitrisé lorsque le système se trouve dans un milieu non accessible aux tiers, fermé (donc sans imprévus liés au climat, à la luminosité, etc.), et structuré (donc sans imprévus liés au sol, à la présence d'objets, d'obstacles, etc.). Comme déjà indiqué dans le chapitre 3, nous considérons que le système ne peut être utilisé que par un seul opérateur. Toute autre personne que l'opérateur est considérée comme faisant partie de l'environnement. Le Facteur de Risque lié à l'environnement (F_{Re}) peut être défini de la façon suivante :

$$F_{Re}: \begin{cases} F_{Re} = \dfrac{\sum_{j=1}^{m} \gamma_j F_{Rej}}{\sum_{j=1}^{m} \gamma_j} \\ avec: \\ m : nombres\ des\ facteurs\ considérés \\ F_{Rej} : j^{ème}\ facteur \qquad \forall\ j\ ,\ F_{Rej} = 0,1 \\ \gamma_j :\ coefficient\ de\ pondération\ pour\ le\ j^{ème}\ facteur \end{cases} \qquad Equation\ (4-22)$$

Niveau de risque lié à l'Evénement dangereux (N_{REd})

Comme indiqué précédemment, l'événement dangereux est fonction de facteurs de risque liés au système, à l'humain et à l'environnement. Par conséquent, le N_{REd} dépend des trois facteurs F_{Rs}, F_{Rh} et F_{Re}. Ces trois facteurs pouvant avoir des poids différents suivant le type de système étudié. Le Niveau de risque lié à l'Evénement dangereux (N_{REd}) peut donc être calculé de la façon suivante :

$$N_{REd}: \begin{cases} N_{REd} = \dfrac{(\delta_1 F_{Rs} + \delta_2 F_{Rh} + \delta_3 F_{Re}\ )}{\sum \delta} \\ avec: \\ \delta_1 : coefficient\ de\ pondération\ pour\ le\ F_{Rs} \\ \delta_2 : coefficient\ de\ pondération\ pour\ le\ F_{Rh} \\ \delta_3 : coefficient\ de\ pondération\ pour\ le\ F_{Re} \end{cases} \qquad Equation\ (4-23)$$

Définition du Niveau de Risque (N_R) du système

Comme déjà détaillé auparavant (équation (7)), le Niveau de Risque attribué au système (N_R) est basé sur le Niveau de Risque lié au phénomène dangereux, N_{RPd}, au niveau de risque lié à la situation dangereuse, N_{RSd}, et au niveau de risque lié à l'Evénement dangereux, N_{REd}. Suivant l'ordre de priorité de réduction de risque proposé dans la norme [FD ISO/TR 14121-2, 2008], nous proposons de pondérer les niveaux de risque. Ainsi, le Niveau de Risque peut s'exprimer de la façon suivante :

$$N_R : \begin{cases} N_R = \dfrac{(\varepsilon_1 N_{RPd} + \varepsilon_2 N_{RSd} + \varepsilon_3 N_{REd})}{\sum \varepsilon} \\ avec: \\ \varepsilon_1 : coefficient\ de\ pondération\ pour\ le\ niveau\ de\ risque\ lié\ au\ Pd \\ \varepsilon_2 : coefficient\ de\ pondération\ pour\ le\ niveau\ de\ risque\ lié\ à\ la\ Sd \\ \varepsilon_3 : coefficient\ de\ pondération\ pour\ le\ niveau\ de\ risque\ lié\ à\ l'Ed \end{cases} \qquad Equation\ (4-24)$$

En s'appuyant sur l'idée de catégorisation proposé dans la norme [NF EN ISO 12100, 2010], nous considérons que $\varepsilon_1 > \varepsilon_2 > \varepsilon_3$.

Il faut noter ici, qu'en cas de présence de plusieurs phénomènes dangereux dans la solution de conception ou le système étudié, le niveau de risque sera calculé pour le phénomène qui présente la valeur ($N_{Pd} + N_{Sd}$) la plus grande.

Définition du Niveau de Risque (N_R) pour les moyens de protection

Comme nous l'avons déjà cité dans le § 4.4.4.2, nous considérons qu'un moyen de protection est un système à part entière. Par exemple, nous considérons le protecteur de l'arbre de transmission à cardans comme un système. Nous avons présenté comment obtenir la valeur du Niveau de Risque (N_R) du système sans moyen de protection. De la même façon, il est possible d'obtenir le N_R attribué aux moyens de protection.

4.3.4.3. Définition de l'Indicateur de Sécurité, I_S

L'indicateur de sécurité peut s'exprimer de la façon suivante :

$$I_S : \{I_S = 1 - P_D \times N_R \qquad Equation\ (4-25)$$

Nous avons considéré le « système » pour l'ensemble «système sans moyens de protection » et « moyens de protection » (voir §4.3.4.1). Le système pouvant être sans ou avec un ou plusieurs moyens de protection, il convient de distinguer chaque élément. Dans ce sens, nous appelons **I**ndicateur de **S**écurité pour le **s**ystème, I_{Ss}, **I**ndicateur de **S**écurité pour le **s**ystème **s**ans **m**oyen de **p**rotection, I_{Sssmp} et **I**ndicateur de **S**écurité pour les **m**oyens de **p**rotection, I_{Smp}. Sachant qu'I_{Ss} doit avoir une valeur comprise entre 0 et 1 et qu'un système sécuritaire est un système avec un I_{Ss} élevé, l'indicateur de sécurité pour le système, c'est-à-dire le système combiné à ses moyens de protection, peut donc être défini de la manière suivante :

$$\begin{cases} I_{Ss} = \dfrac{\mu_1 I_{Sssmp} + \mu_2 \left(\dfrac{\sum_{z=1}^{n} I_{Smp\ z}}{n}\right)}{\mu_1 + \mu_2} \\ avec: \\ I_{Ss} : Indicateur\ de\ sécurité\ pour\ le\ système \\ I_{Sssmp} : Indicateur\ de\ sécurité\ de\ système\ sans\ moyens\ de\ protection \\ I_{Smp\ z} : Indicateur\ de\ sécurité\ du\ z^{ème}\ moyen\ de\ protection \\ \mu_1 : coefficient\ de\ pondération\ pour\ I_{Sssmp} \\ \mu_2 : coefficient\ de\ pondération\ pour\ I_{Smp} \\ n : nombre\ de\ moyen\ de\ protection \end{cases} \qquad Equation\ (4-26)$$

Nous considérerons que $\mu_1 > \mu_2$. Nous n'avons ici ni distingué, ni pondéré les différents types de moyen de protection. Une des perspectives de nos travaux est la prise en compte de cet aspect dans l'I_S.

4.3.4.4. Démarche de calcul de l'Indicateur de Sécurité, I_S

La Figure 4.4 détaille la démarche permettant de calculer l'indicateur de sécurité. Elle se décompose en quatre parties :

- le calcul de la Présence de Danger (P_D) ;
- la définition du Niveau de Risque (N_R) ;
- la définition de l'Indicateur de Sécurité du système sans moyen de protection (I_{Sssmp}) et l'Indicateur de Sécurité des z moyens de protection (I_{Smp}) ; et enfin,
- la définition de l'Indicateur de Sécurité du système (I_{Ss}).

Pour le système sans moyen de protection, nous considérerons z=0 et nous proposons une démarche générale. Voici une brève description des étapes de la démarche :

1. **Définir P_D pour le $z^{ième}$ système :** la démarche commence par le calcul de la Présence de Danger (P_D) pour le système à partir de connaissances sur l'accident et la conception.
2. **Définir N_{RPd} pour le $z^{ième}$ système :** la deuxième étape a pour objectif de définir le Niveau de Risque lié au Phénomène dangereux (N_{RPd}) après calcul des N_R lié aux Phénomènes dangereux en lien avec les risques d'accident, les risques anthropométriques et de non fiabilité technique et les risques d'usage.
3. **Définir N_{RSd} pour le $z^{ième}$ système:** la troisième étape demande de définir le Niveau de Risque lié à la Situation dangereuse (N_{RSd}).
4. **Définir N_{REd} pour le $z^{ième}$ système:** la quatrième étape a pour objectif de définir le Niveau de Risque lié à l'Evénement dangereux (N_{REd}) après avoir définis les Facteurs de Risque liés au système (F_{Rs}), à l'humain (F_{Rh}) et à l'environnement (F_{Re}).
5. **Définir N_R pour le $z^{ième}$ système:** cette étape a pour objectif de définir le Niveau de Risque (N_R) après avoir défini les N_{RPd}, N_{RSd} et N_{REd}. En cas de présence de plusieurs phénomènes dangereux, le niveau de risque sera calculé pour le phénomène qui présente la valeur ($N_{Pd} + N_{Sd}$) la plus élevée.
6. **Définir I_S pour le $z^{ième}$ système:** dans cette étape, nous obtenons l'Indicateur de Sécurité (I_s) calculé pour le $z^{ième}$ système. Il convient alors de recommencer la démarche jusqu'à ce que z =n (n étant égal au nombre de moyens de protection).
7. **Définir I_{Ss}:** Enfin, l'étape finale permet de définir l'Indicateur de Sécurité pour le système.

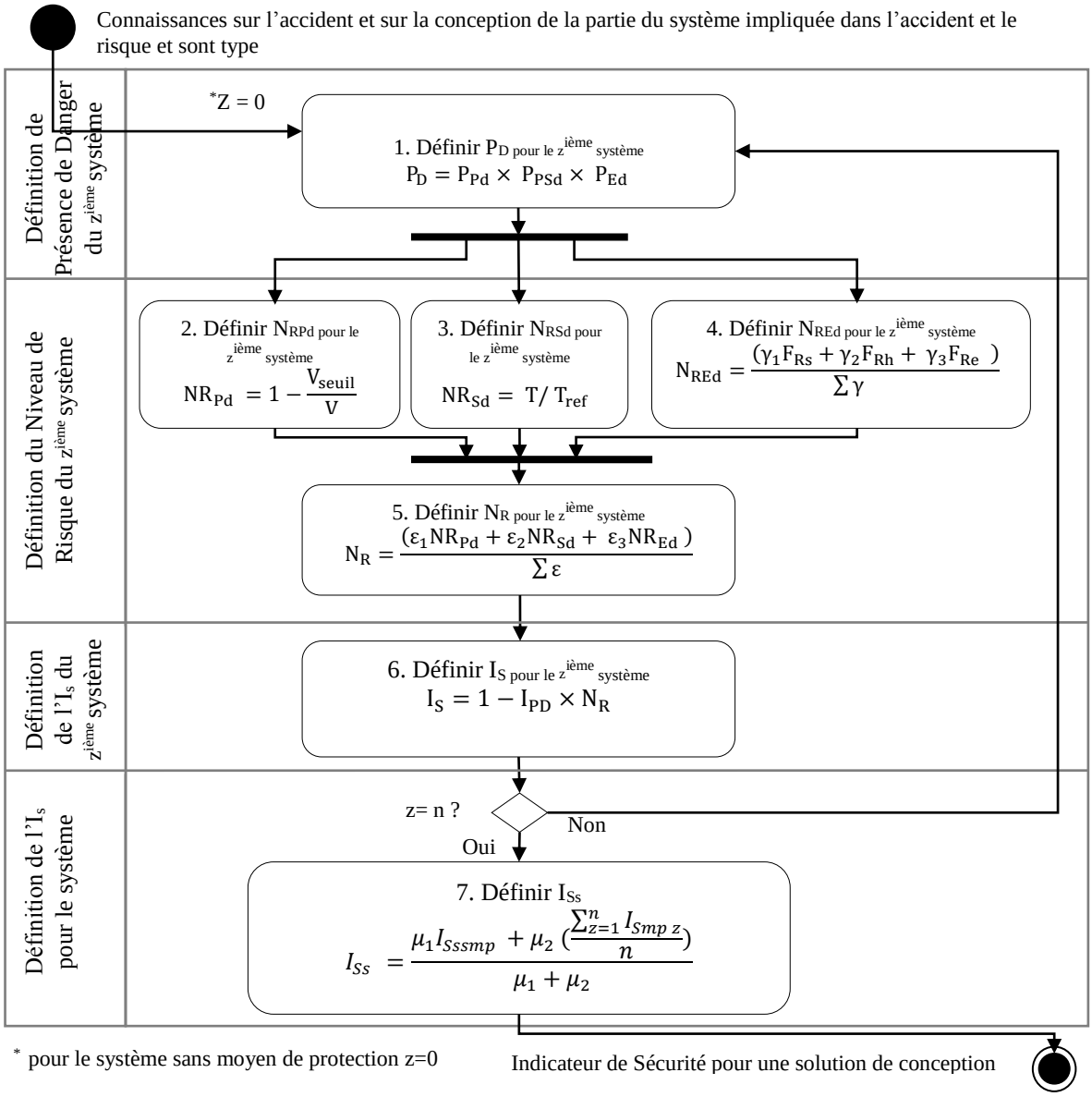


Figure 4.4. Synthèse et démarche pour le calcul de l'indicateur de sécurité.

4.3.5. Application : définition de l'Indicateur de Sécurité de l'ATC

4.3.5.1. Définition de l'Indicateur de Sécurité de l'ATC sans moyen de protection

L'objectif de cette section est de montrer, par l'application à un cas concret, la validité de la méthode proposée et l'intérêt de calculer l'indicateur de sécurité.

Définition de la Présence de Danger (P_D) de l'ATC sans moyen de protection

Dans cette étape, doit être calculée la Présence de Danger de l'ATC sans moyen de protection. Il s'agit d'identifier P_{Pd}, P_{Sd} et P_{Ed} en répondant aux trois questions suivantes à partir de connaissances obtenues suite à l'analyse de rapports formels d'accident (chapitre 3).

- P_{Pd} : Est-ce que la solution comporte un Phénomène dangereux ou non ? La solution, c'est-à-dire l'arbre mobile dégage de l'énergie cinétique. Il y a donc bien présence d'un phénomène dangereux. Donc : $P_{Pd} = 1$.
- P_{Sd} : Est-ce que la solution comporte une Situation dangereuse ou non? l'opérateur pouvant se tenir à proximité de la source d'énergie cinétique, la solution comporte donc une Situation dangereuse : $P_{Sd} = 1$.

- P_{Ed} : Est-ce que la solution comporte un Evénement dangereux ou non ? Un humain peut entrer en contact avec la source d'énergie cinétique. La solution comporte donc un Evénement dangereux. Donc : $P_{Ed} = 1$.

D'après le tableau 4.6 rappelé ci-dessous, comme $P_{Pd} = P_{Sd} = P_{Ed} = 1$, $P_{Dssmp} = 1$ pour l'ATC sans moyen de protection.

Tableau 4.6. Valeurs prises par la Présence de Danger pour un système sans moyen protection (P_{Dssmp}).

P_{Pd}	P_{Sd}	P_{Ed}	P_{Dssmp}
0	0	0	0
1	0	0	0
1	1	1	1

Définition du Niveau de Risque (NR) de l'ATC sans moyen de protection

Dans cette étape, nous devons calculer le Niveau de Risque (N_R) de l'ATC sans ses moyens de protection. Pour cela nous devons calculer les N_{RPd}, N_{RSd} et N_{REd}.

. Niveau de Risque lié au Phénomènes dangereux (N_{RPd})

Comme expliqué dans le chapitre 3, lorsque l'arbre de transmission fonctionne sans protecteur ou avec un protecteur endommagé ou mal ajusté et qu'un humain se tient à proximité de l'arbre de transmission, il y a un risque pour l'humain de happement par l'élément en rotation. La source du phénomène dangereux (rotation de l'arbre) est donc en lien ici avec un risque d'accident. Le calcul du Niveau de Risque lié à ce phénomène dangereux doit être fait en utilisant l'équation (4-12).

$$N_{RPd}\ en\ lien\ avec\ C2: \begin{cases} N_{RPd} = 1 - \dfrac{E_{seuil}}{E} & si \quad E > E_{seuil} \\ N_{RPd} = 0 & si \quad E \leq E_{seuil} \\ avec: \\ E: valeur\ de\ l'énergie\ dégagée\ par\ le\ phénomènedangereux \\ E_{seuil}: valeur\ maximale\ de\ l'énergie\ supportée\ par\ l'humain \end{cases} \qquad Equation\ (4-12)$$

L'énergie mise en jeu est l'énergie cinétique. Le niveau d'énergie se formule donc de la façon suivante :

$$E: \begin{cases} E = E_r = \frac{1}{2} I\ \omega^2 \\ avec: \\ E_r: energie\ cinétique \\ I: moment\ d'inertie \\ \omega: vitesse\ de\ rotation\ de\ l'ATC \end{cases} \qquad Equation\ (4-27)$$

De la même façon, le niveau d'énergie seuil, E_{seuil}, peut être défini par l'équation (4-28) :

$$E_{seuil}: \begin{cases} E_{seuil} = E_r = \dfrac{1}{2} I \omega_{seuil}^2 \\ avec: \\ \omega_{seuil}: vitesse\ de\ rotation\ supporté\ par\ l'humain, ou\ ne\ causant\ pas\ de\ \ danger\ à\ l'humain \end{cases} \qquad Equation\ (4-28)$$

En intégrant ces deux équations dans l'équation pour calculer le niveau de Risque lié à un Phénomène dangereux (équation 4-12), on obtient l'équation suivante :

$$N_{RPd}: \left\{ N_{RPd} = 1 - \frac{E_{seuil}}{E} = 1 - \left(\frac{\omega_{seuil}}{\omega}\right)^2 \right. \qquad Equation\ (4-29)$$

Selon les documents techniques, le couple à la prise de force du tracteur est de 1600 Nm au minimum. Pour qu'un corps humain de 70 kg et dont le centre de masse se trouve à 25

cm de l'axe de rotation de l'arbre soit soulevé par l'arbre tournant, celui-ci doit fournir un couple de 175 Nm, c'est-à-dire quasiment 10 fois inférieur au couple fourni par l'ATC. Si nous considérons le même facteur de proportionnalité entre la vitesse de rotation de l'ATC et la vitesse seuil supportée et ne causant pas de danger à l'humain, nous obtenons :

$$N_{RPd} = 1 - \left(\frac{0,1}{9}\right)^2 = 0,9998$$

. Niveau de Risque lié à la Situation dangereuse (N_{RSd})

Dans cette étape, nous définissons le Niveau de Risque lié à la Situation dangereuse (N_{RSd}). Pour cela, nous appliquons l'équation (4-15).

$$N_{RSd} : \begin{cases} N_{RSd} = T / T_{ref} \\ avec: \\ T : \ temps\ d'exposition\ de\ la\ persone \\ T_{ref} : durée\ du\ cycle\ de\ travail \end{cases} \qquad Equation\ (4-15)$$

Celle-ci demande de déterminer les deux valeurs T et T_{ref}. En se basant sur les rapports d'accident existants et sur les autres éléments du REX. Le temps d'exposition de l'opérateur au phénomène dangereux pendant un cycle de travail complet est, en moyenne, de 30 minutes ; temps calculé sur la durée d'un cycle de travail de 12 heures. Le N_{RSd} de l'ATC peut donc être calculé :

$$N_{RSd} = \frac{T}{T_{ref}} = \frac{0,5}{12} = 0,041$$

. Niveau de Risque lié à l'Evénement dangereux (N_{REd})

Facteur de Risque lié au système (F_{Rs}) : Pour déterminer N_{REd}, il faut tout d'abord définir le F_{Rs} en utilisant l'équation (4-20).

$$F_{Rs}: \begin{cases} F_{Rs} = \dfrac{(\alpha_1 Q_c + \alpha_2 N_f)}{\alpha_1 + \alpha_2} \\ \alpha_1 : coefficient\ de\ pondération\ Q_c \\ \alpha_2 : coefficient\ de\ pondération\ de\ N_f \end{cases} \qquad Equation\ (4-20)$$

Pour déterminer la valeur de F_{Rs} de l'ATC, la Qualité de conception (Q_c) et le Niveau de fiabilité (N_f) de l'ATC doivent être calculé. Nous avons vu dans le chapitre 3 que la conception de l'ATC est une conception couplée. Q_c vaut donc 1. Pour calculer N_f, nous nous basons sur les informations trouvées dans des documents techniques. Selon ces données, la durée de vie de l'ATC est plus élevée que celle du tracteur équipé. De plus, l'ATC ne fait l'objet d'aucune défaillance. Si l'on considère la durée de vie souhaitée de l'ATC comme égale à la durée de vie du tracteur, sa durée de vie avant défaillance sera plus grande que sa durée de vie souhaitée. Nous en concluons que $N_f = 0$. En prenant $\alpha_1 = 2$ et $\alpha_2 = 1$, l'équation du Facteur de Risque devient :

$$F_{Rs} = \frac{(\alpha_1 Q_c + \alpha_2 N_f)}{\alpha_1 + \alpha_2} = \frac{2 + 0}{3} = 0,67$$

Facteur de Risque lié à l'humain (F_{Rh}) : Selon l'équation (4-21), nous avons besoin pour définir F_{Rh} d'identifier les quatre catégories de facteur de risque lié à l'humain (F_{Rh1}: la formation ; F_{Rh2}: l'expérience ; F_{Rh3}: l'état physique ; et F_{Rh4}: l'attitude) en se basant sur les rapports d'accident existants.

$$F_{Rh}: \begin{cases} F_{Rh} = \dfrac{\sum_{i=1}^{n} \beta_i F_{Rhi}}{\sum_{i=1}^{n} \beta_i} \\ avec: \\ n:\ nombre\ des\ facteurs\ considérés \\ F_{Rhi} : i^{ème}\ facteur;\ \forall\ i\ ,\ F_{Rhi} = 0,1 \\ \beta_i : coefficient\ de\ pondération\ pour\ le\ i^{ème}\ facteur \end{cases} \qquad Equation\ (4-21)$$

Dans le cas des accidents étudiés, les victimes avaient été formées à l'utilisation et aux risques liés à l'ATC. Elles étaient expérimentées, avaient une bonne condition physique mais travaillaient sous pression. Par conséquent, $F_{Rh1} = 0$; $F_{Rh2} = 0$; $F_{Rh3} = 0$ et $F_{Rh4} = 1$. Concernant les coefficients de pondération, nous considérons que l'ordre d'importance des quatre catégories de facteur de risque lié à l'humain est le suivant : F_1, F2, F_3 puis F_4. Nous donnons respectivement les valeurs 4, 3, 3 et 1 aux coefficients de pondération β_1, β_2, β_3 et β_4. L'équation donnant F_{Rh} devient :

$$F_{Rh} = \frac{\sum_{i=1}^{n} \beta_i F_{Rhi}}{\sum_{i=1}^{n} \beta_i} = \frac{(4 \times 0) + (3 \times 0) + (2 \times 0) + (1 \times 1)}{4 + 3 + 2 + 1} = 0{,}1$$

Facteur de Risque lié à l'environnement (F_{Re}) : Selon l'équation (4-22), les trois catégories de facteurs environnementaux ont besoin d'être identifiés pour définir F_{Re} (F_{Re1}: présence d'autre personne ; F_{Re2}: environnement fermé ou ouvert ; F_{Re3}: milieu structurée ou naturel).

$$F_{Re}: \begin{cases} F_{Re} = \dfrac{\sum_{j=1}^{m} \gamma_j F_{Rej}}{\sum_{j=1}^{m} \gamma_j} \\ avec: \\ m : nombres\ des\ facteurs\ considérés \\ F_{Rej} : j^{ème}\ facteur \qquad \forall\ j\ ,\ F_{Rej} = 0,1 \\ \gamma_j :\ coefficient\ de\ pondération\ pour\ le\ j^{ème}\ facteur \end{cases} \qquad Equation\ (4-22)$$

Comme pour F_{Rh}, nous nous basons sur les rapports d'accident existants et nous adoptons les valeurs suivantes :

- $F_{Re1} = 1$ car plusieurs personnes peuvent se trouver dans l'environnement de travail ;
- $F_{Re2} = 1$ car le milieu où se trouve l'ATC est un milieu ouvert ;
- $F_{Re3} = 1$ car ce milieu est un milieu naturel non-structuré.

Nous considérons que l'ordre d'importance des trois catégories des facteurs de risque lié à l'environnement est le suivant : F_1, F_2 puis F_3. Nous donnons respectivement les valeurs 3, 2 et 1 aux coefficients de pondération γ_1, γ_2 et γ_3. Ainsi, l'équation donnant F_{Re} devient :

$$F_{Re} = \frac{\sum_{j=1}^{m} \gamma_j F_{Rej}}{\sum_{j=1}^{m} \gamma_j} = \frac{(3 \times 1) + (2 \times 1) + (1 \times 1)}{3 + 2 + 1} = 1$$

Niveau de Risque lié à l'Evénement dangereux (N_{REd}): Dans cette étape, nous voulons obtenir la valeur de N_{REd} en appliquant l'équation (4-23).

$$N_{REd}: \begin{cases} N_{REd} = \dfrac{(\delta_1 F_{Rs} + \delta_2 F_{Rh} + \delta_3 F_{Re})}{\sum \delta} \\ avec: \\ \delta_1 : coefficient\ de\ pondération\ pour\ le\ FR_s \\ \delta_2 : coefficient\ de\ pondération\ pour\ le\ FR_h \\ \delta_3 : coefficient\ de\ pondération\ pour\ le\ FR_e \end{cases} \qquad Equation\ (4-23)$$

Nous considérons que le poids accordé à F_{Rs} doit être le plus important à la vue de notre objectif final d'améliorer la sécurité du système lors de sa conception. De plus, l'humain et son comportement ayant une influence généralement plus forte que l'environnement sur l'occurrence de l'accident, nous considérons que F_{Rh} doit avoir un poids plus important que

F_{Re}. Pour ces raisons, nous donnons respectivement les valeurs 3, 2 et 1 aux coefficients de pondération δ_1, δ_2 et δ_3. Ainsi l'équation donnant N_{REd} devient :

$$N_{REd} = \frac{(\delta_1 F_{Rs} + \delta F_{Rh} + \delta_3 F_{Re})}{\sum \delta} = \frac{(3 \times 0{,}67) + (2 \times 0{,}1) + (1 \times 1)}{3 + 2 + 1} = 0{,}535$$

. Niveau de Risque (N_R)

Enfin, en appliquant l'équation (4-24) et les trois valeurs de N_{RPd}, N_{RSd}, et N_{REd} obtenues ci-dessus, il devient possible de définir le Niveau de Risque de l'ATC sans son moyen de protection.

$$N_R : \begin{cases} N_R = \dfrac{(\varepsilon_1 N_{RPd} + \varepsilon_2 N_{RSd} + \varepsilon_3 N_{REd})}{\sum \varepsilon} \\ avec: \\ \varepsilon_1 : coefficient\ de\ pondération\ pour\ le\ niveau\ de\ risque\ lié\ au\ Pd \\ \varepsilon_2 : coefficient\ de\ pondération\ pour\ le\ niveau\ de\ risque\ lié\ à\ la\ Sd \\ \varepsilon_3 : coefficient\ de\ pondération\ pour\ le\ niveau\ de\ risque\ lié\ à\ l'Ed \end{cases} \qquad Equation\ (4-24)$$

Selon l'ordre de priorité pour la réduction de risque proposé dans la norme [FD ISO/TR 14121-2, 2008], l'élimination du phénomène dangereux est la priorité. Vient ensuite l'élimination de la situation dangereuse et enfin l'événement dangereux. Dans notre calcul du niveau de risque, nous proposons de garder cet ordre de priorité et donc d'adopter respectivement les valeurs 3, 2 et 1 aux facteurs de pondération ε_1, ε_2 et ε_3. L'équation donnant N_R devient :

$$N_R = \frac{(\varepsilon_1 N_{RPd} + \varepsilon_2 N_{RSd} + \varepsilon \delta_3 N_{REd})}{\sum \varepsilon} = \frac{(3 \times 0{,}9998) + (2 \times 0{,}041) + (1 \times 0{,}535)}{3 + 2 + 1} = 0{,}602$$

Indicateur de Sécurité (I_S) de l'ATC sans moyen de protection

En appliquant l'équation (4-26) et les deux valeurs de P_D et de N_R obtenues ci-dessus, l'Indicateur de Sécurité de l'ATC sans moyen de protection obtenue devient :

$$I_{S\ ATC\ smp} = 1 - I_{PD} \times N_R = 1 - (1 \times 0{,}602) = 0{,}398$$

4.3.5.2. Définition de l'Indicateur de Sécurité des moyens de protection de l'ATC

Dans cette étape, nous proposons de calculer l'indicateur de sécurité des moyens de protection du système. Dans le cas de l'ATC, le moyen de protection est un protecteur.

Définition de la Présence de Danger (P_D) du moyen de protection de l'ATC

Selon les connaissances obtenues à partir de l'analyse des rapports d'accident sur l'ATC, le phénomène dangereux et la situation dangereuse sont liées à l'ATC lui-même et non pas au protecteur. Autrement dit, la présence de danger pour le système sans moyen de protection est égal 1. Donc, d'après le tableau 4.7 (a), rappelée ci-dessous, P_D = 1 pour le système ATC avec son protecteur.

Tableau 4.7. Valeurs prises par la Présence de Danger pour le moyen protection de l'ATC (a) dans le cas où PDssmp = 1 et (b) dans cas où PDssmp = 0.

(a) P_{Dssmp} = 1

P_{Pd}	P_{Sd}	P_{Ed}	P_{Dmp}
0	0	0	1
1	0	0	1
1	1	1	1

(b) P_{Dssmp} = 0

I_{PPd}	I_{PSd}	I_{PEd}	P_{Dmp}
0	0	0	0
1	0	0	0
1	1	1	1

Définition du Niveau de Risque (NR) du moyen de protection de l'ATC

Pour le protecteur de l'ATC, $N_{RPd} = 0$ et $N_{RSd} = 0$. Reste à définir N_{REd}.

. Niveau de Risque lié à l'Evénement dangereux(N_{REd})

Facteur de Risque lié au système (F_{Rs}) : Nous calculons le F_{Rs} en utilisant l'équation (4-20).

$$F_{Rs}: \begin{cases} F_{Rs} = \dfrac{(\alpha_1 Q_c + \alpha_2 N_f)}{\alpha_1 + \alpha_2} \\ \alpha_1 : coefficient\ de\ pondération\ Q_c \\ \alpha_2 : coefficient\ de\ pondération\ de\ N_f \end{cases} \qquad Equation\ (4-20)$$

Selon les résultats du chapitre 3, la matrice de conception axiomatique du protecteur est couplée, donc Q_c=1. Pour calculer N_f, nous nous basons sur les informations que nous avons trouvées dans les documents techniques. Selon ces informations, la durée de vie d'un protecteur d'ATC n'est pas élevée. En moyenne, ce protecteur devient défaillant après 1000 heures d'utilisation. Nous considérons la durée de vie souhaitée du protecteur de l'ATC égale à la durée de vie du protecteur avant défaillance, soit 5000 heures. L'équation donnant N_f devient (équation 4-1):

$$N_f = 1 - \frac{Dvad}{Avs} = 1 - \frac{1000}{5000} = 1 - 0{,}2 = 0{,}8$$

L'équation donnant le Facteur de Risque lié au protecteur de l'ATC devient (équation 4-19) :

$$F_{Rs} = \frac{(\alpha_1 Q_c + \alpha_2 N_f)}{\alpha_1 + \alpha_2} = \frac{2 + 0{,}8}{3} = 0{,}93$$

Facteur de Risque lié à l'humain (F_{Rh}) : Il est le même que pour l'ATC sans moyen de protection, donc $F_{Rh} = 0{,}1$

Facteur de Risque lié à l'environnement (F_{Re}) : Il est le même que pour l'ATC sans moyen de protection, donc $F_{Re} = 1$

Niveau de Risque lié à l'Evénement dangereux (N_{REd}): A cette étape, nous pouvons obtenir la valeur de N_{REd} en appliquant l'équation (4-23) et les valeurs obtenues ci-dessus. L'équation donnant N_{REd} devient :

$$N_{REd} = \frac{(\delta_1 F_{Rs} + \delta_2 F_{Rh} + \delta_3 F_{Re})}{\sum \delta} = \frac{(3 \times 0.93) + (2 \times 0.1) + (1 \times 1)}{3 + 2 + 1} = 0.665$$

. Niveau de Risque (N_R)

En reportant les valeurs de F_{Rs}, F_{Rh} et F_{Re} dans l'équation donnant le Niveau de Risque du protecteur de l'ATC, on obtient :

$$N_R = \frac{(\varepsilon_1 N_{RPd} + \varepsilon_2 N_{RSd} + \varepsilon_3 N_{REd})}{\sum \varepsilon} = \frac{(3 \times 0) + (2 \times 0) + (1 \times 0{,}665)}{3 + 2 + 1} = 0{,}11$$

Définition de l'Indicateur de Sécurité (IS) du moyen de protection de l'ATC

En remplaçant les deux valeurs P_D et N_R obtenues ci-dessus dans l'équation (4-25), l'Indicateur de Sécurité du moyen de protection de l'ATC est :

$$I_{S\ ATC\ smp} = 1 - P_D \times N_R = 1 - (1 \times 0{,}11) = 0{,}89$$

4.3.5.3. Définition de l'Indicateur de Sécurité de l'ATC

En remplaçant les indicateurs de sécurité de l'ATC et de son protecteur par leur valeur respectives calculées ci-dessus dans l'équation donnant la valeur de l'indicateur de sécurité du système ATC avec moyen de protection, on obtient :

$$I_{Ss} = \frac{\mu_1 I_{Sssmp} + \mu_2 \left(\frac{\sum_{z=1}^{n} I_{Smp\ z}}{n}\right)}{\mu_1 + \mu_2} = \frac{\mu_1 I_{S\ ATC\ smp} + \mu_2 (\sum_{z=1}^{n} I_{Smp\ de\ l'ATC/1})}{\mu_1 + \mu_2}$$

Dans notre calcul, nous considérons le niveau de sécurité du système lui-même plus important que celui de son moyen de protection. Nous adoptons donc respectivement les valeurs 2 et 1 aux facteurs de pondération µ1 et µ2. L'équation devient :

$$\rightarrow I_{S\ ATC} = \frac{2 \times 0{,}398 + 1 \times 0{,}89}{3} = 0{,}562$$

4.3.5.4. Conclusion sur l'application

Nous avons déterminé le niveau de sécurité, I_s, de l'ATC en déterminant, à la fois, le niveau de sécurité de l'ATC sans moyen de protection et le niveau de sécurité du protecteur de l'ATC. Ce sont des valeurs références. Une solution sera plus sécuritaire que la solution actuelle (ATC et protecteur) si et seulement si l'indicateur de sécurité de cette nouvelle solution est supérieur à $I_{S\ ATC}$, c'est-à-dire 0,562. Dans le cas d'une reconception du protecteur uniquement, la nouvelle solution devra avoir un indicateur de sécurité supérieur à $I_{Smp\ de\ l'ATC}$ donc à 0,89.

Selon notre indicateur, le niveau de sécurité de l'ATC sans protecteur est de I_S = 0,398. Avec protecteur, il est de I_S = 0,562. Leur comparaison permet d'apprécier numériquement l'apport du protecteur dans le sens de l'amélioration de la sécurité du système. Nous pouvons aussi remarquer que la fiabilité et la qualité de la conception du protecteur sont les éléments déterminants du niveau de réduction du risque apporté par ce protecteur.

4.3.6. Conclusion

Dans cette section, nous avons défini un indicateur de sécurité pour l'évaluation du niveau de sécurité d'un système. Cet indicateur de sécurité, I_s, répond à plusieurs manquements ou inconvénients identifiés vis-à-vis des approches existantes dans l'évaluation de la sécurité, et, en particulier, sur les deux points suivants :

- La plupart des travaux existant sur l'évaluation des risques et de la sécurité sont basés sur la définition du risque proposée dans la norme [NF EN ISO 12100, 2010] cité dans le chapitre 1 de ce manuscrit. Les résultats de cette évaluation dépendent donc entièrement d'avis d'experts. L'indicateur de sécurité que nous avons développé ne nécessite pas d'avis d'expert. Il est donc plus objectif.
- Les aspects de la conception du système et de sa qualité de conception sont rarement pris en compte dans les indicateurs existants. Parmi les travaux existants, l'indicateur de sécurité développé par [Coulibaly et al., 2008] est développé pour être appliqué pendant la conception mais uniquement à la phase de la conception architecturale. Notre I_S permet de mesurer la sécurité dès la conception conceptuelle, car :
    - Selon la conception axiomatique, une bonne conception est une conception sans couplage entre les exigences fonctionnelles. Cet aspect de couplage est pris en compte dans notre indicateur de sécurité.
    - La fiabilité, qui fait intervenir la durée de vie du système, ne peut être évaluée que dans la phase architecturale de la conception. Elle est également prise en compte dans le calcul de notre indicateur mais est considéré optimale dans la phase de conception conceptuelle.

Les perspectives que nous proposons à la suite de ce travail de développement d'un indicateur de sécurité sont les suivantes :

- L'indicateur de sécurité proposé prend en compte l'impact de la source du phénomène dangereux sur le niveau de sécurité du système. Le calcul de la valeur de cet impact nécessite la connaissance de certaines valeurs seuils supportées par l'humain. Pour certains sources de phénomènes dangereux (bruit, poussière, port de charge, etc.) les valeurs seuils sont données dans les normes de sécurité. Mais ce n'est pas le cas pour les différents types d'énergies. Il serait donc intéressant de chercher à calculer ces valeurs seuils.
- Nous avons proposé d'exprimer la qualité de la conception (Q_c) sous la forme d'une valeur binaire (présence de couplage ou non). Cette proposition n'est pas tout à fait satisfaisante du fait qu'elle ne permet pas de différentier deux solutions ayant un nombre de couplage différent, sachant que dans certains cas, le concepteur aura à choisir entre de telles solutions. Nous proposons donc de définir une échelle comprise entre 0 et 1 prenant en compte le nombre de couplages dans le système.
- Les Facteurs lié à l'humain (F_{Rh}) et à l'environnement (F_{Re}) sont limités à des valeurs binaires. Afin d'avoir des résultats plus précis, il nous paraît intéressant d'augmenter le nombre de valeurs possibles de ces facteurs.
- L'indicateur étant basé sur de nombreux paramètres pondérés, il est nécessaire de faire une analyse de sensibilité afin d'évaluer l'impact des valeurs des paramètres sur la valeur de l'indicateur.

4.4. Conclusion

Dans le cadre de l'opérationnalisation de la méthode IRAD, nous avons présenté dans ce chapitre l'évaluation de et pour la sécurité. Pour cela, nous avons développé une approche d'identification et de ventilation du risque selon les phases de la conception et défini un indicateur de sécurité pour l'évaluation du niveau de sécurité d'un système.

L'approche d'identification et de ventilation du risque est basée sur les trois contextes C2, C4 et C6 de la méthode IRAD. Cette approche permet au concepteur de définir, pour un risque donné, le type de risque selon les trois phases de la conception. Cette approche a été appliquée sur le risque lié l'ATC. Il en résulte qu'il s'agit d'un risque défini au niveau de la conception conceptuelle, c'est-à-dire un risque d'accident (C2).

Nous avons ensuite détaillé la formule proposée d'un Indicateur de Sécurité (I_s). Pour la construction de cet indicateur de sécurité, nous avons considéré les aspects conception et sécurité du système. L'indicateur de sécurité développé est indépendant de l'avis d'experts en sécurité et permet de mesurer la sécurité à tout moment lors du processus de conception et particulièrement dès la conception conceptuelle. Cet indicateur de sécurité a été calculé au cas de l'ATC sans moyen de protection et au cas du protecteur de l'ATC. Selon les résultats obtenus, L'ATC est davantage sécuritaire avec son moyen de protection que sans. Une analyse plus fine montre également que la fiabilité et la qualité de la conception du protecteur sont des éléments déterminants pour l'amélioration de la sécurité de l'ATC.

Dans le chapitre 5, nous allons nous baser sur les types de risques définis afin de formuler les objectifs de sécurité et identifier les niveaux d'intervention pour améliorer la sécurité. Ensuite, nous utiliserons l'indicateur de sécurité qui, combiné à une démarche de réingénierie fonctionnelle permettra au concepteur de choisir les solutions les plus sécuritaires.

Chapitre 5. Réingénierie fonctionnelle pour la sécurité

5.1. Introduction

Avec l'objectif de proposer un processus itératif d'aide à la décision pour l'intégration de la sécurité dans le processus de conception, le chapitre 3 détaille l'approche FRES d'ingénierie inverse fonctionnelle. Celle-ci permet d'extraire et de formaliser les connaissances techniques et de sécurité du système étudié. L'intégration de ces connaissances se fait en appliquant l'approche FR2ES (Functional REEngineering for Safety) de réingénierie fonctionnelle. Cette méthode et son principe de fonctionnement sont détaillés dans ce chapitre.

L'approche FR2ES est basée sur trois points de vue : sécurité, conception et aide à la décision :

- Point de vue **sécurité**, l'approche FR2ES permet de définir les objectifs de sécurité pour l'amélioration de la sécurité du système. La question à laquelle l'approche doit répondre est : *Comment transcrire de manière formelle et systématique les risques en objectifs de sécurité dans les trois phases de conception?*
- Point de vue **conception**, l'approche FR2ES permet de concevoir un système au niveau de sécurité optimal en s'appuyant sur les objectifs de sécurité définis juste avant. Nous devons ici répondre à la question : *Face aux nouveaux objectifs de sécurité, comment reconstruire le système ?*
- Point de vue **aide à la décision**, l'approche FR2ES doit aider le concepteur à choisir les solutions les plus sécuritaires dans le processus de reconception. Cette aide sera basée sur la mise en œuvre de l'indicateur de sécurité détaillé au chapitre précédent.

Nous avons présenté la vue globale du processus de conception sécuritaire proposé sous la forme d'un diagramme IDEF0 au chapitre 1 (figure 1.14). La fonction A0 « Concevoir de façon sécuritaire » comporte deux sous-fonctions (figure 1.17) : la sous-fonction A1 « Appliquer la démarche FRES » et la sous fonction A2 « Appliquer la démarche FR2ES ». Cette deuxième sous-fonction se décompose en deux sous-fonctions: A21 « Définir et prioriser les objectifs de sécurité» et A22 « Reconcevoir de façon sécuritaire» (figure 5.1).

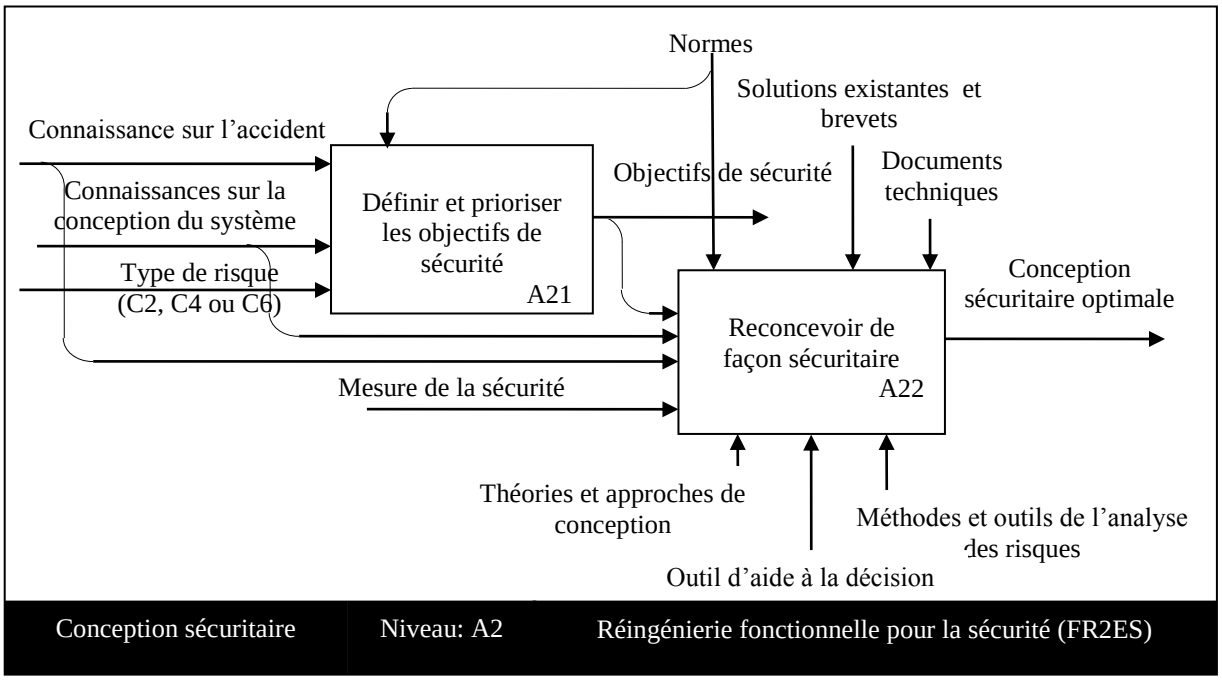


Figure 5.1. Diagramme IDEF0 niveau A2 de processus conception sécuritaire.

L'approche doit donc permettre, à partir de connaissances sur l'accident et de connaissances sur la conception du système, du type de risque identifié et de la mesure de sécurité calculée, de (1) définir les objectifs de sécurité et (2) reconcevoir le système avec un niveau de sécuritaire optimal.

Ce chapitre comporte deux sections principales. La première (section 5.2) propose une approche pour la définition et la priorisation des objectifs de sécurité pour un risque donné et la deuxième (section 5.3) propose une approche de reconception. Comme pour les chapitres précédents (chapitres 3 et 4), chacune de ces deux sections comporte cinq sous sections, l'introduction, l'état de l'art, le développement de l'approche, l'application de l'approche à l'ATC, une conclusion, une discussion et enfin les perspectives envisagées.

5.2. Développement d'une approche de définition et de priorisation des objectifs de sécurité pour un risque donné

5.2.1. Introduction

Dans le cadre de l'opérationnalisation de la méthode IRAD, les risques générés au cours de la conception des solutions technologiques doivent, eux aussi, être retranscrits en exigences de sécurité. Le but de cette partie est de définir les objectifs de sécurité et leurs niveaux d'intervention possibles dans le processus de reconception du système ou de la partie du système impliquée dans l'accident. L'objectif opérationnel de ces travaux est d'aider les concepteurs à réaliser la transition entre la définition des risques et celle des objectifs de sécurité. A l'issue de cette étape, les différentes solutions d'amélioration de la sécurité sont proposées au concepteur. Ces pistes doivent être combinées à des éléments objectifs lui permettant de faire un choix.

Nous proposons donc, dans cette section, une approche guidée permettant de passer de l'analyse des risques à l'expression des objectifs de sécurité. Dans la section 5.2.2, l'état de l'art sur la définition des objectifs de sécurité des points de vue normatif et scientifique est présenté. Dans la section 5.2.3, une approche est proposée afin d'identifier et de hiérarchiser les règles permettant de définir les objectifs de sécurité. Cette approche est basée sur la méthode IRAD et sur les étapes des phases de réduction des risques décrites dans la norme [NF EN ISO 12100, 2010] ainsi que le rapport technique [FD ISO/TR 14121-2, 2008]. La section 5.2.4 présente l'application de l'approche proposée sur l'Arbre de Transmission à Cardans (ATC). Enfin, nous concluons cette section par une synthèse et par des perspectives dans la section 5.2.5.

5.2.2. Définition des objectifs de sécurité

Dans cette section, nous détaillons dans un premier temps la phase de réduction des risques proposé dans la norme internationale [NF EN ISO, 12100, 2010]. Nous présentons ensuite les travaux scientifiques existants sur cette même thématique. Nous revenons enfin plus en détails sur la définition des objectifs de sécurité proposée dans la méthode IRAD.

5.2.2.1. La réduction des risques du point de vue normatif

Comme nous l'avons déjà exprimé dans le premier chapitre de ce manuscrit, la norme [NF EN ISO 12100, 2010] et le rapport technique [FD ISO/TR 14121-2, 2008] proposent huit étapes pour la réduction des risques:

1. Eliminer les phénomènes dangereux par conception ;
2. Réduire le risque par conception;
3. Définir des dispositifs de protection;
4. Proposer des mesures de protection complémentaires ;
5. Informer sur l'utilisation ;

6. Former à l'utilisation;
7. Définir des équipements de protection individuelle ;
8. Décrire les procédures de fonctionnement normal.

Dans notre cas, nous nous intéressons aux deux premières étapes de ce processus de réduction des risques de façon à pouvoir réduire les risques par conception : éliminer les phénomènes dangereux et réduire le risque. Cette réduction des risques par conception peut se faire par l'application de mesures de protection. Celles-ci sont citées ci-dessous par ordre d'efficacité:

1. Elimination des phénomènes dangereux par conception. C'est la mesure de protection la plus efficace pour éliminer le risque en éliminant la source du dommage. Une alternative possible ici est la réduction de la gravité du dommage lié au phénomène dangereux en réduisant, par exemple, l'énergie (force plus faible, hauteur de travail réduite, vitesse réduite) ou en utilisant des équipements techniques pour la prévention ou la réduction des phénomènes dangereux.

2. Elimination des situations dangereuses en éliminant l'exposition de la personne au phénomène dangereux. Une alternative à cette mesure est la réduction de la fréquence et/ou de la durée d'exposition. Cela peut se produire en réduisant, par exemple, la nécessité pour l'opérateur de se placer dans une situation dangereuse (mécanisation ou automatisation de certaines opérations, délocalisation des sites d'intervention) ou en déplaçant les sources du dommage.

3. Elimination des évènements dangereux possibles. En sachant que les événements dangereux peuvent être d'origine technique ou humaine. L'alternative à cette mesure est la réduction de la probabilité d'occurrence des événements dangereux en améliorant, par exemple, la fiabilité des composants de la machine et en appliquant des mesures de conception sûres aux pièces des systèmes de commande relatifs à la sécurité (redondance, …).

Il convient de noter ici qu'il existe plusieurs types de moyens de protection. En se basant sur [NF EN ISO 12100, 2010], nous avons synthétisé les **moyens de protection** en trois types généraux comme suit :

- **Protecteur** : Barrière physique assurant une fonction de protection. Il a, en particulier, un impact sur l'exposition au phénomène dangereux (ex. protecteurs pour restreindre l'accès, …). La norme [NF EN 953+A1, 2009] spécifie « les prescriptions générales applicables à la conception et à la construction de protecteurs destinés essentiellement à protéger les personnes contre les risques mécaniques »;
- **Dispositif de protection** : Moyen de protection autre qu'un protecteur. Il a, en particulier, un impact sur l'occurrence de l'événement dangereux (ex. détecteurs de présence, solutions liées au système de commande, etc.) ;
- **Mesure de prévention complémentaire** : Cette mesure permet, en général, d'éviter ou de limiter le dommage (ex. arrêt d'urgence, mesures de sauvetage, etc.).

La norme [NF EN ISO 12100, 2010] et le rapport technique [FD ISO/TR 14121-2, 2008] proposent donc des démarches structurées permettant d'apprécier et de réduire les risques identifiés. Cependant, elles restent générales et laissent la responsabilité aux concepteurs de la manière de réaliser cette démarche, notamment quant à l'intégration au moment opportun des exigences de sécurité dans le processus de conception. Nous proposons de remédier à cet inconvénient et donc de proposer une démarche et des outils afin que le concepteur puisse introduire la bonne exigence de sécurité au bon moment de la conception.

5.2.2.2. La réduction des risques du point de vue scientifique

Selon [Hollnagel, 2008], le processus de réduction des risques pour améliorer la sécurité est basé sur quatre étapes : (1) identifier s'il existe un risque et comprendre sa nature, (2) comprendre le mécanisme de son apparition, (3) l'évaluer, et (4) trouver les moyens pour son élimination ou sa réduction. Cette description est basée sur la proposition de la norme [NF EN ISO 12100, 2010].

[Mazouni, 2008] définit la réduction des risques comme « *l'ensemble des actions entreprises en vue de diminuer la gravité des conséquences (protection), les probabilités d'occurrence (prévention) ou les deux en même temps* ». Selon lui, la réduction des risques peut s'effectuer par la réduction des temps d'exposition et la multiplication des possibilités d'évitement des situations dangereuses.

La notion de barrière apparait souvent dans les travaux scientifiques relatifs à cette thématique. Selon [Harms-Ringdahl, 2003], les concepts et la terminologie liés aux barrières sont considérablement variés. Les termes relatifs à ce concept et généralement utilisés sont la « fonction de barrière », la « défense », le « dispositif protecteur » et la « couche de protection ». [Zhang et al., 2004] a considéré les barrières dans l'interaction homme-machine comme permettant de réduire les erreurs humaines, de limiter la propagation d'échec et/ou de protéger les opérateurs humains contre des échecs techniques. Plus spécifiquement, les barrières de sécurité sont définies comme « *des obstacles, des obstructions ou des gênes qui peuvent soit prévenir l'exécution d'une action ou l'apparition d'un évènement, soit prévenir ou diminuer l'impact des conséquences* » [Hollnagel, 1999].

Certains travaux scientifiques se focalisent sur ce concept de barrière et le définissent comme un moyen de réduction des risques [Sklet, 2006 ; Hollnagel, 2008b]. La norme ISO 13702:1999 citée dans [Sklet, 2006] distingue trois fonctions à ces barrières : la prévention, le contrôle et la mitigation. La prévention a pour objectif de réduire la probabilité d'un évènement ou de réduire son intensité. Le contrôle limite la déviation d'une situation normale à une situation anormale ou inacceptable. La mitigation consiste à prévenir que l'énergie soit absorbée par la cible. Selon [Shahrokhi, 2006] modifier et ajouter des barrières est le moyen le plus couramment utilisé par les concepteurs pour réduire le risque. Selon lui, une barrière peut avoir des effets sur la source du danger, la cible, la zone dangereuse et sur la probabilité ou la durée de l'impact [Shahrokhi, 2006]. [Shahrokhi et Bernard, 2006] proposent une modélisation par ordinateur afin d'analyser les risques et les effets de la mise en place des barrières.

[Houssin et Coulibaly, 2011] ont proposé une approche basée sur la résolution de contradictions pour la réduction des risques dans les différentes étapes de la conception. L'approche proposée est basée sur quatre étapes : (1) l'intégration systématique de la sécurité en utilisant le modèle de la situation de travail, (2) la prise en compte des exigences des directives et des normes de sécurité, (3) l'identification des contradictions résultant des choix de design, et (4) la résolution de ces contradictions en utilisant des méthodes adaptées comme TRIZ.

[Ghemraoui, 2009] propose, dans la méthode IRAD, de réduire les risques par la traduction des risques en exigences de sécurité dans le processus de risque. Pour chaque risque identifié dans le domaine physique du processus de risque, la méthode IRAD demande d'identifier des exigences de sécurité dans le domaine fonctionnel afin d'éliminer ou de réduire le risque identifié. Dans certains cas, plusieurs exigences de sécurité peuvent être définies pour éliminer ou réduire le risque identifié. L'une des limites de la méthode IRAD est identifiée ici. Effectivement, IRAD ne permet pas de définir un ordre de priorité à ces exigences.

Ce bref état de l'art montre que la plupart des travaux scientifiques sur la réduction des risques afin d'éliminer ou de réduire les risques s'inspirent de la norme. Cependant, hormis le cas de la méthode IRAD, ces travaux ne proposent pas d'introduire les résultats de cette démarche de réduction de risque au bon moment lors de la conception. La méthode IRAD va donc plus loin que les autres travaux mais celle-ci ne guide pas le concepteur dans la définition des exigences de sécurité.

L'idée que nous développons par la suite est de combiner les démarches proposées par les normes d'une part et par la méthode IRAD d'autre part, afin d'ordonner et d'identifier les exigences de sécurité en fonction des types de risques définis. Mais avant de développer cette idée, nous présentons plus en détail dans la partie qui suit la réduction des risques telle que proposée dans le cadre de la méthode IRAD.

5.2.2.3. La réduction des risques dans IRAD

Pour chaque risque identifié dans le domaine physique du processus de risque, la méthode IRAD demande d'identifier des exigences de sécurité dans le domaine fonctionnel afin d'éliminer ou de réduire le risque identifié. Dans certains cas, plusieurs exigences de sécurité peuvent être définies pour éliminer ou réduire le risque identifié. L'une des difficultés dans l'application de la méthode IRAD est alors de définir un ordre de priorité à ces exigences. La méthode IRAD ne guide pas le concepteur dans la définition des exigences de sécurité mais elle donne quelques pistes pour trouver et définir des objectifs de sécurité. La figure 5.2 montre le passage entre le risque et la solution sécuritaire dans IRAD.

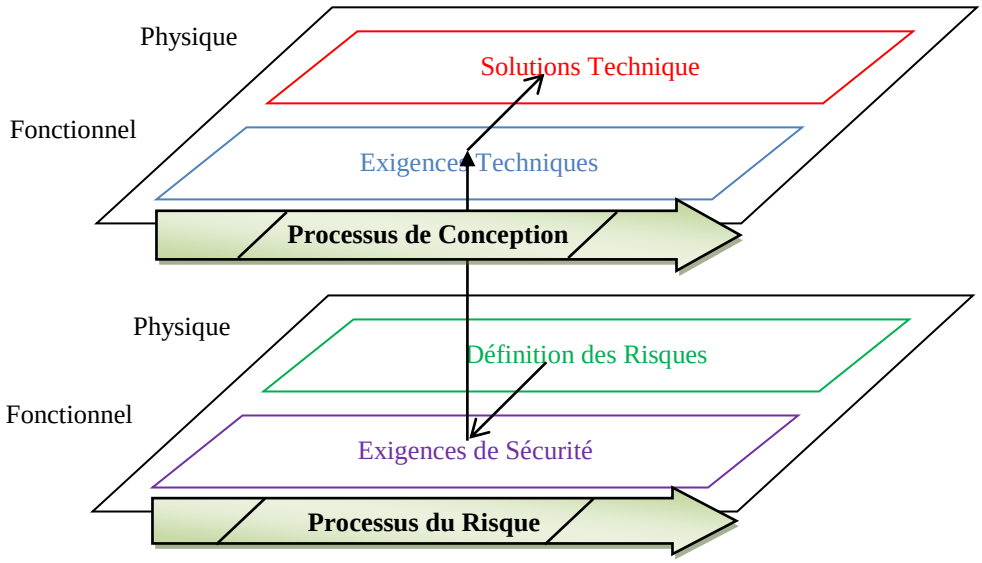


Figure 5.2. Passage entre le risque et la solution sécuritaire dans IRAD.

Les objectifs de la conception du point de vue sécurité présentés dans le **principe 1** de la méthode IRAD, représentent les exigences de sécurité du processus de risque (Contextes C1, C3 et C5). Ces exigences sont obtenues, d'une part, grâce à la formalisation du retour d'expérience, des risques et des exigences identifiées dans le passé en utilisant le même produit ou un produit similaire (cas d'emploi 1). D'autre part, elles sont identifiées par la définition des risques issus des solutions de conception envisageables (cas d'emploi 2). Dans le cas d'un nouveau produit, IRAD propose d'extraire ces exigences de sécurité de la norme et des directives. Les exigences de sécurité liées au niveau conceptuel (contexte C1) peuvent être obtenues à partir des normes de type A. Les exigences de sécurité au niveau architectural (Contexte C3) sont obtenues principalement à partir des normes de type B.

Le **principe 2** de la méthode IRAD exige de conserver l'indépendance des exigences fonctionnelles techniques et de sécurité. Ce principe permet d'évaluer la validité des exigences de sécurité proposées à chaque étape de la conception. Le **principe 3** de la méthode IRAD exige de minimiser l'incompatibilité entre les caractéristiques humaines et les paramètres de la conception. L'ensemble des points de ce principe sont traduits, dans le processus du risque, par la quantification des exigences de sécurité.

La méthode IRAD se base sur les normes pour déterminer les caractéristiques principales de l'humain: caractéristiques morphologiques, force physique, postures et capacité mentale, auxquelles elle ajoute une autre caractéristique : la vulnérabilité de l'humain. Cette quantification des caractéristiques humaines fait l'objet de certaines normes de type B1.

5.2.2.4. Synthèse

Comme nous venons de le voir, la norme [NF EN ISO 12100, 2010] et le rapport technique [FD ISO/TR 14121-2, 2008] proposent des démarches structurées permettant d'apprécier et de réduire les risques identifiés. Mais la proposition de la norme reste générale et laisse la responsabilité aux concepteurs de la manière de réaliser cette démarche, et notamment sur l'intégration au moment opportun des exigences de sécurité dans le processus de conception.

La plupart des travaux scientifiques s'inspirent de la norme afin d'éliminer ou de réduire les risques. La notion de barrière y est souvent utilisée. Cependant, ces travaux ne proposent pas de façon d'intégrer les résultats du processus de réduction des risques au bon moment lors de la conception non plus. À notre connaissance, seule la méthode IRAD permet de réduire les risques tout au long du processus de conception grâce à un processus de risque composé des contextes C1, C3 et C5 permettant de ventiler les exigences de sécurité. Cependant, cette méthode ne définit pas précisément comment réaliser cette ventilation. Une approche permettant d'éliminer ou de réduire les risques en combinant les démarches proposées par les normes et la méthode IRAD doit résoudre ce problème.

5.2.3. Définir et hiérarchiser des objectifs de sécurité selon les phases de conception

Dans le chapitre 4 de ce manuscrit, nous avons développé une approche pour identifier et ventiler les risques en utilisant des informations obtenues à partir de l'analyse de rapports d'accident. Le développement de cette approche est basé sur les trois contextes C2, C4 et C6 de la méthode IRAD. Le concepteur se charge alors de construire des objectifs de sécurité cohérents et adaptés à chaque risque identifié.

5.2.3.1. Risque identifié au niveau conceptuel

Pour un risque identifié au niveau conceptuel (contexte C2) et donc lié à une solution de conception proposée au niveau conceptuel, le phénomène dangereux, la zone dangereuse, la situation dangereuse ainsi que l'éventuel événement dangereux lié à ce risque doivent être précisés [Sadeghi et al., 2012b].

1. Eliminer le phénomène dangereux par conception

Le premier objectif est d'éliminer le phénomène dangereux et donc de modifier ou de changer la solution proposée. Cet objectif de sécurité n'est pas de type « exigence fonctionnelle » mais de type « contrainte ». Elle peut être formulée comme suit « assurer la non présence du phénomène dangereux ». A ce stade, le concepteur doit s rester au même niveau hiérarchique de l'arbre fonctionnel en recherchant des solutions conceptuelles alternatives vérifiant les nouvelles contraintes.

Cette étape de recherche d'élimination du phénomène dangereux peut amener le concepteur à proposer des solutions de conception innovante en rupture avec les solutions similaires existantes. A ce stade, il est difficile pour le concepteur de juger de la sécurité d'une nouvelle solution. La mise en œuvre de la méthode IRAD impose de passer par le processus de risque. Ce passage a l'avantage de permettre au concepteur de se rendre compte des risques liés à la solution proposée et éventuellement de réviser cette solution.

2. Éliminer la situation dangereuse pour la personne

Le deuxième objectif est d'éliminer l'exposition à la situation dangereuse. Cet objectif est de type « contrainte de sécurité ». Il peut être formulé comme suit : « assurer la non-présence de l'opérateur dans la zone dangereuse dans toutes les phases de l'utilisation de la machine ». Cet objectif peut conduire le concepteur à formuler de nouvelles exigences fonctionnelles techniques qui vont dans le sens de l'élimination du besoin d'intervention de l'opérateur dans certaines tâches ou de séparer dans le temps (alterner) la présence de l'opérateur et la présence du phénomène dangereux. Ensuite, le concepteur avance dans le processus de conception en ajoutant ces exigences au niveau hiérarchique inférieur dans l'arbre fonctionnel.

3. Réduire la gravité du dommage lié au phénomène dangereux

Une fois que le concepteur épuise toutes les possibilités de solutions de conception sans phénomène dangereux, ou sans situation dangereuse, il adopte une solution comportant un (ou plusieurs) phénomène(s) dangereux. Il identifie les risques (dans le contexte C2) puis il cherche d'un côté, à réduire la gravité du dommage lié à ce phénomène dangereux et d'un autre coté, à éliminer (ou juste à réduire) la situation dangereuse. Pour cela, il ajoute dans le contexte C3 l'objectif de sécurité « réduire la gravité du dommage lié au phénomène dangereux ». La réduction de la gravité du phénomène dangereux demande donc ici de rajouter dans le processus de conception les exigences de sécurité suivante : « Prévenir le phénomène dangereux » et « Minimiser l'énergie liée à ce phénomène (force, vitesse, pression…) ».

La première exigence « Prévenir le phénomène dangereux » permet au concepteur d'ajouter des solutions de conception réduisant la gravité du dommage (par exemple, un système de ventilation pour répondre à l'exigence « prévenir d'une explosion »). La deuxième exigence « Minimiser l'énergie liée au phénomène dangereux » peut s'exprimer par une expression de minimisation de certains paramètres physiques du système. Comme cela est soulevé dans IRAD, la minimisation de l'énergie va, en général, dans le sens contraire à l'amélioration de la performance. Cette contradiction devrait apparaitre lors de la recherche de solution menée dans l'étape précédente de la conception. L'objectif de cette exigence est de diminuer l'énergie à un niveau acceptable techniquement sans remettre en cause la solution de conception adoptée.

4. Réduire la fréquence et/ou la durée de l'exposition à la situation dangereuse

Le quatrième objectif est de réduire la fréquence ou la durée d'exposition de l'opérateur. La notion de « situation dangereuse » comporte deux aspects ; un aspect temporel (fréquence et durée d'exposition) et un aspect spatial (zone dangereuse). La réduction de l'exposition à la situation dangereuse peut se faire en agissant sur ces deux aspects. Agir sur l'aspect temporel se fait à l'étape de la conception conceptuelle. Agir sur l'aspect spatial se traduit par la réduction de la zone dangereuse, ou plus précisément de l'accessibilité à la zone dangereuse, et relève de la réduction de l' « événement dangereux ». Cette démarche est réalisable à l'étape de la conception architecturale. Effectivement, c'est à ce niveau de la conception que s'effectuent le dimensionnement et l'analyse du système (choix des

paramètres géométriques, des matériaux, des composants, de l'architecture (agencement de différents sous-systèmes), …).

5. Réduire la probabilité d'occurrence de l'événement dangereux

Si le concepteur a réussi à éliminer la situation dangereuse, le risque lié au phénomène dangereux est donc éliminé et la conception proposée ne présente plus de risque pour l'opérateur. Cependant, dans le cas où la situation dangereuse n'a pas été complètement éliminée et que le risque lié à ce phénomène est toujours présent dans le processus de risque, le concepteur doit chercher à réduire la zone dangereuse, ou plus précisément l'accessibilité à la zone dangereuse qui relève de la réduction de l'« événement dangereux ». Elle est réalisée à l'étape de la conception architecturale.

Pour réduire l'événement dangereux, des objectifs de sécurité doivent être proposées au niveau structurel donc dans le contexte C3. L'exigence visant la réduction de la probabilité d'occurrence des événements dangereux peut souvent être exprimée par une équation de minimisation ou de maximisation de certains paramètres géométriques et physiques (« maximiser la distance entre l'opérateur et le phénomène dangereux », « maximiser la rigidité de la pièce tout en minimisant son poids » ou « maximiser la fiabilité des composants »). Pour un élément en rotation, le concepteur peut chercher à répondre à l'exigence de sécurité « Maximiser les distances entre les parties du corps de l'opérateur et l'élément tournant ».

6. Réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place d'un dispositif de protection

Si l'élimination de l'événement dangereux n'est pas réalisable, le concepteur va chercher à réduire la probabilité d'occurrence de l'événement dangereux par la mise en place d'un dispositif de protection au stade de la conception architecturale (par exemple des équipements de protection sensibles pour la détection des personnes dans la zone dangereuse).

7. Eliminer l'événement dangereux en évitant le dommage par la mise en place d'un dispositif de protection

L'élimination de l'événement dangereux supprime la probabilité d'avoir un accident causé par le phénomène dangereux en question. Ici, le concepteur doit chercher à éliminer l'accessibilité à la zone dangereuse par la mise en place d'un dispositif de protection.

Nous considérons qu'un dispositif de protection est un système en lui-même. La conception de ce système auxiliaire passe donc à nouveau par une phase de conception conceptuelle où le concept du dispositif est défini puis une phase de conception architecturale et enfin une phase de conception détaillée. Par conséquent, selon l'objectif de sécurité décidé, un processus de conception parallèle peut commencer. On peut noter ici que les normes de type B offrent au concepteur une grande aide pour alimenter le domaine fonctionnel des exigences de sécurité lors de la conception du dispositif de protection.

Si nous prenons l'exemple d'un élément en rotation, pour répondre à l'exigence « éliminer la possibilité de contact avec l'élément en rotation », le concepteur peut définir des exigences de manière à créer un obstacle entre le poste de travail de l'opérateur et l'élément en rotation. Il peut concevoir un protecteur fixe (en s'appuyant sur la norme NF EN 15811, 2010 intitulée « Protecteurs pour éléments mobiles de transmission de puissance »).

8. Réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place de mesures de protection

Lorsque le dispositif de protection ne remplit pas les objectifs d'élimination de l'événement dangereux ou de réduction de la probabilité d'occurrence des événements

dangereux, il est possible d'utiliser des mesures de protection complémentaires afin d'obtenir une réduction de la probabilité d'occurrence. Cela peut se faire, par exemple, en proposant des mesures relatives à l'accès sécurisé à la machine (voir ISO 12100-2:2003). Dans ce cas, un processus parallèle de conception du moyen de protection doit être mis en œuvre.

9. Eviter ou limiter le dommage après la conception

Finalement, les risques résiduels, non éliminés pendant la conception du système, doivent être évités en phase d'utilisation. Le concepteur doit alors ajouter à la machine des informations sur l'utilisation pour éviter les risques. Ces informations doivent être présentées sur la machine (panneaux d'avertissement, étiquettes pour l'utilisation en toute sécurité, signaux sonores et visuels, etc.) et fournies avec la machine (manuel d'instruction, données techniques). Le fournisseur de la machine doit préciser, dans le manuel d'instruction, si une formation est nécessaire afin de garantir que les utilisateurs sachent correctement utiliser la machine. Le fournisseur doit aussi préciser si un équipement de protection individuelle doit être utilisé pour protéger les personnes des phénomènes dangereux associés au risque résiduel. La figure 5.3 résume le processus d'identification des objectifs de sécurité pour un risque donné C2.

5.2.3.2. Risque identifié au niveau architectural

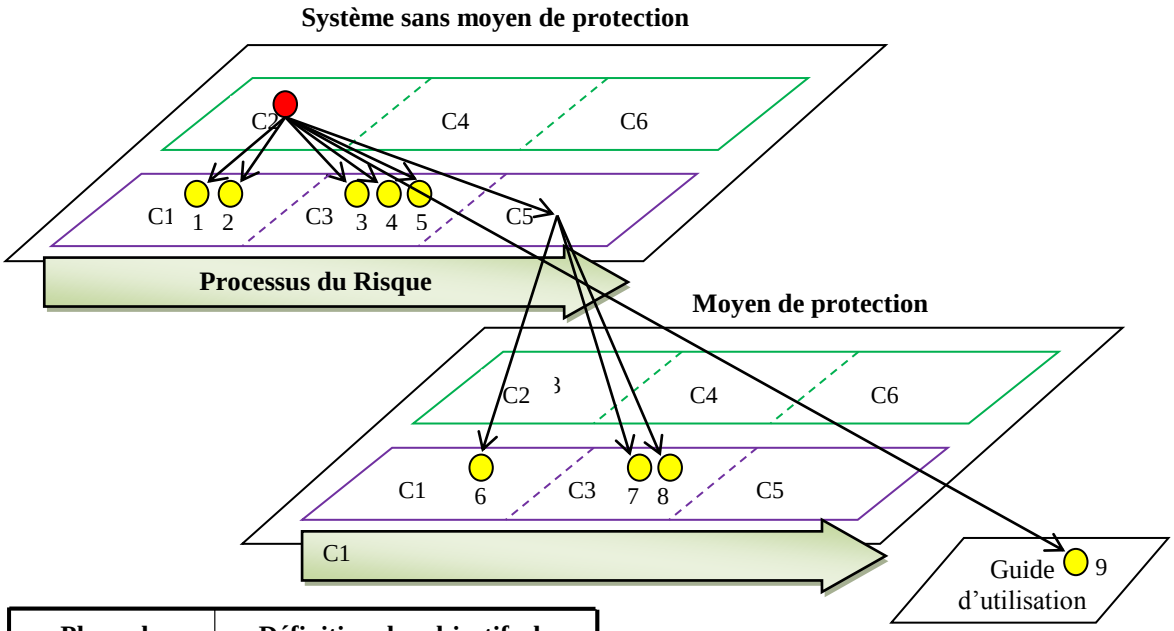
Pour les risques anthropométriques et de non fiabilité technique identifiés au niveau architectural (contexte C4), donc lié à une solution de conception proposée au niveau de la conception architecturale, le phénomène dangereux, la situation dangereuse et l'éventuel évènement dangereux doivent être identifiés [Sadeghi et al., 2012b]. Les origines des phénomènes dangereux liés aux risques C4 peuvent être par exemple une « vibration causée par un défaut d'alignement des pièces en mouvement », une « posture », liées à l'« emplacement des organes de service », «l'éclairage local », une « activité répétitive », ou encore un « effort ».

Pour ce type de risque, le concepteur doit d'abord proposer des objectifs de sécurité permettant d'éliminer le phénomène dangereux. L'élimination du phénomène dangereux se fait, ici, au niveau architectural. Par conséquent, les exigences de sécurité induites seront ajoutées au contexte C3 « éliminer l'origine du phénomène dangereux ». Ces exigences de sécurité peuvent être, par exemple, « Eliminer l'incompatibilité entre les caractéristiques morphologiques et les paramètres géométriques », « Prévenir les vibrations », ou « Minimiser les défauts d'alignement des pièces en mouvement ».

La figure 5.4 présente les objectifs de sécurité à prendre en compte et les contextes auxquels elles se rapportent.

5.2.3.3. Risque identifié au niveau détaillé

Pour un risque d'usage identifié au niveau détaillé (Contexte C6), donc lié à une solution de conception proposée au niveau de la conception détaillée, le phénomène dangereux, la situation dangereuse et l'éventuel évènement dangereux doivent être identifiés. La proposition des objectifs de sécurité se fait, ici, au niveau de la conception détaillée [Sadeghi et al., 2012b]. Ces objectifs de sécurité seront ajoutés au contexte C5, comme illustré à la figure 5.5.

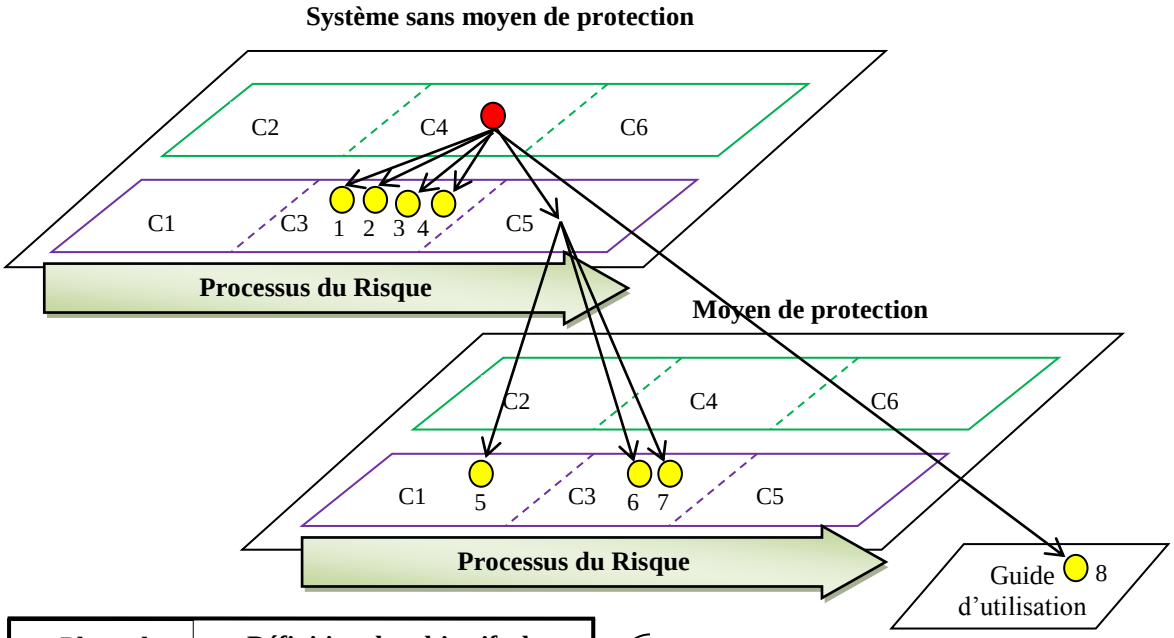


Phase du processus de conception	Définition des objectifs de sécurité pour un risque C2 sur le système
Phase conception conceptuelle Contexte C1	1. Eliminer le phénomène dangereux par conception.
	2. Éliminer la situation dangereuse pour la personne.
Phase conception architecturale Contexte C3	3. Réduire la gravité du dommage lié au phénomène dangereux.
	4. Réduire la fréquence et/ou de la durée de l'exposition à la situation dangereuse.
	5. Réduire la probabilité d'occurrence des événements dangereux.
Phase conception détaillée Contexte C5	-

Phase du processus de conception	Définition des objectifs de sécurité pour un risque C2 en ajoutant un moyen de protection
Phase conception conceptuelle Contexte C1	6. Eliminer l'événement dangereux en évitant le dommage par la mise en place d'un dispositif de protection.
Phase conception architecturale Contexte C3	7. Réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place d'un dispositif de protection.
	8. Réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place de mesures de protection.

Après le processus de conception	Définition des objectifs de sécurité pour un risque C2 sur le système
Guide d'utilisation	9. Eviter ou limiter le dommage après la conception.

Figure 5.3. Objectifs de sécurité fonction de la phase de conception pour un risque C2.

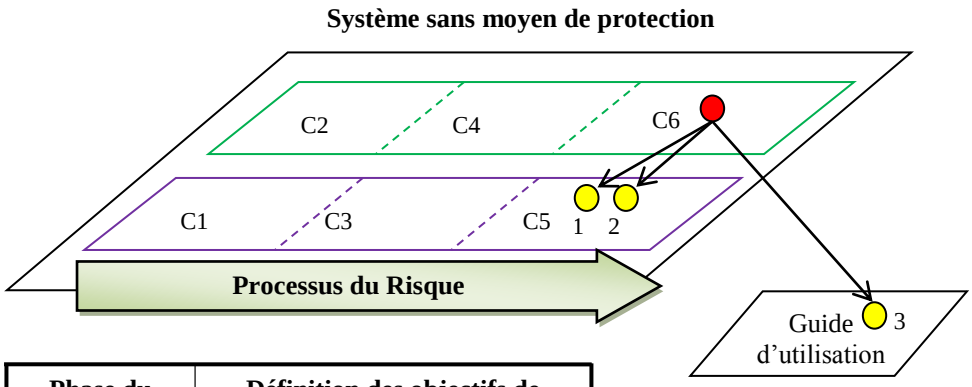


Phase du processus de conception	Définition des objectifs de sécurité pour un risque C4 sur le système
Phase conception architecturale / Contexte C3	1. Eliminer le phénomène dangereux au niveau architectural.
	2. Éliminer la situation dangereuse pour la personne.
	3. Réduire la gravité du dommage lié au phénomène dangereux.
	4. Réduire la fréquence et/ou de la durée de l'exposition à la situation dangereuse.
Phase conception détaillée / Contexte C5	-

Phase du processus de conception	Définition des objectifs de sécurité pour un risque C4 en ajoutant un moyen de protection
Phase conception conceptuelle / Contexte C1	5. Eliminer l'événement dangereux en évitant le dommage par la mise en place d'un dispositif de protection.
Phase conception architecturale / Contexte C3	6. Réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place d'un dispositif de protection.
	7. Réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place de mesures de protection.

Après le processus de conception	Définition des objectifs de sécurité pour un risque C4 sur le système
Guide d'utilisation	8. Eviter ou limiter le dommage après la conception.

Figure 5.4. Objectifs de sécurité fonction de la phase de conception pour un risque C4.



Phase du processus de conception	Définition des objectifs de sécurité pour un risque C4 sur le système
Phase conception détaillée	1. Eliminer le phénomène dangereux au niveau détaillé.
Contexte C5	2. Réduire la gravité du dommage lié au phénomène dangereux.

Après le processus de conception	Définition des objectifs de sécurité pour un risque C6 sur le système
Guide d'utilisation	3. Eviter ou limiter le dommage après la conception.

Figure 5.5. Objectifs de sécurité fonction de la phase de conception pour un risque C6.

5.2.3.4. Synthèse de l'approche proposée

La confrontation des étapes de la phase d'appréciation des risques ainsi que celles de la phase de réduction des risques de la norme [NF EN ISO 12100, 2010] et des six contextes du processus de risque de la méthode IRAD permet d'ordonner et d'identifier à quels stades du processus de conception les indications de la norme peuvent s'avérer pertinentes. En effet, la combinaison des principes et des idées définis dans les normes et la mise en œuvre de la méthode IRAD permettent de guider le concepteur dans la définition des objectifs de sécurité et leurs niveaux d'intervention dans le processus de conception à partir des risques identifiés. Leur prise en compte au moment opportun durant le processus de conception doit permettre de diminuer, voire d'éliminer ces risques à moindre coût. Cet ordre de priorité aide à mieux préciser les objectifs de sécurité à proposer à chaque phase de la conception du système ou de la partie du système impliquée dans l'accident. L'ordre utilisé est donc le suivant:

1. **Eliminer le phénomène dangereux par conception** en écartant la solution qui introduit le phénomène dangereux ;
2. **Éliminer les situations dangereuses pour la personne** en écartant la solution qui introduit l'activité d'utilisation pour assurer la non-présence de l'opérateur dans la zone dangereuse dans toutes les phases de l'utilisation du système ;
3. **Réduire la gravité du dommage lié au phénomène dangereux** par la minimisation de l'énergie liée au phénomène dangereux ou par l'optimisation de certains paramètres physiques du système : force, vitesse, pression, …;

4. **Réduire la fréquence et/ou la durée d'exposition aux situations dangereuses** par la diminution de la fréquence d'utilisation, du temps d'utilisation, … en considérant le dimensionnement et l'analyse du système comme choix des paramètres géométriques, des matériaux, des composants, de l'architecture, … ;
5. **Réduire la probabilité d'occurrence de l'événement dangereux** en optimisant certains paramètres géométriques et physiques : caractéristiques géométriques (taille, hauteur, largeur, longueur, …), dimension, distance, orientation, coordination,… ;
6. **Eliminer l'événement dangereux** en évitant le dommage par la mise en place d'un dispositif de protection;
7. **Réduire la probabilité d'occurrence de l'événement dangereux** en éliminant le dommage par la mise en place d'un dispositif de protection;
8. **Réduire la probabilité d'occurrence de l'événement dangereux** en éliminant le dommage par la mise en place de mesures de protection;
9. **Eviter ou limiter le dommage après la conception** par la rédaction de recommandations insérées au guide d'utilisation afin de suggérer les tâches à faire et à ne pas faire. Ces recommandations pourront être formulées sous la forme de phrases commençant par Faire, Mettre, Éloigner, Faire attention à, Aviser, … Ces informations seront précisées sur la machine (panneaux d'avertissement, étiquettes pour l'utilisation en toute sécurité, signaux sonores et visuels, etc.) et fournies avec la machine (manuel d'instruction, données techniques).

5.2.4. Application : définition des objectifs de sécurité contre le happement par un arbre de transmission à cardans

5.2.4.1. Définition des objectifs de sécurité

Le but de cette partie est de définir comment répondre aux objectifs de sécurité en vue de l'amélioration de la sécurité de l'Arbre de Transmission à Cardans (ATC). Comme présenté dans la partie application du chapitre 3, l'ATC peut causer un « happement » lorsque l'« Homme se tient à proximité de l'arbre de transmission », et que l'« Arbre de transmission à cardans fonctionne », et que la « le protecteur est absent ou le protecteur est endommagé ou bien mal ajusté ». Dans la partie application du chapitre 4, nous avons identifié que le risque lié à cet accident est un risque d'accident (risque C2), c'est-à-dire lié à la phase de la conception conceptuelle. Nous appliquons donc la démarche résumée à la figure 5.3 pour définir les objectifs de sécurité permettant d'éliminer ou de réduire le risque de happement:

Objectif de sécurité n°1. Eliminer le phénomène dangereux par conception : La première idée est de « changer la solution de conception adoptée ». La solution à changer est ici l'arbre assurant la transmission de mouvement entre le tracteur et l'outil (dans l'étape de recherche de solutions, le concepteur peut proposer d'autres concepts, par exemple, une transmission hydraulique, électromagnétique, etc.). L'exigence de sécurité est ici : « Eliminer l'élément en rotation en le remplaçant par un autre élément plus sécuritaire ».

Objectif de sécurité n°2. Éliminer la situation dangereuse pour la personne : Pour éliminer la situation dangereuse « opérateur se tient à proximité de l'arbre de transmission », nous devons « Eliminer le besoin d'intervention de l'opérateur à proximité de l'ATC dans toutes ses phases d'utilisation».

Objectif de sécurité n°3. Réduire la gravité du dommage lié au phénomène dangereux : Pour réduire la gravité du dommage lié au happement par l'ATC, nous pouvons par exemple « Minimiser la vitesse de rotation de l'arbre de transmission ou le couple ».

Objectif de sécurité n°4. Réduire la fréquence et/ou la durée de l'exposition à la situation dangereuse : Pour réduire l'exposition à la situation dangereuse « opérateur se tient à proximité de l'arbre de transmission », nous pouvons « Minimiser la fréquence ou la durée de l'exposition de l'opérateur à proximité de l'ATC ».

Objectif de sécurité n°5. Réduire la probabilité d'occurrence de l'événement dangereux : L'objectif de cette exigence est de réduire la probabilité de contact avec les éléments tournants de l'ATC. Il faut donc assurer l'arrêt de l'arbre en cas de présence de l'opérateur dans la zone dangereuse. Donc, nous devons « Arrêter la rotation de l'arbre en cas d'absence de l'opérateur de son poste de travail ».

Objectif de sécurité n°6. Eliminer l'événement dangereux en évitant le dommage par la mise en place d'un dispositif de protection: L'objectif de sécurité peut être « Eliminer la possibilité de contact de l'opérateur avec l'arbre mobile en cas de manque ou d'endommagement du protecteur » ou « Eliminer la possibilité de cassure et d'endommagement dans les conditions de travail de la liaison tracteur-outil en proposant un nouveau concept de protecteur ».

Objectif de sécurité n°7. Réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place d'un dispositif de protection: L'objectif de sécurité peut être : « Minimiser la possibilité de contact de l'opérateur avec l'arbre mobile en cas de manque ou d'endommagement du protecteur» ou « Maximiser la fiabilité du protecteur ».

Objectif de sécurité n°8. Réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place de mesures de protection: L'objectif de sécurité peut être « Arrêter la rotation de l'arbre en cas de manque ou d'endommagement du protecteur ».

Objectif de sécurité n°9. Eviter ou limiter le dommage après la conception : afin d'éviter ou de limiter les dommages après la conception de l'ATC, nous pouvons proposer les informations suivantes pour l'utilisation :

- « ne pas se tenir à proximité de la prise de force et de l'ATC lorsque la prise de force est en fonctionnement » ;
- «ne nettoyer, graisser ou régler la machine entraînée par une prise de force ou par l'ATC qu'après avoir débrayé la prise de force, coupé le moteur et enlevé la clé de contact » ;
- « arrêter le moteur et retirer la clé de contact avant toute intervention sur la machine» ;
- etc.

La figure 5.6 résume les objectifs de sécurité contre le happement par l'ATC.

Phase du processus de conception	Définition des objectifs de sécurité pour un risque C2 sur l'ATC
Phase conception conceptuelle Contexte C1	1. «Eliminer l'élément en rotation en le remplaçant par un autre élément plus sécuritaire».
	2. « Eliminer le besoin d'intervention de l'opérateur à proximité de l'ATC dans toutes ses phases d'utilisation».
Phase conception architecturale Contexte C3	3. « Minimiser la vitesse de rotation de l'arbre de transmission ou le couple ».
	4. « Minimiser la fréquence ou la durée de l'exposition de l'opérateur à proximité de l'ATC ».
	5. « Arrêter la rotation de l'arbre en cas d'absence de l'opérateur de son poste de travail ».
Phase conception détaillée Contexte C5	-

Phase du processus de conception	Définition des objectifs de sécurité pour un risque C2 en ajoutant un moyen de protection
Phase conception conceptuelle Contexte C1	6. « Eliminer la possibilité de contact de l'opérateur avec l'arbre mobile en cas de manque ou d'endommagement du protecteur » ou « Eliminer la possibilité de cassure et d'endommagement dans les conditions de travail de la liaison tracteur-outil en proposant un nouveau concept de protecteur».
Phase conception architecturale Contexte C3	7. « Minimiser la possibilité de contact de l'opérateur avec l'arbre mobile en cas de manque ou d'endommagement du protecteur» ou « Maximiser la fiabilité du protecteur ».
	8. « Arrêter la rotation de l'arbre en cas de manque ou d'endommagement du protecteur ».

Après le processus de conception	Définition des objectifs de sécurité pour un risque C2 sur le système
Guide d'utilisation	9. « Ne pas se tenir à proximité de la prise de force et de l'ATC lorsque la prise de force est en fonctionnement » ; . «Ne nettoyer, graisser ou régler la machine entraînée par une prise de force ou l'arbre de transmission qu'après avoir débrayé la prise de force, coupé le moteur et enlevé la clé de contact » ; . « Arrêter le moteur et retirer la clé de contact avant toute intervention sur la machine» ; . etc.

Figure 5.6. Objectifs de sécurité contre le happement par l'arbre de transmission à cardans.

5.2.4.2. Conclusion sur l'application

Au cours des chapitres 3 et 4, nous avons déterminé que les faits « Homme se tenant à proximité de l'ATC », « ATC fonctionne », et « Absence de protecteur ou protecteur endommagé ou bien mal ajusté » peuvent causer le « happement ». Le risque lié à l'ATC est un risque conceptuel (C2). En se basant sur ces connaissances, nous avons défini les objectifs

de sécurité pour éliminer ou réduire le risque de happement par l'ATC (figure 5.5). Les objectifs de sécurité numérotés de 1 à 5 sont liés à l'ATC sans moyen de protection, ceux numérotés de 6 au 8 concernent le moyen de protection de l'ATC.

5.2.5. Conclusion

Dans cette section, nous avons développé une approche susceptible de définir les niveaux d'intervention possibles et les phases de conception impactées permettant de répondre à des objectifs de sécurité.

La norme [NF EN ISO 12100, 2010] traite ce sujet. Cependant celle-ci reste très générale et laisse la responsabilité aux concepteurs de la manière de réaliser la démarche de réduction des risques, notamment sur l'intégration au moment opportun des exigences de sécurité dans le processus de conception. La plupart des travaux scientifiques sur la réduction des risques s'inspirent de cette norme afin d'éliminer ou de réduire les risques. Cependant, hormis le cas de la méthode IRAD, ces travaux ne proposent pas d'introduire les résultats de cette démarche de réduction des risques au bon moment lors la conception. La méthode IRAD va donc plus loin que les autres travaux même si elle ne guide pas le concepteur dans la définition des exigences de sécurité.

L'approche proposée répond à ces manquements. Elle permet au concepteur d'introduire la bonne exigence de sécurité au bon moment de la conception. C'est-à-dire que, pour un risque donné (et donc un type de risque donné), nous proposons de définir et de hiérarchiser les objectifs de sécurité et d'identifier leurs niveaux d'intervention dans le processus de conception. L'approche proposée a ensuite été appliquée à l'ATC. Elle a permis de proposer des objectifs de sécurité en vue de l'élimination ou de la réduction du risque de happement induit par l'ATC.

La partie suivante fait suite à celle-ci dans une démarche de reconception sécuritaire. Son objectif est de répondre à la question : *« Face aux nouveaux objectifs de sécurité, comment développer le processus de conception ? » ;* l'idée étant de prendre en considération ces objectifs de sécurité au même titre que les objectifs techniques lors de la synthèse des solutions.

5.3. Développement d'une approche de reconception sécuritaire

5.3.1. Introduction

Comme nous l'avons déjà dit, la problématique globale de nos travaux de recherche est : *Comment mettre en œuvre l'intégration de la sécurité dans le processus de conception pour l'obtention d'un système sécuritaire ?* La section précédente a proposé une approche d'identification et de priorisation des objectifs de sécurité pour un risque donné afin d'éliminer ou de réduire la possibilité d'accident. Le but de cette section est de reconcevoir le système en s'appuyant sur ces objectifs de sécurité. Ainsi, parmi un ensemble de nouvelles solutions, il faut être capable de choisir la solution la plus sécuritaire. Pour cela, nous utilisons notamment l'indicateur de sécurité développé dans le chapitre 4. Cette section doit donc répondre aux deux questions suivantes:

Comment choisir un objectif de sécurité parmi les différents objectifs de sécurité identifiés? Comme nous l'avons proposé, pour chaque risque donné (contexte), il est possible de définir plusieurs objectifs de sécurité. Ce choix est important puisqu'il est à la base du processus de reconception sécuritaire. Nous proposons donc d'aider le concepteur à faire ce choix. Ce choix fait, reste la mise en œuvre du processus de conception sécuritaire. Il conviendra donc ensuite de répondre à la question:

Suite au choix de l'objectif de sécurité, comment reconcevoir de la façon la plus sécuritaire possible? L'approche FRES que nous avons proposée est essentiellement basée sur la conception axiomatique. Cependant, l'application de la conception axiomatique ne permet pas une description claire de la manière avec laquelle on aboutit à une solution. Il est donc nécessaire d'intégrer dans notre approche **les méthodes d'analyse de problèmes et de génération d'idées (**comme l'essai-erreur, le brainstorming ou encore TRIZ), en complément de la conception axiomatique afin d'aider le concepteur à obtenir des solutions. Parmi ces méthodes, la théorie TRIZ semble intéressante du fait qu'elle formalise la conception comme une contradiction à résoudre. En effet, TRIZ formule les solutions en précisant le processus de résolution d'une contradiction. Cet ensemble de solutions trouvé, le choix de la meilleure d'entre-elles pourra être fait en calculant leur indicateur de sécurité respectif tel que proposé dans le chapitre 4.

Dans un premier temps, dans la section 5.3.2, nous présentons un bref état de l'art sur la théorie TRIZ. La section 5.3.3 porte sur le développement de l'approche de reconception sécuritaire. Cette approche est ensuite appliquée sur le cas d'étude : l'Arbre de Transmission à Cardans (ATC) dans la section 5.3.4. Enfin, la section 5.3.5 présente la conclusion et les perspectives de cette partie.

5.3.2. La Théorie de la Résolution des Problèmes Inventifs (TRIZ)

5.3.2.1. Présentation de TRIZ

La Théorie de la Résolution des Problèmes d'invention (TRIZ) a été proposée par [Altshuller, 1984]. Cette théorie n'est pas une méthode de conception car cantonnée à la recherche de concept.TRIZ aide le concepteur à la recherche de solutions en s'appuyant sur des outils d'analyse du problème de conception et sur des bases de connaissances permettant de faire évoluer le problème de conception. La proposition de la méthode TRIZ vient de la constatation que seulement 1% des solutions sont vraiment innovantes, les concepteurs utilisent des idées ou des concepts déjà connus, mais d'une façon nouvelle [Altshuller, 2004 ; Altshuller, 2006]. La figure 5.7 représente le processus de résolution des problèmes selon TRIZ. Ce processus est composé de quatre étapes : (1) Formuler le problème que l'on souhaite résoudre ; (2) Modéliser le problème ; (3) Identifier des modèles de solutions, et (4) Générer des solutions.

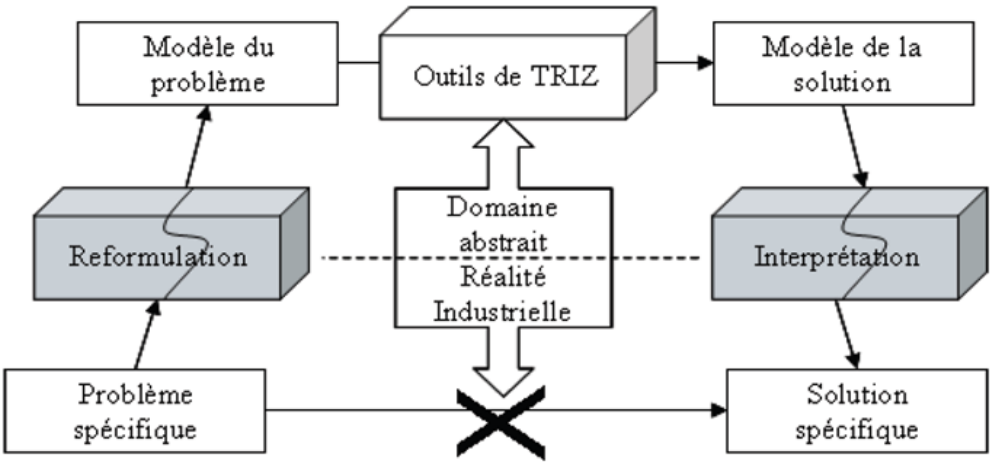


Figure 5.7. Processus de résolution des problèmes selon TRIZ.

L'apport majeur de cette théorie, par rapport aux approches traditionnelles telles que l'Essai-Erreur et le Brainstorming, est qu'elle donne des directions pour la recherche des solutions basées sur des modèles d'ingénierie. L'aléatoire réside principalement dans la formalisation du problème et l'interprétation des directions données [Ghemraoui, 2009].

5.3.2.2. Présentation des outils de TRIZ

La méthode TRIZ propose plusieurs outils et techniques pour aider le concepteur à la recherche de solutions. [Souchkov, 2008] propose un bref aperçu chronologique des outils et techniques de TRIZ, ainsi que les concepts apparus de 1946 à 2008. Plus tard, [Ilevbare et al., 2013] ont identifiés les outils et techniques les plus importants de TRIZ. Ainsi, les auteurs listent 40 principes inventifs, 76 solutions standards, une base de données des effets, les principes de séparation, la matrice de contradiction, les modèles de l'évolution des systèmes techniques, l'IFR (pour Ideal Final Result), l'idéalité, l'essayage, l'analyse de fonction, l'analyse de Su-Field, l'analyse des ressources du système, les neuf fenêtres, les outils de la créativité, et ARIZ (pour Algorithm for Inventive Problem Solving).

[Zlotin et al., 2000] a classé les outils de TRIZ en trois groupes :

- Les outils analytiques : les outils comme l'analyse de Su-Field, l'analyse de fonction, et ARIZ aidant à définir, à formuler et à modéliser un problème ;
- Les outils basés sur des connaissances : les outils comme les 40 principes inventifs et les 76 solutions standards fournissant des recommandations pour la résolution du problème ;
- Les outils psychologiques : ces outils aident à faciliter le processus de résolution de problèmes.

[Moehrle, 2005] fournit un cadre pour structurer les outils selon les applications. Il a identifié cinq domaines d'application. Il s'est ensuite basé sur ces domaines d'application pour classer les concepts, outils et techniques de TRIZ sous le format d'une table (tableau 5.1).

Tableau 5.1. Classification des concepts, outils et techniques de TRIZ basée sur les domaines d'application (Adaptée de [Moehrle, 2005]).

Applications	Question	Concept/ outil/ technique
Situation actuelle	Quelle est la situation actuelle ?	- Analyse de fonction - Contradiction - Analyse de Su-Field - Analyse d'évolution
État prévue	A quoi la situation future est censée ressembler?	- Forte Solution
Objectifs	Quelles objectifs doivent être atteints et dans quelle mesure?	- IFR(Ideal Final Result) - Essayage
Transformation	Comment l'état actuel peut être transformé en l'état prévu?	- Principes inventifs - Matrice de contradiction - Principes de séparation - Analyse de Su-Field - Analyse d'évolution - Analyse des ressources - Base de données des effets
Ressource	Quelles ressources sont disponibles et peuvent être utilisés?	- Analyse des ressources (Analyse de système, Analyse de Su-Field and effectuer une recherche systématique des ressources)

[Filippi et al., 2010] ont proposé une classification des outils et techniques de TRIZ basé sur les phases et types de solutions. Comme illustré dans le tableau ci-dessous, [Filippi et al., 2010] ont décomposé les phases de solution en trois sous phases : les phases d'enquête,

d'abstraction et de solution selon qu'il s'agit de la conception ou de la reconception d'un système.

Tableau 5.2. Classification des méthodes de TRIZ selon [Filippi et al., 2010].

	Phase d'enquête	**Phase d'abstraction**	**Phase de solution**
Reconception	Liste d'innovation Liste des ressources	Analyse de fonction Analyse de Root Conflicts Analyse de RelEvent	Principes inventifs Matrice de contradiction
Conception	Liste d'innovation Liste des ressources	Analyse de fonction Analyse de Root Conflicts Analyse de RelEvent Analyse de Su-Field Tendances de l'évolution	Principes inventifs Matrice de contradiction 76 solutions standards

Ce tableau montre que les Principes inventifs, la Matrice de contradiction et les 76 Solutions standard sont des outils de génération des solutions.

[Dickinson, 2004] a proposé une présentation des éléments basiques de TRIZ sous le format d'une figure (figure 5.8). Cette figure montre que pour améliorer un concept, la Matrice de contradiction, les Principes inventifs, les Modèles d'évolution, et l'Effet physique sont des outils qui semblent intéressants.

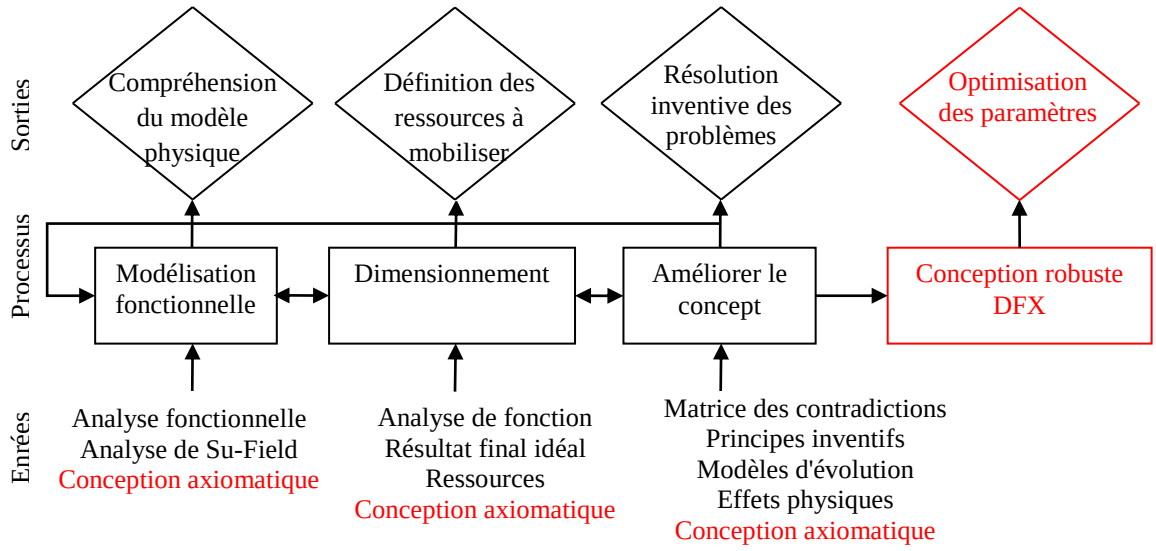


Figure 5.8. Les éléments basiques de la méthode TRIZ [d'après Dickinson, 2004].

Ce bref état de l'art montre que les outils de TRIZ les plus cités et utilisés sont :

- **L'analyse de fonction :** pour comprendre les interactions entre tous les composants du système et faire ressortir les problèmes posés par les interactions.
- **L'analyse de Su-Field :** afin d'aider à cartographier l'ensemble du système et indiquer exactement les problèmes sans ajouter de détails inutiles.
- **La matrice des contradictions :** pour préciser les principes inventifs qui peuvent être appliqués afin de résoudre une contradiction technique.
- **Les 11 principes de séparation :** pour résoudre une contradiction physique.

- **Les 76 solutions standards :** pour résoudre les problèmes du système sans la nécessité d'identifier les contradictions. Ils sont généralement appliqués pour corriger l'interaction indésirable entre deux parties d'un système.
- **Les 40 principes inventifs :** afin de trouver des solutions conceptuelles aux contradictions techniques et physiques.
- **ARIZ (Algorithm for Inventive Problem Solving):** permettant de trouver des solutions et des innovations et basé sur une série d'étapes utilisant une gamme d'outils de TRIZ. Cet outil est le plus approprié pour des problèmes difficiles et complexes.

Il faut noter deux types de contradiction:

- **Contradiction physique** : deux demandes opposées mais sur le même paramètre.
- **Contradiction technique** : deux demandes opposées, chacune sur un paramètre différent.

5.3.2.3. Synthèse et positionnement par rapport à nos objectifs

Dans le cadre de notre approche, nous souhaitons définir les nouvelles solutions sécuritaires en nous basant sur les objectifs de sécurité. Les objectifs de sécurité s'expriment par une maximisation, une minimisation ou un remplacement (ou changement) des paramètres de conception.

L'application de cette maximisation, ou minimisation, entraine souvent une variation d'autres caractéristiques du système dans un sens non désiré et donc une contradiction. Parmi les outils de TRIZ déjà listés, la matrice des contradictions semble la plus intéressante pour répondre aux besoins de maximisation ou de minimisation de paramètres de conception.

Le remplacement (ou le changement) se traduit par une contradiction physique de deux caractéristiques d'un même paramètre. Parmi les outils de TRIZ, les 11 principes de séparation semblent les plus intéressants pour répondre aux exigences de sécurité sous cette forme. Nous présentons ci-dessous ces deux outils de TRIZ plus en détail.

Matrice des contradictions

TRIZ permet d'une part d'identifier les 39 paramètres possibles rencontrés de façon récurrente dans la plupart des brevets caractérisant le problème, et d'autre part, de capter les 40 principes, servant à la résolution de ces contradictions.

Les 39 paramètres de conception et les 40 principes d'innovation sont montrés dans le tableau 5.3.

Tableau 5.3. Les 39 paramètres de conception et les 40 principes d'innovation.

39 paramètres de conception	**40 principes d'innovation**
1 Masse d'un objet mobile	1 Segmentation
2 Masse d'un objet immobile	2 Extraction, séparation
3 Longueur d'un objet mobile	3 Qualité locale
4 Longueur d'un objet immobile	4 Asymétrie
5 Surface d'un objet mobile	5 Fusion, intégration, combinaison
7 Volume d'un objet mobile	6 Universalité, multifonctions
6 Surface d'un objet immobile	7 Imbrication
8 Volume d'un objet immobile	8 Contrepoids
9 Vitesse	9 Action inverse antérieure
10 Force	10 Action préliminaire
11 Tension et pression	11 Protection ou compensation
12 Forme	12 Equipotentialité, élimination de la tension
13 Stabilité	13 Inversion
14 Résistance	14 Courbe, arrondi, cerclage
15 Longévité d'un objet mobile	15 Dynamisation, optimisation
16 Longévité d'un objet immobile	16 Surplus ou la réduction
17 Température	17 Changement de dimension
18 Brillance	18 Oscillation
19 Energie dépensée par l'objet mobile	19 Action périodique
20 Energie dépensée par l'objet immobile	20 Action d'utilité
21 Puissance	21 Aléatoire
22 Perte d'énergie	22 Transformation d'un plus en moins
23 Perte de matière - substance	23 Asservissement
24 Perte d'information	24 Insert ion
25 Perte de temps	25 Self-service
26 Qualité de matière - substance	26 Copie
27 Fidélité	27 Ephémère et l'économique
28 Précision de la mesure	28 Reconception
29 Précision de l'usinage	29 Système hydraulique
30 Facteurs nuisibles agissant sur l'objet	30 Membrane flexible
31 Facteurs nuisibles annexes	31 Porosité du matériau
32 Usinabilité	32 Changement de couleur ou transparence
33 Facilité d'utilisation	33 Homogénéité
34 Aptitude à la réparation	34 Rejet et la régénération
35Adaptabilité	35 Modification (de la valeur, des propriétés) d'un paramètre
36 Complexité de l'appareil	36 L'utilisation des changements de phase
37 Complexité de contrôle	37 Dilatation, expansion thermique
38 Degré d'automatisation	38 Environnement ou atmosphère enrichi, oxydation accélérée
39 Productivité	39 Environnement ou atmosphère inerte
	40 Matériau ou structures composites

Altshuller a ainsi construit une matrice des contradictions, qui se présente sous la forme d'une table où les lignes correspondent aux paramètres à améliorer et les colonnes aux paramètres à ne pas dégrader. A chaque croisement ligne-colonne, la table donne un à quatre principes généraux correspondants aux solutions ou pistes de solutions. Nous montrons l'exemple de résolution représentant la matrice des contradictions dans la figure 5.9 ci-

dessous. Les principes inventifs 26, 35, 18, 19 sont les plus souvent mobilisées dans les brevets, pour améliorer le paramètre **1** « masse d'un objet mobile » sans dégrader le paramètre **38** « degré d'automatisation ».

Paramètre à améliorer \ Paramètre à ne pas dégrader		1 Masse d'un objet mobile	2 Masse d'un objet immobile	3 Longueur d'un objet mobile	4 Longueur d'un objet immobile	... ...	38 Degré d'automatisation	39 Productivité
1	Masse d'un objet mobile		-	15, 8, 29,34	-	…	26, 35 18, 19	35, 3, 24, 37
2	Masse d'un objet immobile	-		-	10, 1, 29, 35	…	2, 26, 35	1, 28, 15, 35
3	Longueur d'un objet mobile	8, 15, 29, 34	-		-	…	17, 24, 26, 16	14, 4, 28, 29
4	Longueur d'un objet immobile	-	35, 28, 40, 29	-		…	-	30, 14, 7, 26
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
38	Degré d'automation	28, 26, 18, 35	28, 26, 35, 10	14, 13, 17, 28	23	…		5, 12, 35, 26
39	Productivité	35, 26, 24, 37	28, 27, 15, 3	18, 4, 28, 38	30, 7, 14, 26	…	5, 12, 35, 26	

Figure 5.9. Utilisation de la matrice des contradictions.

Les 11 principes de séparation

[Alshuller, 2004] en analysant des brevets, a formalisé 11 principes de séparation permettant de résoudre les contradictions physiques. Ces principes sont les suivants:

1. Séparer les paramètres contradictoires dans l'espace ;
2. Séparer les paramètres contradictoires dans le temps ;
3. Associer des systèmes homogènes ou hétérogènes au niveau macro ;
4. Transférer le système vers l'antisystème, ou combiner le système avec l'antisystème ;
5. Attribuer la propriété P au système et l'anti-propriété P' aux différentes sous parties du système ;
6. Transférer un paramètre à un système fonctionnant au niveau micro ;
7. Effectuer une transition de phase d'une partie du système ou d'une partie de l'environnement sans introduction de substances étrangères ;
8. Utiliser les propriétés de deux phases du système. Le changement de phase est alors piloté par les conditions de fonctionnement du système ;
9. Utiliser les phénomènes physiques associés aux changements de phase ;
10. Remplacer un état de substance par un mélange des deux phases de cette même substance ;
11. Faire apparaître ou disparaître une substance par décomposition moléculaire ou recombinaison moléculaire.

5.3.3. Reconception sécuritaire

5.3.3.1. Aide à la décision pour le choix de l'objectif de sécurité à intégrer dans le processus de conception

La première phase de l'approche FR2ES a permis de catégoriser les objectifs de sécurité en fonction du type de risque (risques de types C2, C4 et C6). La seconde phase consiste à reconcevoir le système en intégrant ces objectifs de sécurité dans le processus de conception. Une question importante qui se pose alors est : *Quel objectif de sécurité choisir parmi les différents objectifs de sécurité identifiés ?*

Le choix de l'objectif de sécurité n'est pas fixé au niveau de conception identifié à partir du type de risque. Notamment de par le fait que l'espace des possibles en termes de reconception dépend d'autres paramètres que de la sécurité, le choix peut se faire dans des niveaux d'amélioration de la sécurité moindre. Il est à noter ici que l'importance des modifications à apporter au système est décroissante lorsque que l'on descend dans la hiérarchie des objectifs de sécurité définie au §5.2.3.

Ainsi, si le risque identifié est de type C2, la première phase de conception où l'on doit intervenir est la phase de la conception conceptuelle. L'objectif initial est donc celui arrivant en première position dans la hiérarchie des objectifs de sécurité, c'est-à-dire : « Eliminer le phénomène dangereux par conception ». A ce niveau, le concepteur doit se poser la question suivante : Est-ce que l'on veut/peut éliminer le phénomène dangereux par conception en changeant le concept du système ? Si la réponse est positive, l'objectif de sécurité est fixé. Si la réponse est négative, l'objectif initial de sécurité devient celui arrivant en deuxième position dans la hiérarchie et la question que le concepteur doit alors se poser est : « Est-ce que l'on veut/peut éliminer la situation dangereuse pour la personne ? » Si la réponse est positive, l'objectif de sécurité est fixé. Dans le cas contraire, on passe à l'objectif de sécurité suivant et ainsi de suite jusqu'à obtenir une réponse positive.

Pour un risque de type C4, la première phase de conception où l'on doit intervenir est la phase de la conception architecturale. L'objectif initial est celui arrivant en première position dans la hiérarchie des objectifs de sécurité, c'est-à-dire : « Eliminer le phénomène dangereux au niveau architectural ». A ce niveau, le concepteur doit se poser la question suivante : Est-ce que l'on veut/peut éliminer le phénomène dangereux en changeant l'architecture du système ? Si la réponse est positive, l'objectif de sécurité est fixé. Si la réponse est négative, l'objectif initial de sécurité devient celui arrivant en seconde position dans la hiérarchie et la question que le concepteur doit alors se poser est : « Est-ce que l'on veut/peut éliminer la situation dangereuse pour la personne ? » Si la réponse est positive, l'objectif de sécurité est fixé. Dans le cas contraire, on passe à l'objectif de sécurité suivant et ainsi de suite jusqu'à obtenir une réponse positive.

Pour un risque de type C6, la phase de conception où l'on doit intervenir est la phase de la conception détaillée. La procédure est la même que pour les deux autres types de risques. L'objectif initial est celui arrivant en première position dans la hiérarchie des objectifs de sécurité, c'est-à-dire : « Eliminer le phénomène dangereux au niveau détaillé ». Le concepteur doit se poser la question suivante : Est-ce que l'on veut/peut éliminer le phénomène dangereux en modifiant certains détails du système ? Si la réponse est positive, l'objectif de sécurité est fixé. Si la réponse est négative, l'objectif initial de sécurité devient celui arrivant en deuxième position dans la hiérarchie et la question que le concepteur doit alors se poser est : Est-ce que l'on veut/peut « Réduire la gravité du dommage en modifiant les détails du système ? ». Si la réponse est positive, l'objectif de sécurité est fixé. Dans le cas contraire, la seule alternative possible consiste à éviter ou limiter le dommage par

l'intégration de recommandations dans le guide d'utilisation, l'ajout de pictogramme sur la machine, etc.

5.3.3.2. Définition des exigences fonctionnelles

L'objectif de sécurité maintenant choisi, la question qui se pose est : *Comment cet objectif de sécurité peut être pris en compte dans le processus de conception ?* Pour un objectif de sécurité choisi, il faut définir les exigences fonctionnelles. Un objectif de sécurité s'exprime selon l'une des trois façons suivantes :

- **Maximiser** un paramètre de conception (par exemple « Maximiser la distance entre l'opérateur et l'arbre tournant ») ;
- **Minimiser** un paramètre de conception (par exemple « Minimiser la vitesse de rotation de l'arbre de transmission »);
- **Remplacer** (ou Changer) un paramètre de conception (par exemple « Remplacer l'élément en rotation par un autre élément plus sécuritaire »).

Par exemple, dans le cas de l'ATC, l'objectif « Réduire la gravité du dommage lié au phénomène dangereux » peut se traduire par les exigences « Minimiser la vitesse de rotation », « Minimiser le couple transmis par l'arbre » et « Minimiser l'énergie cinétique de l'arbre ».

5.3.3.3. Définition des solutions candidates

Concevoir consiste à associer une solution à un besoin (objectif). De nombreux travaux scientifiques détaillent comment y parvenir en utilisant les théories de la conception systématique, de la conception axiomatique (AD) et de TRIZ [Yang et Zhang, 2000 ; Dickinson, 2004 ; etc].

D'un côté, l'AD exprime les règles d'une bonne conception par l'intermédiaire de ses deux axiomes, mais ne propose pas de description claire de la manière avec laquelle aboutir à une solution. Autrement dit, l'AD permet de définir des problèmes et d'analyser des solutions, mais ne permet pas de générer des idées.

D'un autre côté, TRIZ formalise la conception comme une contradiction à résoudre. C'est-à-dire, qu'elle formule les solutions en précisant le processus de résolution d'une contradiction. Dans le § 5.3.2, nous avons présenté un état de l'art sur la théorie TRIZ, sur ses outils et techniques pour rechercher des solutions et avons montré que la matrice de contradiction et les 11 principes de séparation conviennent à plusieurs étapes de notre travail.

Lorsque, dans un système, l'amélioration d'un paramètre ou d'une caractéristique technique (en le maximisant ou le minimisant) entraine la détérioration d'un autre paramètre ou caractéristique, on parle de contradictions. Celles-ci peuvent être résolues en utilisant, par exemple, la matrice des contradictions qui propose des pistes de solution (les principes inventifs). Dans ce cas, nous devons :

1. Identifier le paramètre à préserver et le paramètre à améliorer en se basant sur les causes d'accidents lié au système identifié dans le chapitre 3 (§3.2) ;
2. Résoudre la contradiction en utilisant la matrice des contradictions pour trouver les principes appropriés au système étudié ;
3. Proposer des solutions basées sur les principes inventifs retenus.

« Le remplacement » ne présente pas de contradiction technique. Il se traduit par une contradiction physique de deux caractéristiques d'un même paramètre. Parmi les outils de TRIZ, les 11 principes de séparation permettent de répondre aux exigences de sécurité sous la

forme de remplacement des paramètres de conception. La mise en œuvre de ces outils de TRIZ permet d'arriver à un ensemble de solutions.

5.3.3.4. Identification des risques pour l'ensemble des solutions candidates

Un ensemble de solutions ayant été identifié, il convient ensuite d'identifier la meilleure solution possible. Pour cela, la phase d'identification et de ventilation des risques selon les trois phases de la conception (voir chapitre 3) doit être mise en œuvre.

5.3.3.5. Calcul de l'indicateur de sécurité pour l'ensemble des solutions candidates

Un ensemble de solutions ayant été identifié, il convient ensuite d'identifier la meilleure solution possible. Pour cela, la phase d'identification et de ventilation des risques selon les trois phases de la conception (voir chapitre 3) doit être mise en œuvre.

5.3.3.6. Choix d'une solution

A cette étape, le concepteur doit faire le choix de la solution à adopter. Il faut noter que la démarche proposée se focalise sur l'évaluation de solutions du seul point de vue de la sécurité. En réalité, bien d'autres facteurs entrent en ligne de compte. Mais considérer d'autres facteurs sort de notre cadre de recherche. Par la suite, nous considérons donc que le concepteur choisit la solution la plus sécuritaire. Il opte donc pour la solution ayant la valeur de l'indicateur de sécurité la plus élevée. La question à se poser est alors : *la valeur de l'indicateur de sécurité de la solution candidate privilégiée est-elle supérieure à la valeur de l'indicateur de sécurité du système initial ?*

- Si la réponse est négative, il convient alors de choisir l'objectif de sécurité suivant (cf. la liste définie au §5.2.4.1) et de renouveler la démarche (définition des exigences fonctionnelles, des solutions candidates, … jusqu'au choix d'une nouvelle solution).
- Si la réponse est positive, le processus de conception peut se poursuivre.

Cette démarche est représentée à la figure 5.10 ci-dessous dans le cas d'un risque de type C2 et pour lequel le premier objectif de sécurité n'a pas été satisfait. La solution dont la valeur de l'indicateur de sécurité était la plus élevé n'a pas été choisie. L'objectif de sécurité suivant a été sélectionné et une solution liée à cet objectif a été sélectionnée, la valeur de son indicateur de sécurité étant plus élevée que celle du système initial.

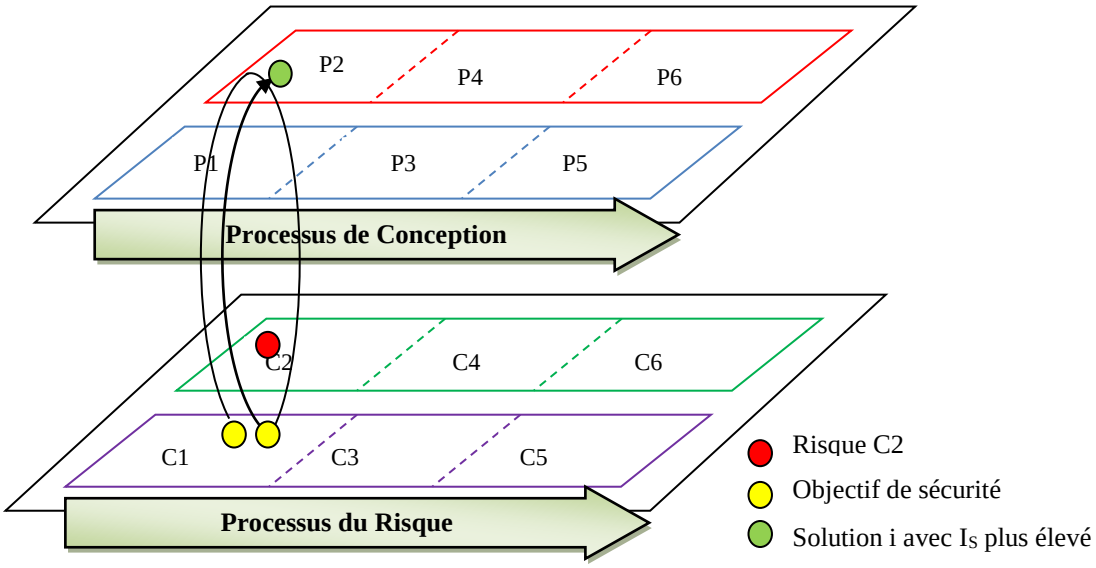


Figure 5.10. Choix d'une solution sécuritaire vis-à-vis d'un risque de type C2.

5.3.3.7. Poursuite du processus de conception

La nouvelle solution choisie, il convient d'en assurer la sécurité jusqu'à la fin du processus de conception. A cette fin, la démarche initiée par le choix d'un objectif de sécurité et allant jusqu'au choix d'une solution doit être reproduite aux phases de conception restantes (architecturale et détaillée pour un risque initial de type C2 et détaillée pour un risque initial de type C4). S'il reste toujours des problèmes de sécurité non solutionnés suite à cette démarche, ces derniers doivent être traduits sous la forme de recommandations. Ces recommandations, destinées aux opérateurs, ont pour objectif de les guider pour un bon usage du système. Elles sont formulées sous la forme de phrases commençant par Faire, Mettre, Éloigner, Faire attention à, Aviser, … Ces informations seront précisées sur la machine (panneaux d'avertissement, étiquettes pour l'utilisation en toute sécurité, signaux sonores et visuels, etc.) et rédigées dans un document fourni avec la machine (manuel d'instruction, données techniques). Ces différentes itérations sont schématisées à la figure 5.11 ci-dessous.

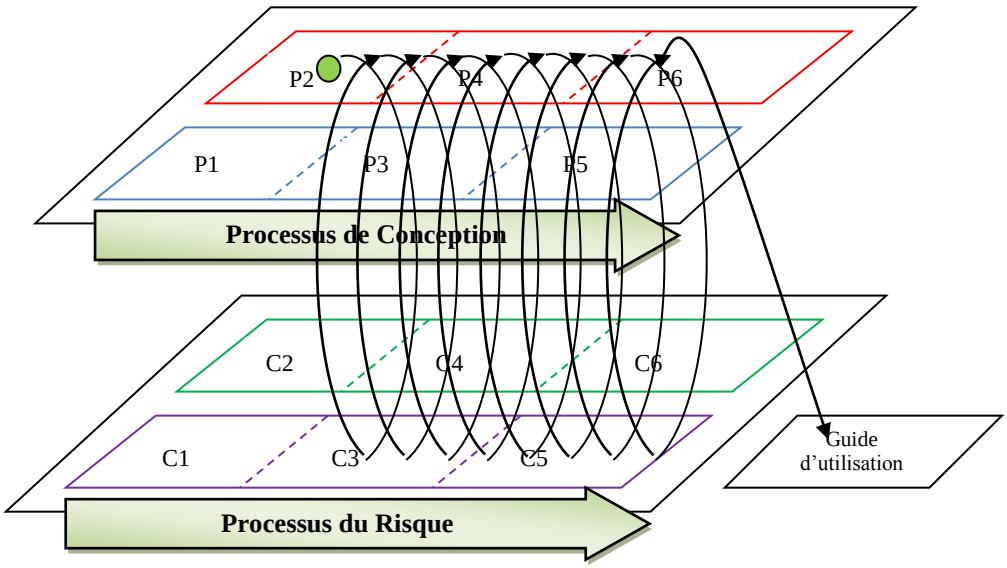


Figure 5.11. Itérations dans processus de conception.

5.3.3.9. Synthèse sur la démarche de reconception sécuritaire proposée

Dans cette section nous avons développé une approche de reconception d'un système ou d'une partie d'un système de façon sécuritaire à partir des objectifs de sécurité définis. Cette approche est essentiellement basée sur la théorie de la conception axiomatique et de TRIZ. Elle utilise un indicateur de sécurité pour l'aide à la décision. La figure 5.12 détaille les différentes étapes de cette approche. Elle se décompose en 5 étapes :

1. **Choix d'un objectif de sécurité :** Cette étape a pour rôle de choisir un objectif de sécurité pour éliminer ou réduire un risque identifié. Ce dernier a pu être défini suite à l'application de l'approche d'ingénierie inverse fonctionnelle proposée (démarche FRES).
2. **Définition des exigences fonctionnelles :** Cette étape permet de définir les nouvelles exigences fonctionnelles intégrant l'objectif de sécurité choisi.
3. **Définition des solutions candidates :** Dans cette étape, les solutions de conception répondant aux objectifs de sécurité sont définies. TRIZ est une des méthodes permettant d'y parvenir.
4. **Identification des risques pour l'ensemble des solutions candidates :** Cette étape a pour rôle d'identifier les risques liés à chacune des nouvelles solutions ;

5. **Calcul de l'indicateur de sécurité pour l'ensemble des solutions candidates :** Dans cette étape, l'indicateur de sécurité est calculé pour chaque solution candidate.
6. **Choix d'une solution :** Parmi l'ensemble des solutions, la solution pour laquelle la valeur de l'indicateur de sécurité est la plus élevée est choisie.
7. **Itérations suivantes du processus de conception :** Suite à ces 5 étapes, une solution plus sécuritaire que la solution initiale est choisie. Même si les risques liés à cette nouvelle solution sont moins importants, il convient d'en minimiser l'impact. Pour y parvenir, nous proposons de mettre en œuvre une démarche très proche de celle présentée juste avant. Elle est schématisée à la figure 5.13.

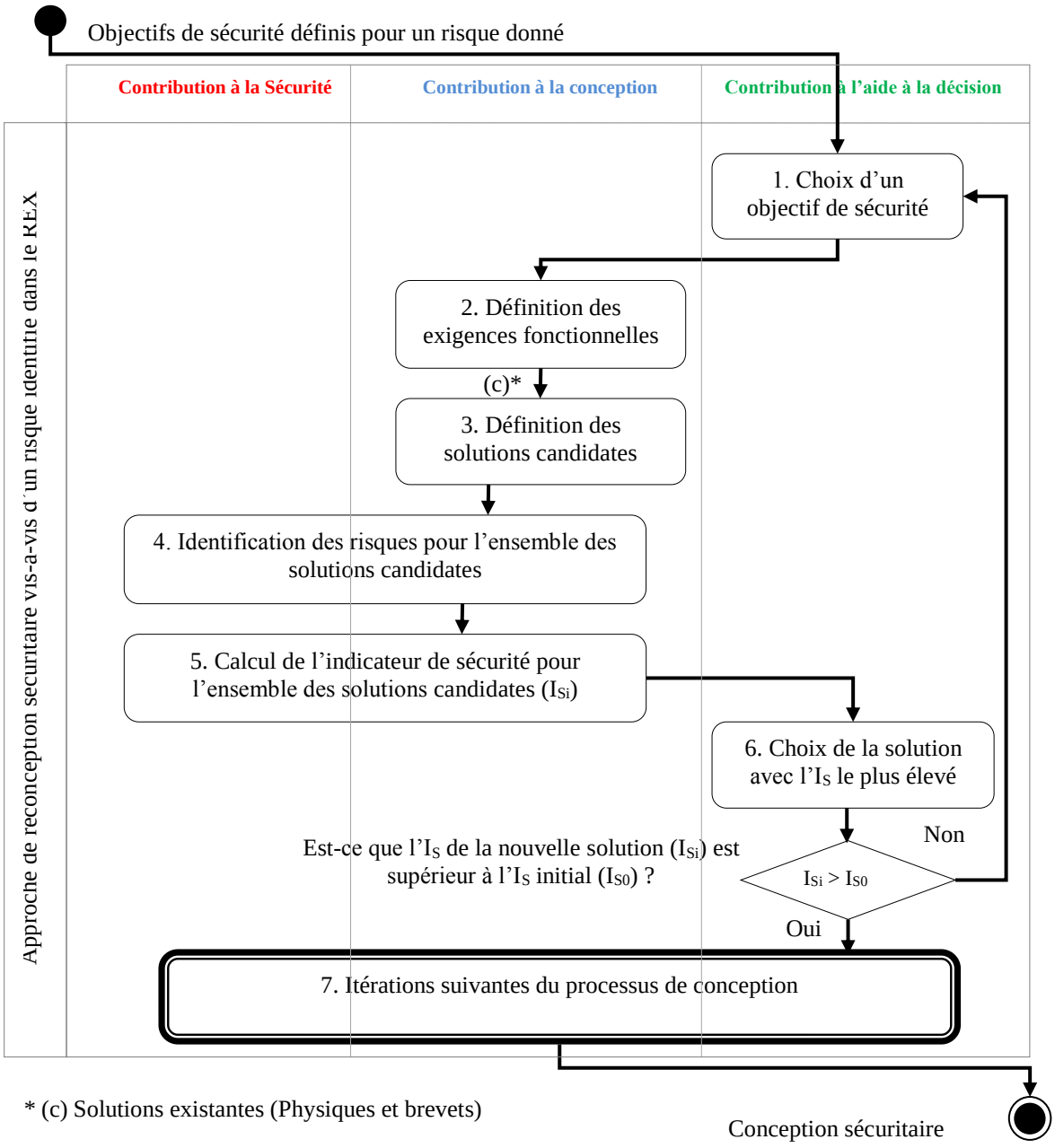


Figure 5.12. Approche de reconception sécuritaire vis-à-vis d'un risque identifié dans le REX.

Les risques, les types de risque et l'indicateur de sécurité liés à la nouvelle solution sont connus puisque identifiés et calculés aux étapes 4 et 5 de l'approche de conception sécuritaire. Les types de risques identifiés permettent de définir les objectifs de sécurité liés à

cette solution (étape 7.1). Les objectifs de sécurité identifiés, les exigences fonctionnelles du niveau inférieur (étape 7.2) puis les solutions candidates répondant à ces exigences (étape 7.3) peuvent être définies. Après avoir identifiés les risques liés à ces solutions (étape 7.4), ces dernières sont évaluées d'un point de vue sécurité par le calcul de leur indicateur de sécurité (étape 7.5). La solution dont la valeur de l'indicateur de sécurité est la plus élevés est sélectionnée (7.6). Ces étapes (étapes 7.1 à 7.6) sont répétées jusqu'à que l'on soit à la fin du processus de conception. Les risques résiduels sont alors traduits en recommandations.

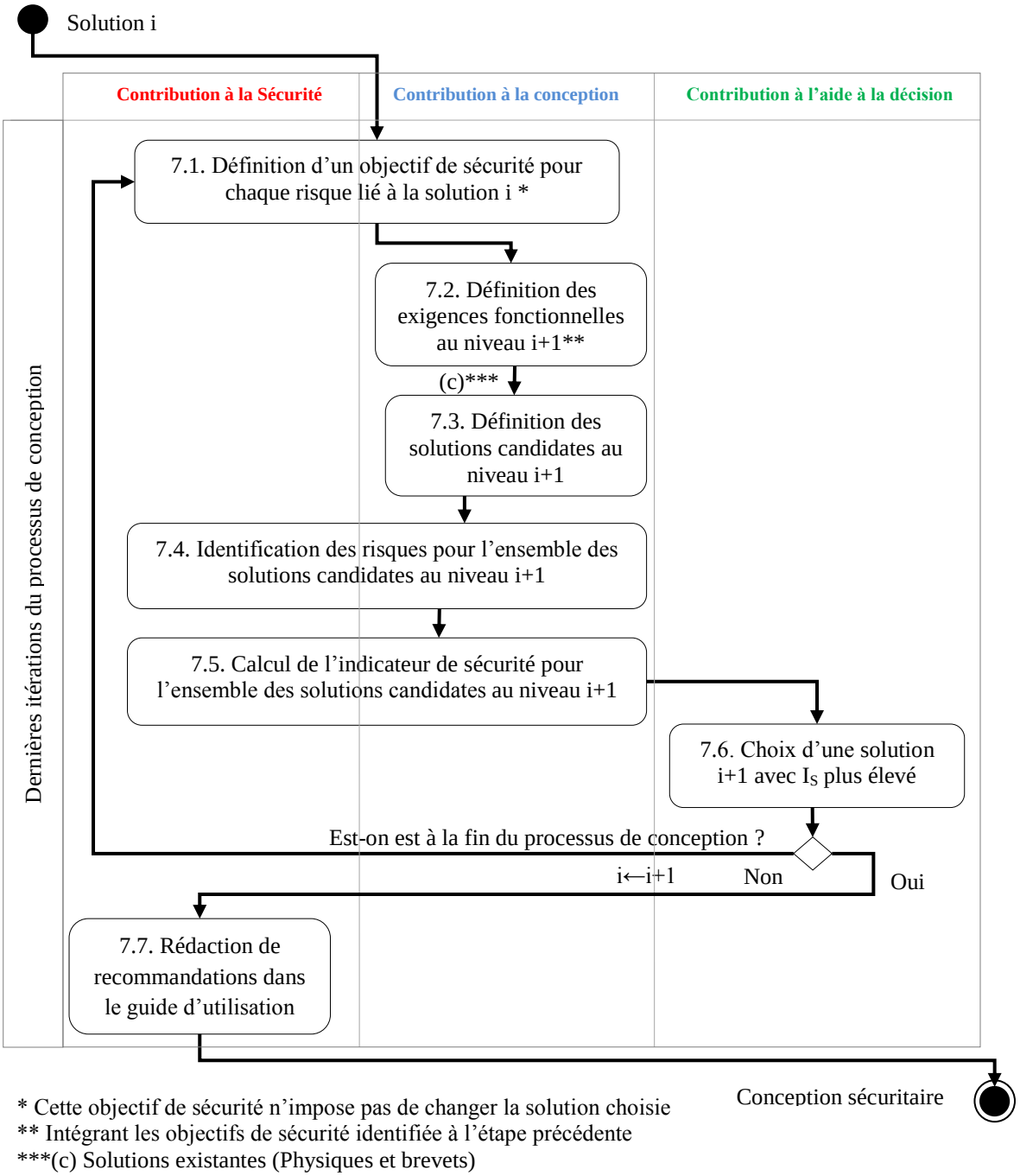


Figure 5.13. Dernières itérations du processus de conception.

Dans la section suivante, nous appliquons cette approche à l'Arbre de Transmission à Cardans (ATC).

5.3.4. Application : reconception sécuritaire de l'arbre de transmission à cardans

5.3.4.1. Choix de l'objectif de sécurité

La définition des objectifs ayant été réalisée (§5.2.4.1), il convient ici au concepteur de choisir l'objectif de sécurité dont dépendra la suite de la reconception. Pour cela, la démarche décrite au §5.3.3.1 est mise en œuvre.

Nous prenons ici comme hypothèse de travail que le concepteur ne souhaite pas modifier la conception de l'ATC et impose de conserver le concept du moyen de protection (présence d'un protecteur). Il s'agit de l'une des hypothèses plausibles permettant au concepteur d'améliorer la sécurité du système à moindre frais et répondant aux conclusions des rapports d'accidents analysées concernant l'ATC (le happement de l'opérateur a lieu lorsque le protecteur est endommagé, c'est-à-dire lorsque au moins un des deux bols est cassé).

Le concepteur répond donc négativement aux 6 premières questions (Est-ce que l'on veut/peut éliminer le phénomène dangereux par conception en changeant le concept du système ? jusqu'à Est-ce que l'on veut/peut éliminer l'événement dangereux en évitant le dommage par la mise en place d'un dispositif de protection ?) et positivement à la 7ème question (Est-ce que l'on veut/peut réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place d'un dispositif de protection). L'objectif de sécurité formulé sera donc lié à la phase de la conception architecturale.

La traduction de cet objectif de sécurité à l'ATC peut être : « réduire les possibilités de contact de l'opérateur avec l'arbre mobile en cas de manque ou d'endommagement du protecteur » ou encore « améliorer la fiabilité du protecteur ».

Nous faisons ici l'hypothèse que le concepteur choisit d'améliorer la fiabilité du protecteur. L'objectif de sécurité est donc d'améliorer la fiabilité du protecteur et plus précisément des bols de protection.

5.3.4.2. Définition des exigences fonctionnelles

L'objectif de sécurité d'améliorer la fiabilité du protecteur peut se traduire en l'exigence fonctionnelle suivante : « Maximiser la résistance des bols ».

5.3.4.3. Définition des solutions candidates

Pour trouver une solution candidate à l'exigence fonctionnelle définie, nous mettons en œuvre la théorie de résolution des problèmes inventifs TRIZ.

1. Identification du paramètre à préserver et du paramètre à améliorer

La préservation de la résistance de l'ATC sans dégradation de son protecteur est une contradiction technique. Les deux paramètres choisis pour traiter cette contradiction sont :

- **Le paramètre à préserver :** perte de substance ;
- **Le paramètre à améliorer :** résistance.

2. Résolution de la contradiction

Connaissant ces deux paramètres, il suffit de sélectionner dans la matrice des contradictions (figure 5.14) la colonne où figure le paramètre à préserver (la perte de substance) (colonne 23) et la ligne correspondant au paramètre à améliorer (la force - résistance) (ligne 14). La case, intersection de la colonne 23 et de la ligne 14, contient les références des principes d'innovation conseillés.

Paramètre à améliorer \ Paramètre à ne pas dégrader		1 Poids d'un objet mobile	2 Poids d'un objet fixe	3 Longueur d'un objet mobile	... ...	28 Perte de matière - substance	... ...	39 Productivité
1	Poids d'un objet mobile		-	15, 8, 29,34	…	5, 35, 3, 31	…	35, 3, 24, 37
2	Poids d'un objet fixe	-		-	…	5, 8, 13, 30	…	1, 28, 15, 35
3	Longueur d'un objet mobile	8, 15, 29, 34	-		…	4, 29, 23, 10	…	14, 4, 28, 29
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
14	Force-Résistance	1, 8, 40, 15	40, 26, 27, 1	1, 15, 8, 35	…	35,28, 31,40	…	23, 35, 40, 3
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
38	Degré d'automation	28, 26, 18, 35	28, 26, 35, 10	14, 13, 17, 28	…	35, 10, 18, 5	…	5, 12, 35, 26
39	Productivité	35, 26, 24, 37	28, 27, 15, 3	18, 4, 28, 38	…	28, 10, 35, 23	…	

Figure 5.14. La matrice des contradictions pour la préservation de la stabilité de l'arbre de transmission à cardans sans dégradation.

Les principes d'innovation conseillés sont : 28 - Reconception, 31 - Porosité du matériau, 35 - Modification (de la valeur, des propriétés) d'un paramètre et 40 - Matériau ou structure composite**.**

3. Choix des principes appropriés

L'analyse des causes des défaillances des différents composants du protecteur montre que le frottement avec des éléments extérieurs au système peut être la cause de la dégradation de la bague. Elle identifie également que la conception trop fragile des bols de protection peut être la cause de sa dégradation. Pour ces raisons, nous choisissons deux des quatre principes d'innovation proposés par TRIZ: la « Reconception » pour diminuer les frottements et la « Modification (de la valeur, des propriétés) d'un paramètre » pour diminuer la fragilité du bol de protection.

Le principe « Reconception » propose de changer le concept de protection ou de modifier la forme des surfaces de contact entre de bol de protection et l'arbre. Le principe « Modification (de la valeur, des propriétés) d'un paramètre » propose de changer le matériau des bols.

4. Proposition de solutions

La partie suivante est consacrée à détailler chaque principe d'innovation et à proposer des solutions techniques afin d'éliminer les causes de défaillances du protecteur.

4.a. Mise en œuvre du principe « Reconception »

Ce principe permet de remplacer les surfaces planes par des surfaces sphériques. A partir de ce principe et afin de stabiliser le protecteur, nous proposons d'intégrer, au niveau de la bague faisant le contact entre le protecteur et l'ATC, soit un roulement à billes ou à

rouleaux, soit des roulettes. Les bagues actuelles sont composées de surfaces Cylindriques (figure 5.15). Celles-ci entraînent un frottement important entre la bague et les embouts de l'ATC dû à la rotation de l'ATC. Les pièces qui sont souvent endommagées sont : la bague, les bols de protections des joints à cardans et les chainettes anti rotation du protecteur.

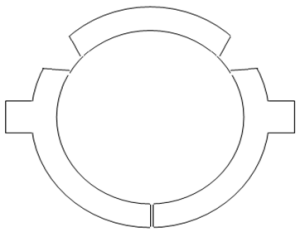
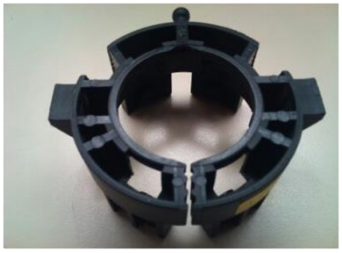


Schéma simplifiée de la bague



La bague réelle

Figure 5.15. Bague établissant le contact entre le protecteur et l'ATC.

Trouver une solution pour diminuer les frottements s'avère une étape nécessaire et judicieuse pour prolonger la durée de vie de ces pièces et éviter de les détériorer. La figure 5.16 montre la bague modifiée [Benziane, 2013].

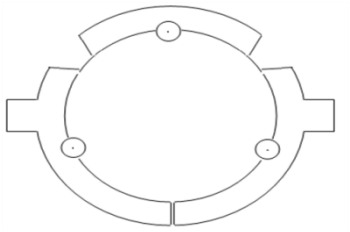


Schéma simplifié de la bague modifiée

Exemple de roulette à ajouter

Figure 5.16. Bague à roulettes avec embout.

L'idée est d'intégrer des roulettes au niveau de l'anneau intérieur de la bague. Ces derniers faciliteront la rotation de la bague autour des embouts. D'autre part la torsion du tube flexible sera moins importante car le couple de torsion sera plus faible. Ainsi, les bols de protection des joints à cardans seront davantage protégés. La force d'entrainement au démarrage de l'ATC sera également moins importante, entrainant des efforts plus faibles au niveau de l'anneau de fixation de la chaînette évitant ainsi sa rupture. La figure 5.17 montre le prototype de la bague à roulettes avec l'embout.

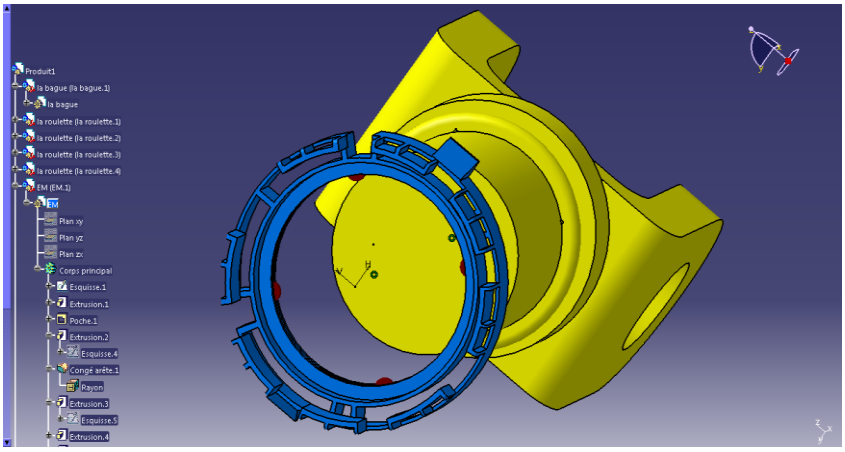


Figure 5.17. Prototype de la bague à roulettes avec embout [Benziane, 2013].

4.b. Mise en œuvre du principe « Modification (de la valeur, des propriétés) d'un paramètre »

Dans le cas de notre système, nous proposons de remplacer le bol de protection du joint de cardans actuel par un bol flexible. Le protecteur pourra ainsi se déformer sous les effets des efforts de traction et de compression sans se dégrader.

Dans le cadre d'un stage effectué à l'Irstea [Benziane, 2013], la méthode d'Ashby a été mise en œuvre afin de choisir les matériaux pouvant s'adapter aux conditions agressives rencontrées. Après comparaison entre les propriétés des matériaux proposés, le choix s'est porté sur un caoutchouc naturel du fait de ses propriétés mécaniques particulièrement adaptées aux milieux soumis à un phénomène d'usure provoqué par des frottements, par l'abrasion et par une exposition continue à des chocs. Effectivement, les propriétés du caoutchouc naturel sont d'excellentes propriétés physiques, notamment élastique, des capacités d'amortissement et d'anti-vibration, des propriétés d'étanchéité à l'eau, à l'air, au gaz et aux bruits. De plus, il s'agit d'un matériau recyclable.

5.3.4.4. Identifier le risque pour toutes solutions possibles

Dans le cas de l'ATC, la source du phénomène dangereux, l'élément en rotation, a été liée au système ATC sans son moyen de protection. Dans cette phase de reconception, nous avons choisi d'améliorer la conception du protecteur. La source du phénomène dangereux ne change donc pas. Nous sommes donc en présence d'un risque de type C2.

5.3.4.5. Calcul de l'indicateur de sécurité pour l'ensemble des solutions candidates

Nous avons proposé d'améliorer la conception du protecteur de l'ATC. La partie de la formule de l'indicateur de sécurité concernant le système sans protecteur reste donc inchangée :

$$I_{Ss} = \frac{\mu_1 I_{Sssmp} + \mu_2 \left(\frac{\sum_{z=1}^{n} I_{Smp\ z}}{n}\right)}{\mu_1 + \mu_2} = \frac{\mu_1 I_{S\ ATC\ smp} + \mu_2 (\sum_{z=1}^{n} I_{Smp\ d'ATC/1})}{\mu_1 + \mu_2}$$

Les modifications apportées au protecteur de l'ATC entrainent uniquement une modification de la valeur de son niveau de fiabilité N_f.

- Le roulement diminue le frottement entre la bague et l'embout. La durée de vie du protecteur va donc augmentée. Par conséquent, la valeur de N_f sera plus grande que celle de la solution initiale. La valeur de l'I_S de la nouvelle solution sera supérieure à celle de la solution initiale.
- Le nouveau matériau proposé a également pour objectif de prolonger la durée de vie du protecteur. La valeur de N_f va donc être plus élevée et la valeur de l'I_S de la nouvelle solution sera, là aussi, supérieure à celle de la solution initiale.

Nous ne détaillons pas davantage la suite de la mise en œuvre de l'approche, le but de notre travail n'étant pas d'aller jusqu'à fin de conception.

5.3.4.6. Conclusion sur l'application

Dans le cas de l'ATC, nous avons mis en évidence que les risques sont relatifs au système ATC sans moyen de protection. Nous avons proposé d'améliorer la conception du **bol de protection** de l'ATC. Pour cela, et en nous basant sur la théorie TRIZ, nous avons proposé une première solution permettant de diminuer le frottement entre la bague et l'embout et une seconde modifiant le matériau des bols de protection. Ces deux solutions permettent d'augmenter le niveau de fiabilité du système et donc d'augmenter la valeur de

l'indicateur de sécurité. L'une des perspectives ici est d'améliorer la conception du tube et de la chainette de l'ATC.

5.3.5. Conclusion

Après avoir défini les objectifs de sécurité pour un risque donné, il faut choisir un objectif parmi ceux-ci et le prendre en compte dans le processus de conception. Pour cela, nous avons proposé une approche de reconception sécuritaire. Dans la première étape, nous identifions l'objectif de sécurité à prendre en considération. Cet objectif de sécurité est ensuite traduit en une ou plusieurs exigences fonctionnelles. Ensuite, et afin d'aider le concepteur à trouver de(s) solution(s), nous proposons d'utiliser une méthode de génération d'idées telle TRIZ afin de trouver des solutions. L'indicateur de sécurité est alors calculé pour chaque solution candidate dans l'objectif de choisir la solution plus sécuritaire. Cette solution est normalement plus sécuritaire que la solution initiale. La valeur de son indicateur de sécurité doit le confirmer. Dans le cas contraire, le concepteur doit choisir l'objectif de sécurité suivant et renouveler la démarche jusqu'au choix d'une nouvelle solution sécuritaire.

5.4. Conclusion

Dans le cadre de l'opérationnalisation de la méthode IRAD, nous avons présenté dans ce chapitre une approche de réingénierie fonctionnelle pour la sécurité baptisée FR2ES. Elle se décompose en deux sous parties : une approche pour la définition et la priorisation des objectifs de sécurité pour un risque donné et une approche de reconception basée sur les objectifs de sécurité définis.

L'approche pour la définition et la priorisation des objectifs de sécurité pour un risque donné est basée sur la confrontation des étapes de la phase d'appréciation des risques ainsi que celles de la phase de réduction des risques de la norme [NF EN ISO 12100, 2010] et des six contextes du processus des risques de la méthode IRAD. Cette approche permet d'ordonner et d'identifier à quels stades du processus de conception les indications de la norme peuvent s'avérer pertinentes. Nous avons appliqué la première approche à l'arbre de transmission à cardans (ATC). Le risque lié à l'ATC étant un risque de type conceptuel (C2), neuf objectifs de sécurité y sont proposés.

L'approche de reconception pour la sécurité permet de choisir un objectif de sécurité parmi plusieurs et de reconcevoir à partir de l'objectif de sécurité choisi. Nous y proposons d'utiliser la théorie TRIZ afin d'aider le concepteur à trouver des solutions. Enfin, nous avons mis en œuvre la seconde approche. Elle a permis de définir deux nouvelles solutions augmentant le niveau de fiabilité du moyen de protection de l'ATC et donc le niveau de sécurité de celui-ci.

Le chapitre suivant a pour objectif de synthétiser les deux approches de FRES et FR2ES proposée dans les chapitres 3, 4 et 5. Nous les appliquerons ensuite sur un cas d'étude déjà étudié et présenté dans [Ghemraoui, 2009] : la Liaison Trois Points (LTP).

Chapitre 6. Structuration d'une approche de conception sécuritaire

6.1. Introduction

Dans le premier chapitre, il a été précisé que l'objectif de ce travail porte sur deux développements complémentaires : une approche basée sur l'ingénierie inverse fonctionnelle pour la sécurité (ou FRES pour Functional Reverse engineering for Safety) et une seconde sur la réingénierie fonctionnelle pour la sécurité (ou FR2ES pour Functional REEngineering for Safety).

La démarche FRES est basée sur l'analyse du Retour d'Expérience (REX) et plus précisément sur l'analyse des rapports d'accident. Nous avons proposé dans le second chapitre une approche de formalisation des rapports d'accidents. Ensuite, nous avons développé les deux approches dans les chapitres 3, 4 et 5. Dans ces chapitres sont résolus certains problèmes ou manques de la méthode IRAD. Dans ce dernier chapitre, nous synthétisons ces deux développements. En effet, en s'appuyant sur la synthèse des cinq chapitres précédents, nous développons une approche globale de conception sécuritaire. L'intérêt de cette approche peut être vu selon trois points de vue :

- Point de vue **sécurité**, cette approche permet :
  - d'extraire et de formaliser les connaissances sur les accidents en analysant des rapports formel d'accident ;
  - d'identifier les risques ;
  - d'évaluer le niveau de sécurité de la partie du système impliquée dans l'accident ;
  - de définir les objectifs de sécurité pour l'amélioration de la sécurité du système.
- Point de vue **conception**, cette approche permet :
  - d'extraire des connaissances sur la conception à partir de l'analyse d'un rapport formel d'accident ;
  - de traduire les caractéristiques et les aspects techniques du système au niveau de la sécurité. Cette évaluation permet l'identification des paramètres techniques à optimiser pour obtenir un système plus sécuritaire;
  - de concevoir un système au niveau de sécurité optimal en s'appuyant sur l'atteinte des objectifs de sécurité.
- Point de vue **aide à la décision**, cette approche permet :
  - de déterminer l'étape de la conception où a été fait le choix de la solution cause d'un accident ;
  - de fournir un indicateur qui aide le concepteur à identifier et à choisir les solutions les plus sécuritaires parmi les différentes alternatives de solutions possibles durant le processus de conception.

Ce chapitre comporte trois sections principales. La section 6.2 détaille la démarche de conception sécuritaire proposée. Pour évaluer l'efficacité de notre approche, nous l'appliquons dans la section 6.3 sur un cas déjà étudié et présenté dans [Ghemraoui, 2009] : la Liaison Trois Points (LTP). Enfin, nous clôturons ce chapitre par une conclusion et les perspectives des travaux à la section 6.4.

6.2. Démarche de conception sécuritaire proposée

Nous avons intégré l'ensemble des démarches développées dans ce mémoire dans une approche de conception sécuritaire. Le diagramme présenté ci-dessous (figure 6.1) détaille cette approche. Il est constitué de trois colonnes pour indiquer la contribution de chaque étape des points de vue conception, sécurité et aide à la décision. Il est également composé de trois lignes permettant de distinguer la démarche FRES, l'évaluation pour la sécurité et la démarche FR2ES. L'approche se décompose en 6 sous-processus (non représentés sur le diagramme mais utilisés dans la suite pour décrire l'approche). Elle est mise en œuvre à partir d'un problème de sécurité et peut être appliquée par un concepteur ou un expert en sécurité, suivant l'objectif attendu. Les trois sorties de la démarche sont :

a Des connaissances sur la conception du système et sur l'accident lié à ce système ;

b Le type de risque et la mesure du niveau de sécurité du système ;

c Des objectifs de sécurité ou des pistes possibles afin d'éliminer ou de réduire le risque ;

d Des détails de conception nécessaires à la fabrication d'un nouveau système plus sécuritaire.

Les documents utilisés au cours de l'approche sont :

(a) Le REX (structure type de rapport d'accidents complétée)

(b) Les documents techniques, les normes, …

(c) Les solutions existantes (physiques et brevets)

De manière très succincte, ces sous-processus de conception sécuritaire traitent les questions suivantes :

- *Comment extraire des connaissances sur un accident ?*
- *Comment extraire des connaissances sur la conception d'un système ?*
- *Comment ventiler les risques selon les phases du processus de conception ?*
- *Comment mesurer le niveau de sécurité d'un système ?*
- *Comment transcrire de manière formelle et systématique les risques en exigences de sécurité ?*
- *Comment intégrer ces exigences de sécurité dans le processus de conception ?*

De façon plus détaillée, l'approche proposée de conception sécuritaire se décompose en 19 étapes. Dans les six sections suivantes (correspondant au 6 sous-processus), nous expliquons l'intérêt de chacune d'elles.

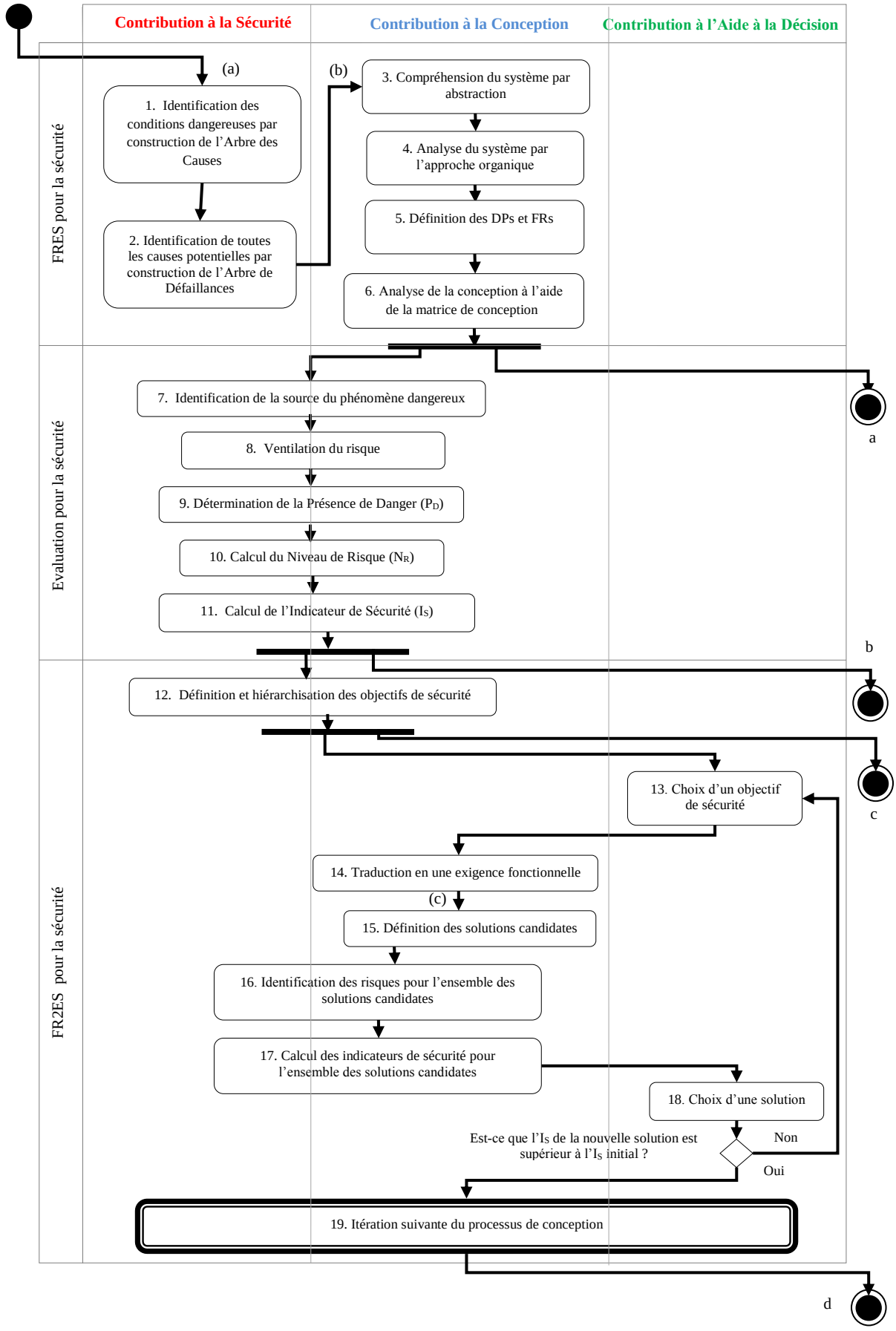


Figure 6.1. Approche de conception sécuritaire proposée.

6.2.1. Extraction des connaissances sur l'accident

Le point de départ de la démarche est un problème de sécurité sur un système rapporté dans un(ou plusieurs) rapport(s) d'accident, le but étant de définir, comprendre et décrire les causes de ce problème de sécurité. Les données d'entrée se trouvent dans trois des parties d'un rapport type d'accident complété :

- La partie Dommage qui précise la partie du corps touchée et décrit la blessure ;
- La partie Type d'accident qui précise à quel type d'accidents appartient l'accident en question. Un type d'accident regroupe les accidents ayant les mêmes conséquences et les mêmes sources du phénomène dangereux et qui sont causés par le même type de système ou sous-système.
- La partie Conditions de l'accident qui décrit les conditions de fonctionnement du système, le comportement et les capacités de l'opérateur et les conditions environnementales.

Ce 1er sous-processus est composé de deux étapes décrites ci-dessous :

Etape 1. Identification des conditions **dangereuses de l'accident :** Les conditions dangereuses (le phénomène dangereux, la situation dangereuse et l'événement dangereux) sont déterminées suite à la construction et l'analyse de l'Arbre des Causes (AdC).

Etape 2. Identification de toutes les causes potentielles de l'accident : L'ensemble des causes potentielles de l'accident est défini ici. Ceci est possible en se basant sur la réalisation d'un Arbre de Défaillance (AdD). Sa construction est basée sur les AdCs décrivant les causes des évènements non désirés réels identifiées à l'étape 1 ainsi que les autres causes potentielles identifiables à partir de documents techniques (défaillance du système, facteur non prévu lié à l'humain ou à l'environnement).

6.2.2. Extraction des connaissances sur la conception du système impliqué dans l'accident

Ce deuxième sous-processus met en œuvre plusieurs types d'analyse afin d'obtenir des connaissances sur la conception du système : une analyse fonctionnelle, une analyse organique et l'analyse axiomatique. Les premières connaissances issues de l'analyse du rapport d'accident et les données issues de documents techniques décrivant le système sont les données d'entrée de ce sous-processus. Il est composé de quatre étapes décrites ci-dessous :

Etape 3. Compréhension du système par abstraction : L'abstraction est un premier niveau de compréhension du fonctionnement du système. Elle initie la réalisation de l'étape suivante.

Etape 4. Analyse du système par l'approche organique : Cette étape se décompose en deux sous-étapes pour analyser le système. La première est la représentation des composants du système et des relations qui les lient par la réalisation du Bloc Diagramme Fonctionnel (BDF) du système. La seconde consiste à décomposer hiérarchiquement le système en utilisant l'Organigramme Technique étendu (OTé).

Etape 5. Définition des DPs et FRs : Cette étape demande de définir les DPs et FRs à partir des résultats de l'étape précédente, c'est-à-dire l'analyse du BDF et de l'OTé réalisés.

Etape 6. Analyse de la conception du système: Cette étape finalise l'analyse de la conception du système. Elle débute par la construction de la matrice de conception et se termine par son analyse d'un point de vue technique.

6.2.3. Identification et ventilation des risques selon les trois phases de conception

Ce 3ème sous-processus permet d'identifier et de ventiler les risques selon les trois phases de la conception grâce à la confrontation des trois contextes C2, C4 et C6 de la méthode IRAD et les travaux normatifs portant sur la classification des sources des phénomènes dangereux. Les données d'entrée sont les conditions dangereuses déterminées à la 1ère étape. Il est composé de deux étapes décrites ci-dessous :

Etape 7. Identification de la source du phénomène dangereux : La lecture des différents niveaux de l'AdC, construit à l'étape 1, permet de déterminer les conditions dangereuses (événement dangereux, situation dangereux et phénomène dangereux). A ce niveau, la source et la conséquence de l'ensemble des phénomènes dangereux sont identifiées.

Etape 8. Ventilation du risque : Le lien entre la source d'un phénomène dangereux et la phase de conception impactée a été défini au chapitre 4 (§4.2.3.2). Ventiler le risque selon les trois phases de conception demande de répondre aux questions suivantes :

- *Est-ce que la source du phénomène dangereux est liée à une énergie ?*
- *Est-ce que la source du phénomène dangereux est liée à des caractéristiques dimensionnelles ou géométriques, à l'ergonomie ou au matériau ?*
- *Est-ce que la source du phénomène dangereux est liée à des caractéristiques de forme ou à des propriétés d'un matériau?*

Une réponse positive à la première question indique que le risque est de type C2 (est donc lié à la phase de conception conceptuelle), une réponse positive à la deuxième question un risque de type C4 (est donc lié à la phase de conception architecturale), et une réponse positive à la troisième question un risque de type C6 (est donc lié à la phase de la conception détaillée).

6.2.4. Evaluation du niveau de sécurité du système

Ce 4ème sous-processus permet de mesurer le niveau de sécurité du système. Il est composé de trois étapes décrites ci-dessous :

Etape 9. Détermination de la Présence de Danger (P_D) : Le P_D, est une valeur binaire. Elle vaut 1 si la solution évaluée comporte un phénomène dangereux, une situation dangereuse et un événement dangereux. Elle permet de décider s'il faut aller plus loin dans le calcul du niveau de risque et si l'indicateur de sécurité aura sa valeur maximale ou non (Si $P_D = 0$ alors Is = 1).

Etape 10. Calcul du Niveau de Risque (N_R) : Le N_R est lié à un dommage. L'évaluation du niveau de risque, N_R, nécessite donc l'évaluation des niveaux de risque liés au phénomène dangereux, à la situation dangereuse et à l'évènement dangereux.

Etape 11. Calcul de l'Indicateur de Sécurité (I_S) : Cette étape permet de calculer l'indicateur de sécurité Is fonction du niveau de risque N_R et de la présence de danger P_D.

$$I_S : \{I_S = 1 - P_D \times N_R$$

6.2.5. Définition et priorisation des objectifs de sécurité

Ce 5ème sous-processus permet d'introduire la bonne exigence de sécurité au moment opportun de la conception. C'est-à-dire que pour un risque donné et donc son type identifié à l'étape 8, il propose de définir et de hiérarchiser les objectifs de sécurité et enfin d'identifier leur niveau d'intervention dans le processus de conception. Il est composé d'une seule étape décrite ci-dessous :

Etape 12. Définition et hiérarchisation des objectifs de sécurité : La confrontation des étapes de la phase d'appréciation des risques ainsi que celles de la phase de réduction des risques de la norme [NF EN ISO 12100, 2010] et des six contextes du processus des risques de la méthode IRAD permet d'ordonner et d'identifier à quels stades du processus de conception les indications de la norme peuvent s'avérer pertinentes. Cette étape consiste à définir les objectifs de sécurité permettant d'éliminer ou a minima de réduire un risque. Un objectif de sécurité s'exprime selon l'une des trois formulations suivantes : maximiser un paramètre de conception, minimiser un paramètre de conception ou remplacer un paramètre de conception.

6.2.6. Reconception sécuritaire

Ce 6ème sous-processus permet dans un premier temps de faire le choix d'un objectif de sécurité et dans un second temps de reconcevoir le système de la façon la plus sécuritaire possible. Il est composé de six étapes décrites ci-dessous suivant le type de risque identifié :

Etape 13. Choix d'un objectif de sécurité : Afin de choisir l'objectif de sécurité le plus judicieux parmi les objectifs de sécurité possibles, il est nécessaire de répondre à certaines des neuf questions ci-dessous:

1. Est-ce que l'on veut/peut « Eliminer le phénomène dangereux » ?
2. Est-ce que l'on veut/peut « Éliminer la situation dangereuse pour la personne »?
3. Est-ce que l'on veut/peut « Réduire la gravité du dommage lié au phénomène dangereux » ?
4. Est-ce que l'on veut/peut « Réduire la fréquence et/ou la durée de l'exposition aux situations dangereuses » ?
5. Est-ce que l'on veut/peut « Réduire la probabilité d'occurrence de l'événement dangereux » ?
6. Est-ce que l'on veut/peut « Eliminer l'événement dangereux en évitant le dommage par la mise en place d'un dispositif de protection » ?
7. Est-ce que l'on veut/peut « Réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place d'un dispositif de protection » ?
8. Est-ce que l'on veut/peut « Réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place de mesures de protection » ?
9. Est-ce que l'on veut/peut « Eviter ou limiter le dommage après la conception » ?

Dans le cas où le risque identifié est de type C2, il convient de répondre à ces 9 questions dans l'ordre de leur numérotation ci-dessus. Si le risque est de type C4, il est nécessaire de répondre aux questions de 1 à 4 puis de 6 à 9 dans cet ordre. Si le risque est de type C6, il faut répondre aux questions 1, 3 et 9 dans cet ordre.

Etape 14. Traduction de l'objectif de sécurité en exigence fonctionnelle : Il convient ici de traduire l'objectif de sécurité choisi sous la forme d'une exigence fonctionnelle.

Etape 15. Définition des solutions: Une démarche de définition de solutions doit être mise en œuvre ici. Elle peut se baser sur des techniques de résolution créative de problème tel que le brainstorming par exemple ou des méthodes plus élaborées comme TRIZ.

Etape 16. Identification des risques pour l'ensemble des solutions candidates : Un ensemble de solutions ayant été identifié, il convient ensuite d'identifier la meilleure solution possible. Pour cela, l'étape 7 doit être mise en œuvre ici.

Etape 17. Calcul de l'indicateur de sécurité pour l'ensemble des solutions candidates : l'objectif de cette étape est d'évaluer les conséquences des choix de conception sur la sécurité. Cette évaluation permettra d'obtenir un classement des solutions en fonction des valeurs de l'indicateur de sécurité. Pour cela, les étapes 9 à 11 doivent être mise en œuvre.

Etape 18. Choix d'une solution : A cette étape, le choix de la solution à adopter doit se faire en se posant la question : *l'I_S de la solution candidature privilégiée est-il supérieur à l'I_S du système initial ?* Si la réponse est non, il est nécessaire de revenir en arrière dans la démarche en choisissant un autre objectif de sécurité. Si la réponse est oui, il convient alors de poursuivre la démarche en se posant la question de savoir si l'on est à la fin du processus de conception c'est-à-dire que les trois phases de conception ont été passées en revue ou non.

Etape 19. Itération suivante du processus de conception. Après avoir choisi une solution, le processus de conception peut se poursuivre. Cette étape a été schématisée dans le chapitre 5, à la figure 5.13.

6.2.7. Conclusion sur la démarche de conception sécuritaire proposée

Notre travail de recherche consiste à rendre la méthode IRAD opérationnelle. Pour y parvenir, nous avons développé deux démarches complémentaires : une démarche d'ingénierie inverse fonctionnelle pour la sécurité (ou FRES pour Functional Reverse Engineering for Safety) et une démarche de réingénierie fonctionnelle pour la sécurité (ou FR2ES pour Functional REEngineering for Safety). La démarche d'évaluation de et pour la sécurité, qui est en réalité une partie de la démarche FRES, a été traité séparément.

La démarche de conception sécuritaire proposée consiste en la mise en œuvre de ces trois démarches (FRES, l'évaluation de et pour la sécurité et FR2ES) dans cet ordre. Cette démarche se compose de 6 sous-processus composé chacun de 1 à 6 étapes. Les démarches FRES et d'évaluation de et pour la sécurité permettent de rendre opérationnel le premier cas d'emploi de la méthode IRAD. Elles correspondent aux sous-processus de 1 à 4. La démarche FR2ES rend opérationnelle les cas d'emploi 2 et 3 de la méthode IRAD. Elle correspond aux sous-processus 5 et 6.

Dans la section suivante, nous allons appliquer cette démarche de conception sécuritaire sur un problème de sécurité lié à la Liaison Trois-points (LTP).

6.3. Application : conception sécuritaire de la liaison trois points (LTP)

6.3.1. Extraction des connaissances sur l'accident impliquant la liaison trois points

Cette section a pour but de décrire l'extraction des connaissances issues de deux rapports d'accidents liés à la LTP. Ces deux rapports ont été présentés dans le chapitre 2, §2.5.2.

Comme détaillé dans le § 2.5.2, nous avons identifié le dommage, le type d'accident et les conditions de l'accident impliquant l'ATC pour un accident. Les résultats sont résumés dans le tableau ci-dessous :

Tableau 6.1. Dommage, type d'accident et conditions de l'accident pour l'accident étudié impliquant la LTP.

	Accident 1
Dommage	*Blessure sans incapacité permanente (Perte de doigts, ...)*
Type d'accident	- Conséquence d'accident: *écrasement* - Source d'accident: *énergie potentielle*
Conditions de l'accident	- Phase d'utilisation de la machine : *Montage, installation, mise en service* - Tâche : *attacher l'outil au tracteur* - État de la machine : *fonctionnement normal* - Comportement de l'opérateur : *l'opérateur utilisait la machine en respectant la procédure et les consignes de sécurités fournies par le constructeur* - Capacités de l'opérateur *:* *L'opérateur avait reçu une formation adéquate pour l'utilisation de la machine,* *il était expérimenté,* *il était sans capacités physiques limitées, ni stressé, ni fatigué et sans préoccupations particulières.* - Présence de *tiers* - Environnement *ouvert* - Milieu *naturel*

Etape 1. Identification des conditions dangereuses de l'accident : Après avoir identifié le dommage, le type de l'accident et extrait les conditions de l'accident impliquant la LTP dans le rapport d'accident, nous avons établi l'AdC pour l'accident (figures 6.2). Ainsi, sur cette figure, nous avons déterminé les conditions dangereuses. Pour cet accident, les AdCs sont établis jusqu'au 4ème niveau.

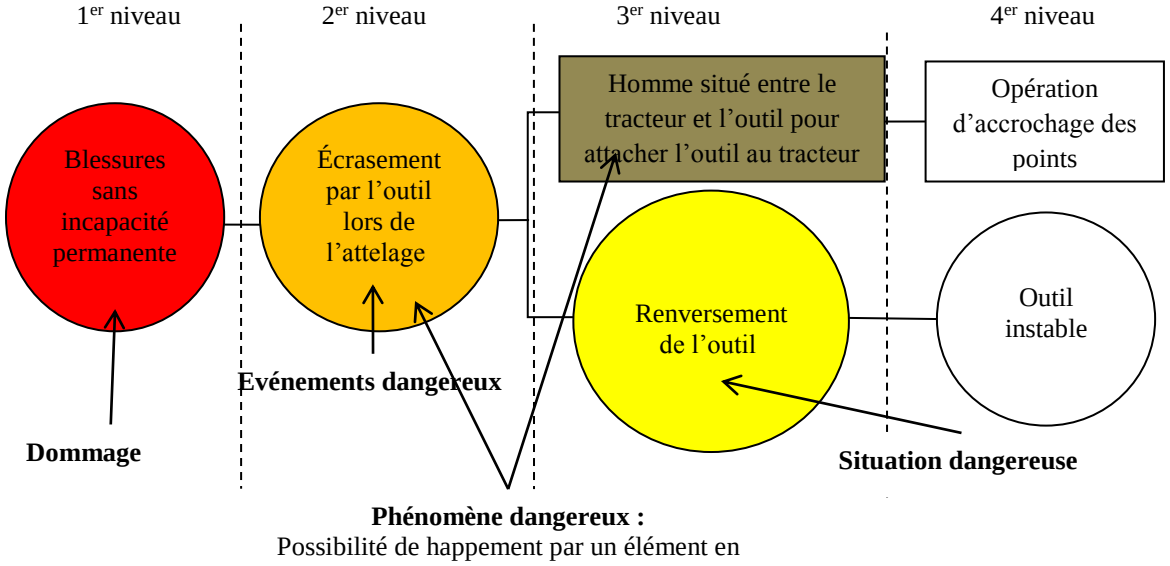


Figure 6.2. Définition des conditions dangereuses de la LTP par l'AdC.

L'analyse du rapport montre que l'accident se traduit par l'écrasement de la victime par l'outil lors de l'attelage de l'outil au tracteur. L'attelage est réalisé lors de la sous-phase de « Montage, installation, mise en service » de la phase d'usage.

Etape 2. Identification de toutes les causes potentielles de l'accident : Afin de construire l'Arbre de Défaillances (AdD), nous passons de l'étude des rapports d'accidents à l'étude d'un type d'accident : « accident par écrasement par l'outil lors de l'attelage».

L'analyse de plusieurs accidents de ce type indique que les faits « Homme situé entre le tracteur et l'outil pour attacher l'outil au tracteur » et « Renversement de l'outil » entraînent l'« écrasement » [Sadeghi et al., 2012a]. Nous remarquons ici que le poids de l'outil a un impact direct sur le type de blessure.

Nous présentons l'AdD avec différents niveaux de détails aux figures 6.3 et 6.4. L'AdD présentant les 3 premiers niveaux est représenté à la figure 6.3. La suite de l'analyse permet de générer d'autres déclencheurs de l'évènement. En effet, l'opérateur, l'outil et l'environnement peuvent entraîner l'accident par écrasement soit indépendamment soit de manière combinée.

La première question à se poser est liée à la source du phénomène dangereux : *Pourquoi l'outil s'est renversé?* Trois raisons sont identifiées : « Outil instable », « Coactivité » et « Erreur d'attelage ». La deuxième question est liée à la situation dangereuse: *Pourquoi l'homme se trouve entre le tracteur et l'outil ?* Les raisons faisant que l'homme se tient entre le tracteur et l'outil sont : « approche de mise en position imprécis » et une « opération d'accrochage des points ».

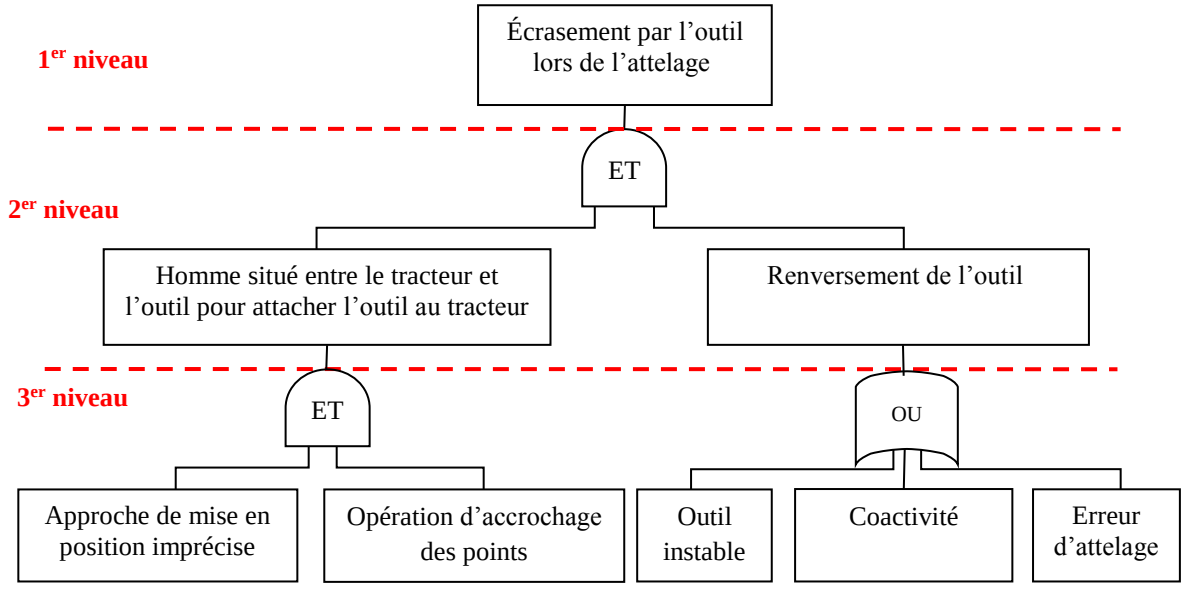


Figure 6.3. Causes de l'écrasement par l'outil.

La figure 6.4 présente les causes possibles d'une approche de mise en position imprécise et montre également que l'opération d'accrochage des points consiste en l'accrochage des bras inférieurs et du troisième point.

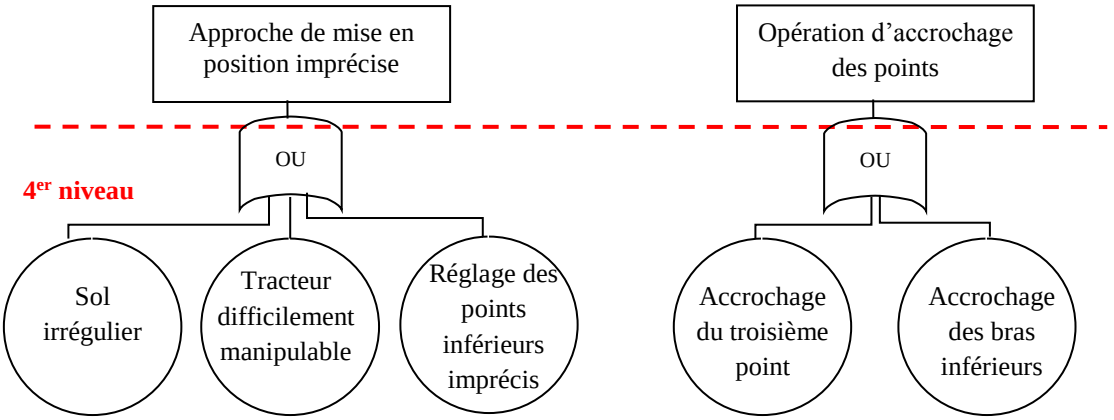


Figure 6.4. Causes entrainant le fait « Homme situé entre le tracteur et l'outil ».

Les causes de « outil instable » peuvent être : pas de béquilles, sol en pente ou mauvaises conditions métrologiques. Les causes « coactivité » et « erreur d'attelage » sont liées à un manque d'expérience ou de formation de l'opérateur. Cette analyse montre qu'éliminer le risque d'écrasement par l'outil peut revenir soit à rendre l'outil stable soit à éliminer la présence de l'opérateur entre l'outil et le tracteur.

6.3.2. Extraction des connaissances sur la conception de la liaison trois points

Etape 3. Compréhension de la LTP par abstraction. La figure 6.5 représente l'abstraction de la LTP. Le tracteur se trouve sur la gauche de la figure et l'outil à droite. Sur cette figure, les cercles rouges montrent les liaisons sphériques et les lignes rouges et violettes représentent les éléments constitutifs de la LTP. Les points d'appui de la LTP avec l'arrière du tracteur correspondent aux points (K, L, M). Lorsque les trois barres sont considérées dissociées du tracteur, les trois points (K, L, M) sont notés, du côté du tracteur (K1, L1, M1) et du côté des barres (K2, L2, M2). Ainsi, les trois barres sont notées (K2-O1, L2-E1, M2-N1). Les trois points (O, E, N) constituent le plan de la liaison trois points avec l'outil. Quand l'outil est décroché du tracteur, nous notons ces trois points, du côté du tracteur (O1, E1, N1) et du côté de l'outil (O2, E2, N2). Les deux barres (G-I) et (H-J) correspondent aux chandelles. Les barres dont la longueur est réglable sont représentées en rouge.

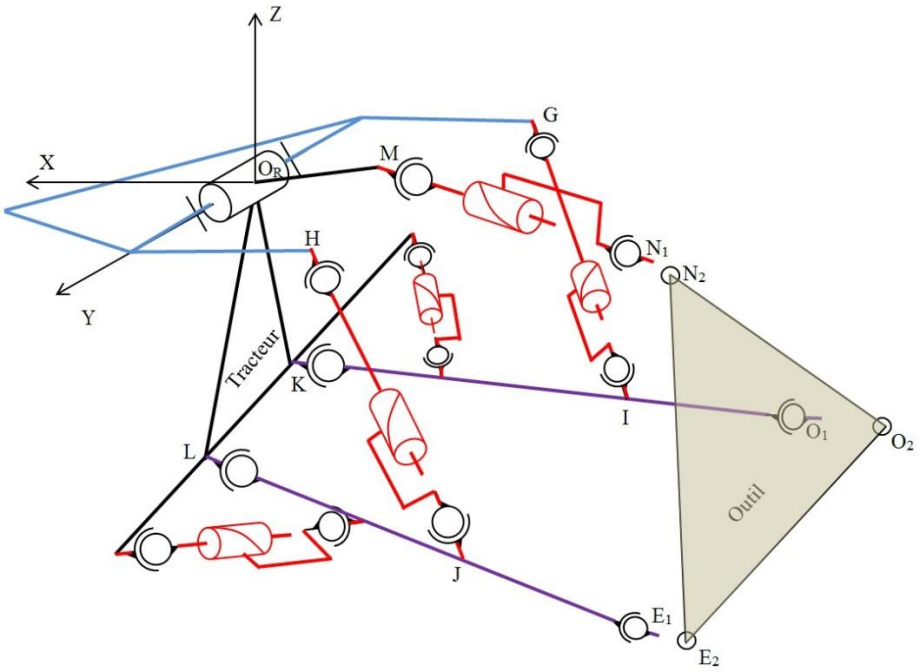


Figure 6.5. Abstraction de la LTP.

Etape 4. Analyse de la LTP par l'approche organique. La LTP est composé de trois unités principales : deux « bras inférieurs » et un « bras supérieur ». Le bras supérieur comporte trois sous-ensembles : « Rotule côté tracteur », «Barre supérieur» et « Rotule côté outil ». Chaque bras inférieurs est composé de quatre ensembles : un « Bras de relevage », une « Barre inférieure », une « Chandelle » et un « stabilisateur latéral ». Ces composants sont montrés à la figure 2.9 du chapitre 2 (§2.4.3).

Le BDF est ensuite construit (figure 6.6). Sur ce diagramme, le flux représenté en bleu correspond à la fonction principale et la ligne en pointillés correspond au contact entre le tracteur et la LTP.

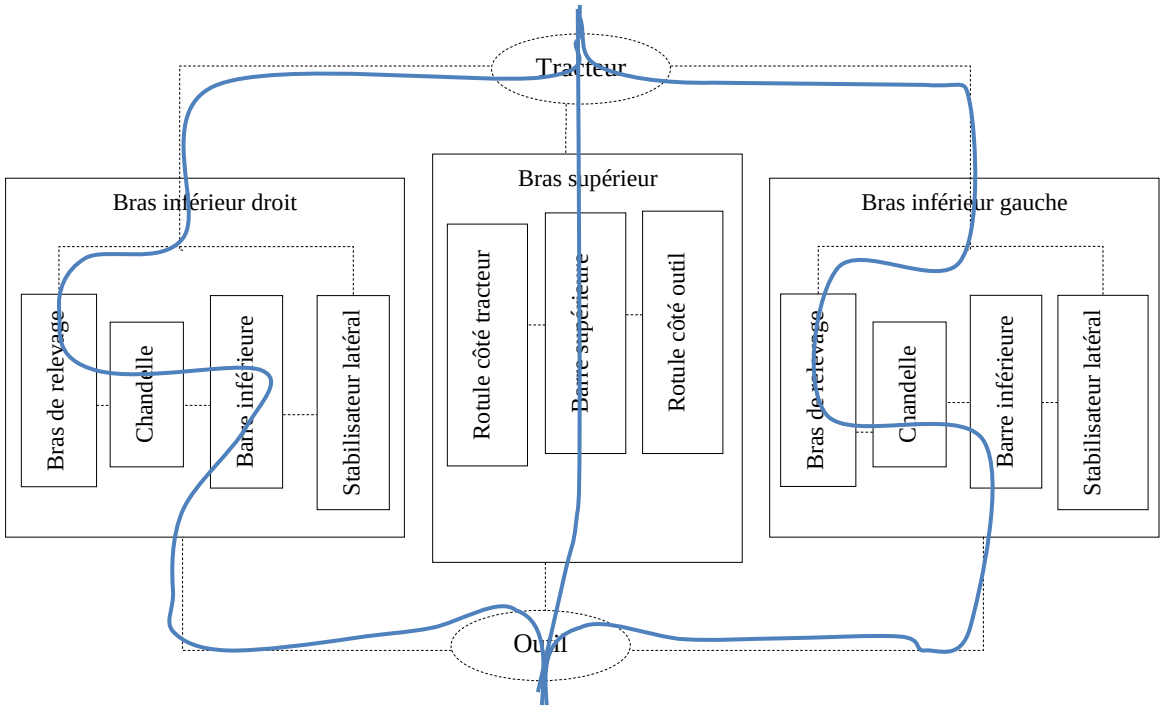


Figure 6.6. Bloc Diagramme Fonctionnel (BDF) du système LTP.

La figure 6.7 montre la décomposition structurelle de la LTP. Nous retrouvons la LTP au niveau 0. Ses trois unités, les deux bras inférieurs et le bras supérieur, apparaissent au niveau 1. Enfin, au niveau 2, sont listés les composants de chaque unité.

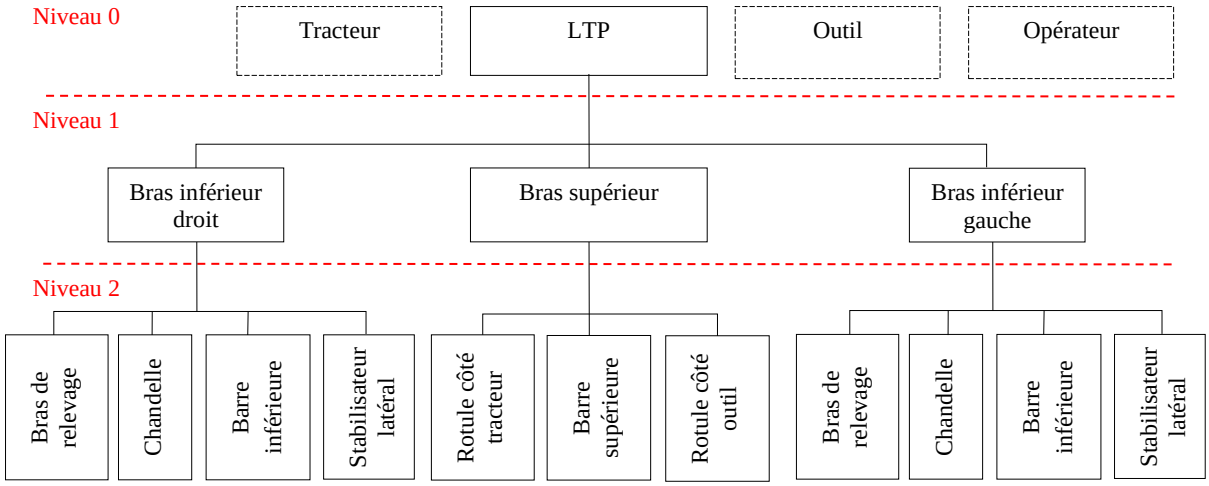


Figure 6.7. Organigramme Technique étendu de la LTP.

Etape 5. Définition des DPs et FRs de la LTP. Pour définir les DPs et FRs liés aux composants de la LTP, nous nous basons sur l'OTé de la LTP (figure 6.7) et sur le guide d'identification des DPs et FRs (§3.3.3.3 - tableau 3.4). La LTP peut être définie comme un « Système trois points» (DP0) composé de « Trois barres » (DP1) et d'un « Ensemble de rotules permettant la rotation selon l'axe Y » (DP2). La fonction principale de la LTP est FR0 « Porter l'outil par le tracteur». Nous décomposons le DP1 en six paramètres de conceptions DP11 à DP16, auxquels nous avons affectés les exigences fonctionnelles FR11 à FR16. Nous n'avons pas détaillé les sous-fonctions liées au DP2 car non liées à l'accident. Nous décomposons les DP11, DP13 et DP15 en trois paramètres de conception.

La figure 6.8 résume les DPs et FRs identifiés jusqu'ici :

0	DP	Système trois points	
1	DP	Trois barres	
1.1	DP	Bras inférieur 1	
1.1.1	DP	-	
1.1.2	DP	Stabilisateur 1	
1.1.3	DP	Chandelle 1	
1.2	DP	Liaison O (Forme cylindrique + goupille)	
1.3	DP	Bras inférieur 2	
1.3.1	DP	-	
1.3.2	DP	Stabilisateur 2	
1.3.3	DP	Chandelle 2	
1.4	DP	Liaison E (Forme cylindrique + goupille)	
1.5	DP	Bras supérieure	
1.5.1	DP	Liaison hélicoïdale	
1.5.2	DP	Liaison sphérique (rotation Z)	
1.5.3	DP	Liaison sphérique (rotation Y)	
1.6	DP	Liaison N (Forme sphérique + crochet)	
2	DP	Ensemble de rotules permettant la rotation selon l'axe Y	
0	FR	Porter l'outil par le tracteur	
1	FR	Lier l'outil au tracteur	
1.1	FR	Positionner le point O1 de la première barre inférieure en O2	
1.1.1	FR	Positionner le point O1 en O2 selon l'axe X	
1.1.2	FR	Positionner le point O1 en O2 selon l'axe Y	
1.1.3	FR	Positionner le point O1 en O2 selon l'axe Z	
1.2	FR	Lier et maintenir O1 en O2	
1.3	FR	Positionner le point E1 de la deuxième barre inférieure en E2	
1.3.1	FR	Positionner le point E1 en E2 selon l'axe X	
1.3.2	FR	Positionner le point E1 en E2 selon l'axe Y	
1.3.3	FR	Positionner le point E1 en E2 selon l'axe Z	
1.4	FR	Lier et maintenir E1 en E2	
1.5	FR	Positionner le point N1 de la barre supérieure en N2 de l'outil	
1.5.1	FR	Positionner le point N1 en N2 selon l'axe X	
1.5.2	FR	Positionner le point N1 en N2 selon l'axe Y	
1.5.3	FR	Positionner le point N1 en N2 selon l'axe Z	
1.6	FR	Lier et maintenir N1 en N2	
2	FR	Permettre le réglage de hauteur de l'outil par rapport au tracteur	

Figure 6.8. DPs et FRs de la LTP.

Etape 6. Analyse de la conception de la LTP: La matrice de conception relative à la décomposition hiérarchique présentée à la figure 6.8 est montrée à la figure 6.9. Nous avons rempli cette matrice comme suit :

- Les Trois barres (DP1) répondent à Porter l'outil par le tracteur (FR1).
- L'Ensemble de rotules permettant la rotation selon l'axe Y (DP2) répond à Porter l'outil par le tracteur (FR2).
- Le Bras inférieur 1 (DP11) répond à Positionner le point O1 de la première barre inférieure en O2 (FR11).
- La Liaison O (Forme cylindrique + goupille) (DP12) répond à Lier et maintenir O1 en O2 (FR12).
- Le Bras inférieur 2 (DP13) répond à Positionner le point E1 et de la deuxième barre inférieure en E2 (FR13).
- La Liaison E (DP14) répond à Lier et maintenir E1 en E2 (FR14).
- Le Bras supérieur (DP15) répond à Positionner le point N1 de la barre supérieure en N2 (FR15).

- Le Liaison N (DP16) répond à Lier et maintenir N1 en N2 (FR16).
- Il n'a y pas de solution prévue (et donc de DPs) pour les fonctions Positionner le point O1 en O2 selon l'axe X (FR111) et Positionner le point O1 en O2 selon l'axe Z (FR131). Ces fonctions permettent le déplacement des deux bras inferieurs selon X. En effet, ce déplacement est actuellement réalisé par le déplacement du tracteur ; déplacement difficile car réalisé depuis la cabine du tracteur par l'utilisateur (mauvaise visibilité de la LTP depuis la cabine).
- Les chandelles DP113 et DP133 assurent une translation selon son axe principal. Cette translation permet un déplacement selon Z mais également, du fait de la cinématique, un léger déplacement selon X et Y.
- Les stabilisateurs DP112 et DP132 assurent une translation leur axe principal. Cette translation permet un déplacement selon Y mais également un léger déplacement selon X.
- Les liaisons sphériques DP152 et DP153 relient le bras supérieur au tracteur et assure ainsi le déplacement selon Y et Z du point N. Ces déplacements sont également liés à un déplacement selon X.

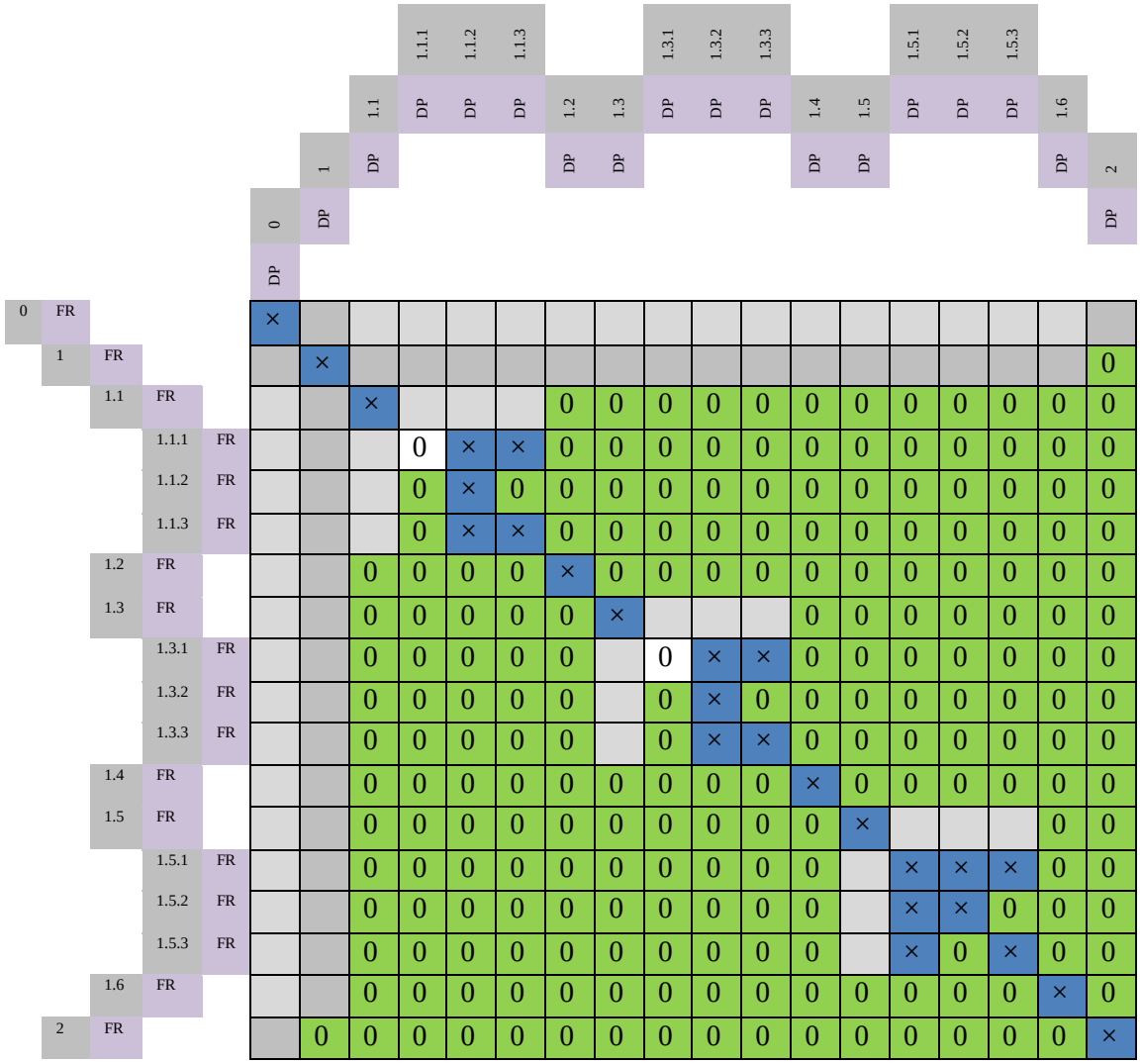


Figure 6.9. Matrice de conception de la LTP.

La matrice de conception réalisée ici n'est ni diagonale, ni triangulaire. La conception est donc dite couplée. 12 couplages apparaissent dans cette matrice. Par exemple, 3 FRs sont

liés à 2 DPs pour l'exigence fonctionnelle FR11. Il en est de même pour FR13. Les couplages sont ici relatifs au manque de DPs. Effectivement, ces deux exigences n'admettant pas de DP sont liées au besoin de mise en position des points d'accrochage par rapport à l'outil.

6.3.3. Identification et ventilation des risques selon les trois phases de conception

Etape 7. Identification de la source du phénomène dangereux : Les résultats des étapes 1 et 2 indiquent que les faits « Homme situé entre le tracteur et l'outil pour attacher l'outil au tracteur » et « Renversement de l'outil » entraînent l'« écrasement ». Ils montrent également que la conséquence du phénomène dangereux est l'« écrasement » et sa source le renversement de l'outil donc une « chute d'objets ».

Etape 8. Ventilation du risque : La première étape consiste à répondre à la question : *Est-ce que la source du phénomène dangereux est liée à une énergie* ? Selon la classification des sources des phénomènes dangereux mécaniques et leur lien avec les phases de la conception présentée au chapitre 4, §4.2.3.2 (tableau 4.2), « chute d'objets » est lié à l'énergie. La réponse à la question est donc positive. Nous pouvons donc en conclure que le risque lié à ce phénomène dangereux est un risque d'accident (C2).

6.3.4. Evaluation du niveau de sécurité de la liaison trois points

Etape 9. Définition de la Présence de Danger : Dans cette étape, doit être calculée la Présence de Danger de la LTP. Il s'agit d'identifier les P_{Pd}, P_{Sd} et P_{Ed} en répondant aux trois questions suivantes à partir des connaissances obtenues suite à l'analyse des rapports d'accident :

- P_{Pd} : Est-ce que la solution comporte un Phénomène dangereux ou non ? L'attelage demande de produire un effort sur l'outil. Il y a donc bien présence d'un phénomène dangereux. Donc $P_{Pd} = 1$.
- P_{Sd} : Est-ce que la solution comporte une Situation dangereuse ou non? L'opérateur pouvant se situer entre le tracteur et l'outil pour attacher l'outil au tracteur, la solution comporte une situation dangereuse. Donc $P_{Sd} = 1$.
- P_{Ed} : Est-ce que la solution comporte un Evénement dangereux ou non ? Un humain peut être écrasé par l'outil lors de l'attelage. La solution comporte donc un événement dangereux. Donc $P_{Ed} = 1$.

D'après le tableau 4.6 (Chapitre 4, §4.3.4.1) rappelé ci-dessous (tableau 6.2), sachant que $P_{Pd} = P_{Sd} = P_{Ed} = 1$, $P_{Dssmp} = 1$ pour la LTP. Il convient de noter que la LTP est un système sans moyen de protection. Il n'y a donc pas lieu ici de mettre en œuvre la partie de la démarche demandant l'évaluation de la sécurité des moyens de protection du système.

Tableau 6.2. Valeurs prises par la Présence de Danger pour un système sans moyen protection (P_{Dssmp}).

P_{Pd}	P_{Sd}	P_{Ed}	P_{Dssmp}
0	0	0	0
1	0	0	0
1	1	1	1

Etape 10. Définition du Niveau de Risque (N_R) : Pour définir N_R, il convient de calculer N_{RPd}, N_{RSd} et N_{REd}.

. Niveau de Risque lié au Phénomènes dangereux (N_{RPd}) : Comme expliqué à l'étape 1, les faits « Homme situé entre le tracteur et l'outil pour attacher l'outil au tracteur » et « Renversement de l'outil » peuvent causer un « Ecrasement ». Les étapes 7 et 8 indiquent que la source du phénomène dangereux est en lien avec un risque d'accident (C2). Le calcul

du Niveau de Risque lié à ce phénomène dangereux doit donc être fait en utilisant l'équation (4-12).

$$N_{RPd}\ en\ lien\ avec\ C2: \begin{cases} N_{RPd} = 1 - \dfrac{E_{seuil}}{E} & si \quad E > E_{seuil} \\ N_{RPd} = 0 & si \quad E \leq E_{seuil} \\ avec: \\ E: valeur\ de\ l'énergie\ dégagée\ par\ le\ phénomènedangereux \\ E_{seuil}: valeur\ maximale\ de\ l'énergie\ supportée\ par\ l'humain \end{cases} \qquad Equation\ (4-12)$$

L'énergie mise en jeu est l'énergie potentielle. Le niveau d'énergie se formule donc de la façon suivante :

$$E: \begin{cases} E = E_{pp} = mgh \\ avec: \\ E_{pp}: Energie\ potentielle \\ m: masse \\ h: altitude \\ g: pesanteur \end{cases} \qquad Equation\ (6-1)$$

De la même façon, le niveau d'énergie seuil, E_{seuil}, peut être défini par l'équation suivante :

$$E_{seuil}: \begin{cases} E_{seuil} = E_{pp} = m_{seuil} g h_{seuil} \\ avec: \\ m_{seuil}: masse\ de\ l'humain \\ h_{seuil}: taille\ de\ l'humain \end{cases} \qquad Equation\ (6-2)$$

En intégrant ces deux équations dans l'équation permettant le calcul du Niveau de Risque lié à un Phénomène dangereux (équation 10), on obtient l'équation suivante :

$$N_{RPd}: \left\{ N_{RPd} = 1 - \frac{E_{seuil}}{E} = 1 - \frac{m_{seuil} h_{seuil}}{mh} \right.$$

Nous considérons :

- un humain pesant 70 kg, mesurant 170 cm et dont le centre de masse se situe à 85 cm de hauteur ;
- un outil du type « cultivateur » pesant 925 kg, positionné à 80 cm du sol et dont le centre de masse se situe à 40 cm de hauteur par rapport à sa base.

Le N_{RPd} de la LTP peut donc être calculé :

$$N_{RPd} = 1 - \frac{m_{seuil} h_{seuil}}{mh} = 1 - \frac{70 \times 85}{925 \times 40} = 0{,}84$$

. Niveau de Risque lié à la Situation dangereuse (N_{RSd})

Dans cette étape, nous définissons le Niveau de Risque lié à la Situation dangereuse (N_{RSd}). Pour cela, nous appliquons l'équation (4-15).

$$N_{RSd}: \begin{cases} N_{RSd} = T / T_{ref} \\ avec: \\ T: temps\ d'exposition\ de\ la\ persone \\ T_{ref}: durée\ du\ cycle\ de\ travail \end{cases} \qquad Equation\ (4-15)$$

En se basant sur les rapports d'accident existants et sur les autres éléments du REX. Le temps d'exposition de l'opérateur au phénomène dangereux pendant un cycle de travail complet est, en moyenne, de 5 minutes ; temps calculé sur la durée d'un cycle de travail de 20 minutes. Le N_{RSd} de la LTP peut donc être calculé :

$$N_{RSd} = \frac{T}{T_{ref}} = \frac{5}{20} = 0{,}25$$

. Niveau de Risque lié à l'Evénement dangereux (N_{REd})

Facteur de Risque lié au système (F_{Rs}) : Pour déterminer N_{REd}, il faut tout d'abord définir le F_{Rs} en utilisant l'équation (4-20).

$$F_{Rs}:\begin{cases} F_{Rs} = \dfrac{(\alpha_1 Q_c + \alpha_2 N_f)}{\alpha_1 + \alpha_2} \\ \alpha_1 : coefficient\ de\ pondération\ Q_c \\ \alpha_2 : coefficient\ de\ pondération\ de\ N_f \end{cases} \qquad Equation\ (4-20)$$

Pour déterminer la valeur de F_{Rs} de la LTP, la Qualité de conception (Q_c) et le Niveau de fiabilité (N_f) de la LTP doivent être calculé. Nous avons vu à l'étape 6 que la conception de la LTP est une conception couplée. Q_c vaut donc 1. Pour calculer N_f, nous nous basons sur les informations trouvées dans des documents techniques. Selon ces données, la durée de vie de la LTP est plus élevée que celle du tracteur équipé. Si l'on considère la durée de vie souhaitée de la LTP comme égale à la durée de vie du tracteur, sa durée de vie avant défaillance sera plus grande que sa durée de vie souhaitée. Nous en concluons que $N_f = 0$. En prenant $\alpha_1 = 2$ et $\alpha_2 = 1$, l'équation du Facteur de Risque devient :

$$F_{Rs} = \frac{(\alpha_1 Q_c + \alpha_2 N_f)}{\alpha_1 + \alpha_2} = \frac{2+0}{3} = 0{,}67$$

Facteur de Risque lié à l'humain (F_{Rh}) : Selon l'équation (4-21), nous avons besoin pour définir F_{Rh} d'identifier les quatre catégories de facteur de risque lié à l'humain (F_1: la formation ; F_2: l'expérience ; F_3: l'état physique ; et F_4: l'attitude) en se basant sur les rapports d'accident existants.

$$F_{Rh}:\begin{cases} F_{Rh} = \dfrac{\sum_{i=1}^{n} \beta_i F_{Rhi}}{\sum_{i=1}^{n} \beta_i} \\ avec: \\ n:\ nombre\ des\ facteurs\ considérés \\ F_{Rhi} : i^{ème}\ facteur;\ \forall\ i\ ,\ F_{Rhi} = 0,1 \\ \beta_i : coefficient\ de\ pondération\ pour\ le\ i^{ème}\ facteur \end{cases} \qquad Equation\ (4-21)$$

Dans le cas des accidents étudiés, les victimes avaient été formées à l'utilisation et aux risques liés à l'attelage de la LTP. Elles étaient expérimentées, avaient une bonne condition physique mais travaillaient sous pression. Par conséquent, $F_1 = 0$; $F_2 = 0$; $F_3 = 0$ et $F_4 = 1$. Concernant les coefficients de pondération, nous considérons que l'ordre d'importance des quatre catégories de facteur de risque lié à l'humain est le suivant : F_1, F2, F_3 puis F_4. Nous donnons respectivement les valeurs 4, 3, 3 et 1 aux coefficients de pondération β_1, β_2, β_3 et β_4. L'équation donnant F_{Rh} devient :

$$F_{Rh} = \frac{\sum_{i=1}^{n} \beta_i F_i}{\sum_{i=1}^{n} \beta_i} = \frac{(4\times 0) + (3\times 0) + (2\times 0) + (1\times 1)}{4+3+2+1} = 0{,}1$$

Facteur de Risque lié à l'environnement (F_{Re}) Selon l'équation (4-22), les trois catégories de facteurs environnementaux ont besoin d'être identifiés pour définir F_{Re} (F_{Re1}: présence d'autre personne ; F_{Re2}: environnement fermé ou ouvert ; F_{Re3}: milieu structurée ou naturel).

$$F_{Re}:\begin{cases} F_{Re} = \dfrac{\sum_{j=1}^{m} \gamma_j F_{Rej}}{\sum_{j=1}^{m} \gamma_j} \\ avec: \\ m : nombres\ des\ facteurs\ considérés \\ F_{Rej} : j^{ème}\ facteur \qquad \forall\ j\ ,\ F_{Rej} = 0,1 \\ \gamma_j :\ coefficient\ de\ pondération\ pour\ le\ j^{ème}\ facteur \end{cases} \qquad Equation\ (4-22)$$

Comme pour F_{Rh}, nous nous basons sur les rapports d'accident existants et nous adoptons les valeurs suivantes :

- $F_{Rh1} = 1$ car plusieurs personnes peuvent se trouver dans l'environnement de travail ;
- $F_{Rh2} = 1$ car le milieu où se trouve la LTP est un milieu ouvert ;
- $F_{Rh3} = 1$ car ce milieu est un milieu naturel non-structuré.

Nous considérons que l'ordre d'importance des trois catégories des facteurs de risque lié à l'environnement est le suivant : F_1, F_2 puis F_3. Nous donnons respectivement les valeurs 3, 2 et 1 aux coefficients de pondération γ_1, γ_2 et γ_3. Ainsi, l'équation donnant F_{Re} devient :

$$F_{Re} = \frac{\sum_{j=1}^{m} \gamma_j F_j}{\sum_{j=1}^{m} \gamma_j} = \frac{(3 \times 1) + (2 \times 1) + (1 \times 1)}{3 + 2 + 1} = 1$$

Niveau de Risque lié à l'Evénement dangereux (N_{REd}): Dans cette étape, nous voulons obtenir la valeur de N_{REd} en appliquant l'équation (4-23).

$$N_{REd}: \begin{cases} N_{REd} = \dfrac{(\delta_1 F_{Rs} + \delta_2 F_{Rh} + \delta_3 F_{Re})}{\sum \delta} \\ avec: \\ \delta_1 : coefficient\ de\ pondération\ pour\ le\ F_{Rs} \\ \delta_2 : coefficient\ de\ pondération\ pour\ le\ F_{Rh} \\ \delta_3 : coefficient\ de\ pondération\ pour\ le\ F_{Re} \end{cases} \qquad Equation\ (4-23)$$

Nous considérons que le poids accordé à F_{Rs} doit être le plus important à la vue de notre objectif final d'améliorer la sécurité du système lors de sa conception. De plus, l'humain et son comportement ayant une influence généralement plus forte que l'environnement sur l'occurrence de l'accident, nous considérons que F_{Rh} doit avoir un poids plus important que F_{Re}. Pour ces raisons, nous donnons respectivement les valeurs 3, 2 et 1 aux coefficients de pondération δ_1, δ_2 et δ_3. Ainsi l'équation donnant N_{REd} devient :

$$N_{REd} = \frac{(\delta_1 F_{Rs} + \delta F_{Rh} + \delta_3 F_{Re})}{\sum \delta} = \frac{(3 \times 0{,}67) + (2 \times 0{,}1) + (1 \times 1)}{3 + 2 + 1} = 0{,}535$$

. Niveau de Risque (N_R)

Enfin, en appliquant l'équation (4-24) et les trois valeurs de N_{RPd}, N_{RSd}, et N_{REd} obtenues ci-dessus, il devient possible de définir le Niveau de Risque de la LTP.

$$N_R : \begin{cases} N_R = \dfrac{(\varepsilon_1 N_{RPd} + \varepsilon_2 N_{RSd} + \varepsilon_3 N_{REd})}{\sum \varepsilon} \\ avec: \\ \varepsilon_1 : coefficient\ de\ pondération\ pour\ le\ niveau\ de\ risque\ lié\ au\ Pd \\ \varepsilon_2 : coefficient\ de\ pondération\ pour\ le\ niveau\ de\ risque\ lié\ à\ la\ Sd \\ \varepsilon_3 : coefficient\ de\ pondération\ pour\ le\ niveau\ de\ risque\ lié\ à\ l'Ed \end{cases} \qquad Equation\ (4-24)$$

Selon l'ordre de priorité pour la réduction de risque proposé dans la norme [FD ISO/TR 14121-2, 2008], l'élimination du phénomène dangereux est la priorité. Vient ensuite l'élimination de la situation dangereuse et enfin l'événement dangereux. Dans notre calcul du niveau de risque et comme pour le cas de l'ATC, nous proposons de garder cet ordre de priorité et donc d'adopter respectivement les valeurs 3, 2 et 1 aux facteurs de pondération ε_1, ε_2 et ε_3. L'équation donnant N_R devient :

$$N_R = \frac{(\varepsilon_1 N_{RPd} + \varepsilon_2 N_{RSd} + \varepsilon \delta_3 N_{REd})}{\sum \varepsilon} = \frac{(3 \times 0{,}84) + (2 \times 0{,}25) + (1 \times 0{,}535)}{3 + 2 + 1} = 0{,}5925$$

Etape 11. Définition de l'Indicateur de Sécurité : En appliquant l'équation (24) et les deux valeurs de P_D et de N_R obtenues ci-dessus, l'Indicateur de Sécurité de la LTP devient :

$$I_{S\ LTP\ smp} = 1 - I_{PD} \times N_R = 1 - (1 \times 0{,}5925) = 0{,}4075$$

Le système LTP n'a pas un moyen de protection, la valeur de l'indicateur de sécurité du système la LTP est égale à celle du système sans moyen de protection.

$$I_{Ss} = \frac{\mu_1 I_{Sssmp} + \mu_2 \left(\frac{\sum_{z=1}^{n} I_{Smp\ z}}{n}\right)}{\mu_1 + \mu_2} = I_{S\ LTP\ smp} = 0{,}4075$$

Selon notre indicateur, le niveau de sécurité de la LTP est de $I_S = 0{,}4075$.

6.3.5. Définition et priorisation des objectifs de sécurité

Etape 12. Définition et hiérarchisation des objectifs de sécurité : Cette étape consiste à définir des objectifs de sécurité face au risque d'« écrasement par l'outil lors de l'attelage ». L'étape 1 a montré que les faits « Homme situé entre le tracteur et l'outil pour attacher l'outil au tracteur » et « Renversement de l'outil » peuvent causer l'« écrasement ». De plus, les étapes 7 et 8 ont montré que la source du phénomène dangereux est une « chute d'objets » et que le risque lié à ce phénomène est un risque d'accident (donc de type C2). Nous nous rapportons donc à la liste des objectifs de sécurité définie au chapitre V (§5.2.3.1) concernant ce type de risque. Ces objectifs sont définis ci-dessous :

Objectif de sécurité n°1. Eliminer le phénomène dangereux par conception : La première idée est de changer la solution de conception adoptée. La solution à changer est ici le « système trois points permettant de porter l'outil par le tracteur ». L'objectif de sécurité pourrait être, par exemple, formulé ainsi : « Eliminer la possibilité de renversement de l'outil ».

Objectif de sécurité n°2. Éliminer la situation dangereuse pour la personne : Pour éliminer la situation dangereuse, on peut « Eliminer le besoin d'intervention de l'opérateur entre le tracteur et l'outil lors de l'attelage ».

Objectif de sécurité n°3. Réduire la gravité du dommage lié au phénomène dangereux : Pour réduire la gravité du dommage lié à l'écrasement par l'outil, on peut par exemple « Minimiser le poids et le hauteur de l'outil ». Cette exigence est relative à l'outil et donc en dehors de notre périmètre d'étude.

Objectif de sécurité n°4. Réduire la fréquence et/ou la durée de l'exposition à la situation dangereuse : Pour réduire l'exposition à la situation dangereuse, il est possible de « Minimiser la fréquence et la durée d'intervention de l'opérateur entre le tracteur et l'outil lors de l'attelage ».

Objectif de sécurité n°5. Réduire la probabilité d'occurrence de l'événement dangereux : On peut ici, par exemple, « Minimiser les efforts sur l'outil lors de l'opération d'accrochage des points ».

Objectif de sécurité n°6. Eliminer l'événement dangereux en évitant le dommage par mise en place de dispositif de protection : L'objectif de sécurité peut être formulé de la manière suivante «Mise en place d'une protection temporaire lors de l'attelage éloignant l'opérateur de l'outil».

Objectif de sécurité n°7. Réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place d'un dispositif de protection :

L'objectif de sécurité peut être celui-ci : « Mise en place d'une protection temporaire lors de l'attelage formant un support à l'outil ».

Objectif de sécurité n°8. Réduire la probabilité d'occurrence de l'événement dangereux en éliminant le dommage par la mise en place de mesures de protection: On peut imaginer ici l'objectif de sécurité suivant : « Mise en place d'un système d'alarme se déclenchant lors du renversement de l'outil ».

Objectif de sécurité n°9. Eviter ou limiter le dommage après la conception : Pour éviter ou limiter les dommages après la conception de la LTP, nous pouvons proposer d'intégrer au guide d'utilisation la directive suivante (si celle-ci n'y est pas déjà): « N'attacher l'outil au tracteur lorsque celui-ci est dans une position instable ».

La figure 6.10 résume les objectifs de sécurité proposés pour la LTP.

Phase du processus de conception	Définition des objectifs de sécurité pour un risque C2 sur la LTP
Phase conception conceptuelle / Contexte C1	1. «Eliminer le renversement de l'outil ».
	2. «Eliminer le besoin d'intervention de l'opérateur entre le tracteur et l'outil lors de l'attelage ».
Phase conception architecturale / Contexte C3	3. « Minimiser le poids et la hauteur de l'outil ».
	4. « Minimiser la fréquence et la durée d'intervention de l'opérateur entre le tracteur et l'outil lors de l'attelage ».
	5. « Minimiser les efforts sur l'outil lors de l'opération d'accrochage des points ».
Phase conception détaillée / Contexte C5	-

Phase du processus de conception	Définition des objectifs de sécurité pour un risque C2 en ajoutant un moyen de protection
Phase conception conceptuelle / Contexte C1	6. «Mise en place d'une protection temporaire lors de l'attelage éloignant l'opérateur de l'outil».
Phase conception architecturale / Contexte C3	7. «Mise en place d'une protection temporaire lors de l'attelage formant un support à l'outil ».
	8. « Mise en place d'un système d'alarme se déclenchant lors du renversement de l'outil ».

Après le processus de conception	Définition des objectifs de sécurité pour un risque C2 sur le système
Guide d'utilisation	9. « Ne pas atteler l'outil au tracteur si celui-ci est dans une position instable». …

Figure 6.10. Objectifs de sécurité contre l'écrasement par l'outil lors de l'attelage.

6.3.6. Reconception sécuritaire de la liaison trois points

Etape 13. Choix d'un objectif de sécurité: Dans les objectifs de sécurité éliminant ou minimisant, le risque d'« écrasement par l'outil lors de l'attelage», présenté à la figure 6.10, nous nous positionnons dans les phases de conception conceptuelle de la LTP, et nous choisissons comme premier objectif de sécurité d'« éliminer le renversement d'outil » pour éliminer le phénomènes dangereux.

Etape 14. Définition des exigences fonctionnelles: Dans l'accident étudié, le phénomène dangereux existe lorsque l'opérateur agit sur l'outil pour l'accrocher au tracteur. L'outil se renverse alors sur lui. L'analyse de la matrice de conception de la LTP a notamment montré qu'aucune solution n'assure le déplacement selon X des deux bras inférieurs (voir §6.3.2). En effet, il n'y a pas de solution répondant aux deux exigences « FR111 : Positionner le point O1 en O2 selon l'axe X» et « FR131 : Positionner le point E1 en E2 selon l'axe X ». Par conséquent, éliminer le phénomène dangereux demande notamment de proposer des paramètres de conception permettant de répondre à ces exigences. Il faut noter que cette proposition est nécessaire mais pas suffisante pour éliminer le phénomène dangereux. Elle ne permettra que de le minimiser.

Nous traduisons l'objectif de sécurité « éliminer le renversement de l'outil » en une exigence fonctionnelle : « stabiliser l'outil avant l'attelage ».

Etape 15. Définition des solutions : Deux solutions candidates ont été définies lors d'une séance de brainstorming réunissant experts en mécanique, en conception et en machinisme agricole :

- Un bras supérieur rigide permettant de fixer la distance entre le tracteur et l'outil ;
- Un bras robotisé permettant de fixer la distance entre le tracteur et l'outil.

Etape 16. Identification des risques pour l'ensemble des solutions candidates : Pour les deux solutions proposées, l'écrasement de l'utilisateur devient impossible. Nous avons donc éliminé le risque identifié au niveau conceptuel.

Au niveau inférieur, c'est-à-dire au niveau architectural, le risque principal des deux solutions proposées est le « rapprochement d'un élément en mouvement avec une pièce fixe » (voir chapitre 4, §4.2.3, tableau 4.2). Il s'agit d'un risque de type risque anthropométrique ou de non fiabilité technique, c'est-à-dire un risque de type C4 (et donc lié à la phase de la conception architecturale).

Etape 17. Calcul de l'indicateur de sécurité pour l'ensemble des solutions candidates : Le risque d'« écrasement par l'outil lors d'attelage » étant éliminé, il n'existe plus de risque au niveau conceptuel. En conséquence, $P_D = 0$ et donc $I_S = 1$.

Au niveau architectural et par rapport à la solution initiale, la seule variable de l'indicateur qui va évoluer est le « Niveau de Risque lié au Phénomène dangereux (N_{RPd}) ». Cependant, le passage d'un risque au niveau conceptuel à un risque au niveau architectural diminue implicitement le niveau de risque lié au phénomène dangereux maintenant en lien avec les risques anthropométriques et de non fiabilité technique (C4). Nous pouvons donc, sans calculer sa valeur, conclure que l'indicateur de sécurité sera nécessairement supérieur.

Etape 18. Choix d'une solution : Différents contraintes telles que l'exiguïté de l'espace entre le tracteur et l'outil, la modification du châssis du tracteur de façon à fixer le bras au tracteur, la rusticité de la LTP et l'environnement de travail difficile (poussière, …) font que la solution du bras robotisée est abandonnée. La solution choisie est donc celle du bras supérieur fixé à l'outil rigide permettant de fixer la distance entre le tracteur et l'outil.

Etape 19. Itération suivante du processus de conception : La solution choisie, le processus de conception peut se poursuivre. Nous ne détaillons pas davantage la suite de la mise en œuvre de l'approche, le but de notre travail n'étant pas d'aller jusqu'à la fin de conception.

6.3.7. Conclusion sur la reconception sécuritaire de la liaison trois points

Dans les paragraphes précédents, nous avons appliqué l'approche proposée à la reconception sécuritaire de la Liaison Trois Points (LTP). Nous avons mis en évidence que les risques liés à la LTP sont relatifs au besoin de mise en position de la LTP par rapport à l'outil pendant la phase d'attelage ; l'outil se renversant sur l'opérateur lorsque ce dernier y applique un effort.

Des propositions ont été faites suite à la mise en œuvre de la démarche. Une solution permettant de stabiliser l'outil avant l'attelage, et donc d'éliminer le risque d'écrasement par l'outil, a été choisie.

L'application de la démarche proposée et la comparaison des résultats de l'application avec ceux obtenus par [Ghemraoui, 2009] en appliquant la méthode IRAD, nous permettent de noter, en particulier, les points suivants:

- La démarche proposée offre le moyen d'obtenir un éventail de solutions sécuritaires, ce que ne propose pas la méthode IRAD. L'application de la méthode IRAD sur la LTP a permis de trouver une solution réduisant la probabilité du renversement de l'outil, donc réduisant la probabilité de l'événement dangereux. Alors que la démarche que nous proposons permet de déduire l'ensemble des objectifs de sécurité améliorant la sécurité du système, donc l'ensemble des pistes et des solutions d'amélioration, et de pouvoir choisir l'objectif assurant le niveau de sécurité souhaité.
- La démarche proposée offre un indicateur permettant de mesurer le niveau de sécurité d'une solution et donc de comparer différentes alternatives de solutions permettant d'améliorer la sécurité de la LTP (alternatives proposées par le concepteur ou trouvées dans les brevets). L'analyse des couplages fait partie de cet indicateur. La méthode IRAD ne propose pas une telle démarche méthodique. Elle ne se base essentiellement que sur l'analyse des couplages de la solution.

6.4. Conclusion

Dans ce chapitre, nous avons présenté une approche de conception sécuritaire. Cette approche est la synthèse des démarches FRES et FR2ES, dans laquelle l'opérationnalisation d'IRAD est démontrée. Elle est composée de 19 étapes allant de l'identification des conditions dangereuses de l'accident à la finalisation du processus de conception.

La démarche proposée montre l'ensemble des étapes, boucles et itérations permettant de répondre aux objectifs des trois cas d'emploi de la méthode IRAD. Elle comporte différents points d'entrée et de sortie permettant de répondre à ces trois cas séparément mais permet également de répondre à d'autres objectifs pouvant être considéré comme intermédiaire. Ces objectifs sont, par exemple, l'identification des points faibles dans la conception d'un système impliqué dans un accident, la comparaison du point de vue sécurité de différents systèmes ou de solutions de conception ou encore l'identification de pistes d'amélioration de la sécurité d'un système.

Cette approche de conception sécuritaire a ensuite été appliquée au cas déjà étudié dans le cadre du développement de la méthode IRAD : la Liaison Trois Points (LTP). A partir d'un rapport d'accident, nous avons identifié le problème de sécurité. Nous avons ensuite analysé la conception du système LTP. Nous avons abouti, dans un premier temps, à un

ensemble d'objectifs de sécurité puis, dans un deuxième temps, à des pistes pouvant améliorer la sécurité du système. Nous avons adopté l'objectif de sécurité qui assure le plus haut niveau de sécurité possible, c'est-à-dire celui qui permet d'éliminer le phénomène dangereux. Ce choix s'est ensuite traduit par la proposition de deux idées de solution.

Dans le cadre de l'application de la méthode IRAD au cas de la LTP, [Ghemraoui, 2009] propose de réduire la probabilité de l'évènement dangereux (et non pas d'éliminer le phénomène dangereux, comme nous l'avons fait). Les résultats applicatifs obtenus sont par conséquent différents. Ces différences montrent l'influence de la prise de décision sur le résultat final et pointent l'intérêt du cadrage du passage du domaine physique au domaine fonctionnel du risque. La démarche proposée, par l'intermédiaire de la hiérarchie des objectifs de sécurité définie, intègre ce cadrage avant la formulation des exigences de sécurité. L'application de la démarche proposée permet donc d'obtenir les solutions les plus sécuritaires possibles, ce que ne peut pas prétendre la méthode IRAD.

Enfin, dans le cadre de la recherche de nouvelles solutions, la méthode IRAD dirige directement le concepteur vers la résolution des couplages en lien avec le problème de sécurité. Ce principe facilite la tâche du concepteur. Nous pensons qu'intégrer ce principe dans la démarche proposée serait une piste d'amélioration intéressante.

Conclusion générale et Perspectives

L'objectif de cette thèse était d'opérationnaliser la méthode IRAD (Innovative Risk Assessment Design). Pour atteindre cet objectif scientifique, nous avons proposé deux développements complémentaires : l'ingénierie inverse fonctionnelle pour la sécurité (ou FRES pour Functional Reverse Engineering for Safety) et la réingénierie fonctionnelle pour la sécurité (ou FR2ES pour Functional ReEngineering for Safety). Nous avons ensuite développé une approche de conception sécuritaire en nous basant sur ces deux développements complémentaires.

Notre problématique était à l'intersection de trois disciplines, la conception, la sécurité et l'aide à la décision. Neuf questions de recherche ont été identifiées. Ces questions et les réponses proposées sont rappelées ci-après.

1. Comment formaliser le REX en lien avec les problèmes de sécurité ? Nous avons répondu à cette question en proposant une structure type de rapport d'accident. D'un rapport correctement complété, il est possible d'extraire des connaissances utiles et applicables afin de les utiliser dans le processus de reconception du système ou de la partie du système impliquée dans l'accident. Le rapport d'accident est un des documents du REX sur l'accident. D'autres types de REX existent. Les formaliser serait intéressant et utile afin de compléter les connaissances en amont des problèmes de sécurité.

2. Comment extraire les connaissances d'un accident ? Le rapport type d'accident a été construit de manière à collecter des connaissances précises permettant de définir les conditions dangereuses liées à l'accident dans un premier temps et l'ensemble des causes potentielles dans un second temps.

3. Comment extraire les connaissances de la conception d'un système ? La mise en œuvre d'une analyse fonctionnelle, d'une analyse organique et de la conception axiomatique permet d'extraire des connaissances d'un système. Il s'agit dans un premier temps de comprendre le système par la schématisation puis d'analyser le système par l'approche organique, de définir des paramètres de conception et exigences fonctionnelles et enfin d'analyser la conception du système par la construction et l'analyse de la matrice de conception.

4. Comment ventiler les risques selon les phases du processus de conception ? Répondre à cette question, nous a demandé de nous appuyer sur l'analyse des connaissances des accidents et de la conception du système, sur les trois contextes C2, C4 et C6 de la méthode IRAD et sur les travaux normatifs portant sur la classification des sources des phénomènes dangereux. L'approche développée consiste à identifier la source du Phénomène dangereux et ensuite à ventiler les risques. Cette approche utilise une liste de sources de phénomènes dangereux. Celle-ci pourrait être encore améliorée.

5. Comment mesurer le niveau de sécurité d'un système ? Un indicateur de sécurité a été défini. La démarche d'évaluation de la sécurité se décompose en quatre parties principales. Elle demande dans un premier temps d'identifier la présence de danger, de définir le niveau de risque puis de calculer l'indicateur de sécurité du système sans moyen de protection,

l'indicateur de sécurité des moyens de protection et enfin de définir l'indicateur de sécurité du système. Cet indicateur de sécurité possède l'avantage de s'affranchir de l'avis d'experts. Il est donc plus objectif. De plus, les aspects de conception du système et sa qualité de conception sont pris en compte ce qui permet de mesurer la sécurité du système dès la phase de la conception conceptuelle.

6. Comment transcrire de manière formelle et systématique les risques en exigences de sécurité ? Pour répondre à cette question, nous avons proposé de définir et de hiérarchiser les objectifs de sécurité pour un risque donné et d'identifier leurs niveaux d'intervention dans le processus de conception. Cette approche permet au concepteur d'introduire la bonne exigence de sécurité au bon moment de la conception.

7. Comment intégrer ces exigences de sécurité dans le processus de conception ? Une approche de reconception sécuritaire permettant de choisir un objectif de sécurité parmi plusieurs et d'aider à reconcevoir de manière sécuritaire à partir de l'objectif de sécurité choisi a été développée.

8. Comment formuler des connaissances, des données et des contraintes relatives à la sécurité pour aider aux choix faits lors de la conception? La formalisation des connaissances faisant le lien entre sécurité et phases de conception a été développée. Cependant, celle-ci doit être poursuivie dans le futur.

9. Comment faire pour que la méthode IRAD soit facile à utiliser par les concepteurs, les bureaux d'études, les équipes de R & D, les fabricants, ...? Nous avons commencé à architecturer un outil expérimental support de la démarche et exploitant le formalisme proposé. Dans les travaux futurs, nous devons compléter cet outil.

L'objectif industriel consistait à sécuriser les liaisons tracteurs-outils. L'approche de conception sécuritaire proposée a été appliquée à deux de ces systèmes : l'arbre de transmission à cardans et la liaison trois points. Ces applications ont permis de valider l'approche d'une part et de proposer des solutions permettant de sécuriser ces systèmes d'autre part.

Références Bibliographiques

Références Normatives

[FD ISO/TR 14121-2, 2008] FD ISO/TR 14121-2, 2008. Sécurité des machines: Appréciation du risque - Partie 2: Lignes directrices pratiques et exemples de méthodes.

[NF EN ISO 12100, 2010] NF EN ISO 12100, 2010. Sécurité des machines: Principes généraux de conception- Appréciation du risque et réduction du risque.

[NF EN ISO 6385, 2004] NF EN ISO 6385, 2004. Principes ergonomiques de la conception des systèmes de travail.

[NF EN 45020, 2007] NF EN 45020, 2007. Normalisation et activités connexes - Vocabulaire général.

[ISO 15226, 1999] ISO 15226. 1999. Documentation technique de produits - Modèles de cycle de vie et affectation de documents

[FD X50-153, 2009] FD X50-153. 2009. Analyse de la valeur - Recommandations pour sa mise en œuvre

[ISO 5673-1, 2005] ISO 5673-1. 2005. Tracteurs et matériels agricoles - Arbres de transmission à cardans de prise de force et arbre récepteur de la machine - Partie 1 : exigences générales de fabrication et de sécurité

[ISO 5673-2, 2005] ISO 5673-2.2005. Tracteurs et matériels agricoles - Arbres de transmission à cardans de prise de force et arbre récepteur de la machine - Partie 2 : spécifications relatives à l'utilisation des arbres de transmission à cardans de prise de force, et position et dégagement de la ligne de transmission de prise de force et de l'arbre récepteur de la machine pour différents systèmes d'attelage

[NF EN ISO 5674, 2009] NF EN ISO 5674, 2009. Tracteurs et matériels agricoles et forestiers - Protecteurs d'arbres de transmission à cardans de prise de force - Essais de résistance mécanique et d'usure et critères d'acceptation.

[NF EN 12965 + A2, 2009] NF NE 12965+A2. 2009. Tracteurs et matériels agricoles et forestiers - Arbres de transmission à cardans de prise de force et leurs protecteurs - Sécurité

[NF EN ISO 15535, 2013] NF EN ISO 15535, 2013. Exigences générales pour la création de bases de données anthropométriques.

[NF EN 614-1+A1, 2009] NF EN 614-1+A1, 2009. Sécurité des machines - Principes ergonomiques de conception - Partie 1 : terminologie et principes généraux

[NF EN ISO 9612, 2009] NF EN ISO 9612, 2009. Acoustique - Détermination de l'exposition au bruit en milieu de travail - Méthode d'expertise.

[NF EN ISO 11688-1,2009] EN ISO 11688-1,2009. Acoustique - Pratique recommandée pour la conception de machines et d'équipements à bruit réduit - Partie 1 : planification.

[NF EN ISO 11688-2, 2004] NF EN ISO 11688-2, 2004. Acoustique - Pratique recommandée pour la conception de machines et équipements à bruit réduit - Partie 2 : introduction à la physique de la conception à bruit réduit

[NF EN 1299+A1, 2009] NF EN 1299+A1, 2009. Vibrations et chocs mécaniques - Isolation vibratoire des machines - Informations pour la mise en oeuvre de l'isolation des sources.

[NF EN 12198-1, 2008] NF EN 12198-1, 2008. Sécurité des machines - Estimation et réduction des risques engendrés par les rayonnements émis par les machines - Partie 1 : principes généraux.

[NF EN 1005-2+A1, 2008] NF EN 1005-2+A1, 2008. Sécurité des machines - Performance physique humaine - Partie 2 : manutention manuelle de machines et d'éléments de machines.

[NF EN 1005-3+A1, 2008] NF EN 1005-3+A1, 2008. Sécurité des machines - Performance physique humaine - Partie 3 : limites des forces recommandées pour l'utilisation de machines.

[NF EN 1005-4, 2008] NF EN 1005-4, 2008. Sécurité des machines - Performance physique humaine - Partie 4 : évaluation des postures et mouvements lors du travail en relation avec les machines

[NF ISO 11228-2, 2007] NF ISO 11228-2, 2007. Ergonomie - Manutention manuelle - Partie 2 : actions de pousser et de tirer.

[NF EN ISO 15535, 2013] NF EN ISO 15535, 2013. Exigences générales pour la création de bases de données anthropométriques.

[NF EN 45020, 2007] NF EN 45020, 2007. Normalisation et activités connexes - Vocabulaire général.

[NF EN ISO13849-1, 2008] NF EN ISO13849-1, 2008. Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1 : principes généraux de conception.

[NF EN 953+A1, 2009] NF EN 953+A1, 2009. Sécurité des machines - Protecteurs - Prescriptions générales pour la conception et la construction des protecteurs fixes et mobiles.

Références Scientifiques

[Alting, 1993] Alting L., "*Life-Cycle Design of Products: A New Opportunity for Manufacturing Enterprises, Concurrent Engineering: Automation, Tools, and Techniques"*, ed. by Andrew Kusiak, John Wiley & Sons, New York, ISBN 0-471-55492-8, 1993.

[Altshuller, 1984] Altshuller G., "Creativity as an exact science. The theory of the solution of inventive problems*"*, Gordon and Breach Science Publishers, 1 janv, 1984.

[Altshuller, 2004] Altshuller G., "40 Principes d'innovation", 2004.

[Altshuller, 2006] Altshuller G., "Et soudain apparut l'inventeur: les idées de TRIZ", 2006.

[Aven, 2009] Aven T., "Safety is the antonym of risk for some perspectives of risk". Safety Science 47, 25–930, 2009.

[Banas et al, 2006] Banas B., Berte R., Cheze B., Coroenne F., Cosme Ch., Derdek D., Dufumier D., et al. "Les liaisons tracteurs-outils Pour des opérations d'attelage et de dételage aisées et sûres*"*, Ed. Educagri, 2006.

[Banas et al, 2007] Banas B., Berte R., Bouvard M., Coroenne F., Derdek D., Dufumier D., Gallien M. et al. "Les liaisons tracteurs-outils. L'arbre de transmission à cardans quelle évolution*"*, 2007.

[Béler, 2008] Béler C., "Modélisation générique d'un retour d'expérience cognitif Application à la prévention des risques*", Thèse de Doctorat, Université de Toulouse, Soutenue le* 14 novembre, 2008.

[Benziane, 2013] Benziane, H., " L'ingénierie inverse et la conception axiomatique pour la prise en compte d'exigences de sécurité en conception", Rapport de stage, Irstea, 2013.

[Bernard et Hasan, 2002] Bernard A., Hasan R. "Working situation model for safety integration during design phase", Annals *of the CIRP Manufacturing, Vol.* 51, 119-122, 2002.

[Caputo et al., 2013] Caputo A.C., Pelagagge, P.M., Salini P., "AHP-based methodology for selecting safety devices of industrial machinery", Safety Science, Vol. 53, 202–218, 2013.

[Clermont et al., 2007] Clermont Ph., Béler C., Rakoto H., Desforges X., Geneste L., "Capitalisation et exploitation du retour d'expérience : un raisonnement à partir de cas étendu aux systèmes socio-techniques, in Raisonnement à partir de cas, conception et configuration de produits*"*, vol. 1, série Informatique et Systèmes d'Information, collection Hermès, pp. 249--277, janvier, 2007.

[Coulibaly et al., 2008] Coulibaly A., Houssin R., Mutel B., "Maintainability and safety indicators at design stage for mechanical products", Computers in Industry, Vol. 59, 438–449, 2008.

[CSST et IRSST, 2008] CSST et IRSST, "Sécurité des machines. Prévention des phénomènes dangereux d'origine mécanique, Protecteurs fixes et distances de sécurité*"*, Bibliothèque et Archives nationales du Québec, ISBN 978-2-550-51563-0, 2008.

[De La Garza, 2005] De La Garza C., "L'intégration de la sécurité lors de la conception de machines à risques pour les opérateurs : comparaison de logiques

différentes de conception", *Pistes*, Vol. **7**, 2005.

[De La Garza et Fadier, 2007] De la Garza C., Fadier E. "Le retour d'expérience en tant que cadre théorique pour l'analyse de l'activité et la conception sûre*"*, @ctivités, 4, 2007.

[Dickinson, 2004] Dickinson A.L., "Integrating axiomatic design into *a* design *for* six sigma deployment", International Conference on Axiomatic Design, 4th ICAD, Firenze, June 13-16, 2006.

[Didelot, 2002] Didelot A., "Contribution à l'identification et au contrôle des risques dans le processus de conception", Thèse de Doctorat, INRS, 2002.

[Fadier et al., 2003] Fadier E., De La Garza C., Didelot A., "Safety Design and human activity: construction of a theoretical framework from analysis of a printing sector". *Safety Design*, 41, 759-789, 2003.

[Filippi et al., 2010] Filippi S., Motyl B., Massimo Ciappina F., "Classifying TRIZ methods to speed up their adoption and the ROI for SMEs", Procedia Engineering, Vol.9, 172–182, 2010.

[Ge et al., 2002] Ge P., Lu S. C.-Y., Suh N., "An axiomatic approach for target cascading of parametric design of engineering systems", CIRP Annals - Manufacturing Technology, Vol.51, 111-114, 2002.

[Ghemraoui et al., 2009] Ghemraoui, R., Mathieu, L., Tricot, N., "Design method for systematic safety integration", *CIRP Annals - Manufacturing Technology*, Vol. 58, 161-164, 2009.

[Ghemraoui, 2009] Ghemraoui R., "Méthodologie de conception innovante intégrant la sécurité des utilisateurs –Application à la liaison tracteur-outils", *Thèse de Doctorat,* Ecole Normale Supérieure de Cachan, *Soutenue le* 17 novembre 2009.

[Harms-Ringdahl, 2003] Harms-Ringdahl L., "Investigation of barriers and safety functions related to accidents", Preprint version of article in proceedings of ESREL 2003, European Safety and Reliability Conference 2003,

[Hasan, 2002] Hasan R., "Contribution à l'amélioration des performances des systèmes complexes par la prise en compte des aspects socio-techniques dès la conception : proposition d'un modèle original de SITUATION DE TRAVAIL pour une nouvelle approche de conception", *Thèse de Doctorat, Université Henri Poincaré, Nancy I, Soutenue le22 mars 2002.*

[Hasan et al., 2004] Hasan R., Martin P., Bernard A., "Solving Contradictions Problems Related To Safety Integration In Design Process", TRIZ Journal, 2004.

[Helander, 2007] Helander M. G., "Using design equations to identify sources of complexity in humanmachine interaction", Theoretical Issues in Ergonomics Science, Vol. 8, 123-146, 2007.

[Hellevik, 1999] Hellevik O., "Research Methodology in Sociology and Political Science", Universitetsforlaget, Oslo, Norway (In Norwegian), 1999.

[Ho Kon Tiat, 2006] Ho Kon Tiat V., "Aide à la décision pour la conception préliminaire de procédés d'évaporation flash", Doctoral thesis, Laboratoire interétablissements CNRS, ENSAM, ENSCPB, Université Bordeaux 1, France, 2006.

[Hollnagel, 1999] Hollnagel E., "Accident and barriers", *7th European Conference on Cognitive Science Approaches to Process Control*, September 21-24, France, 1999.

[Hollnagel, 2008] Hollnagel E., "Risk + barriers = safety?", *Safety Science*, Vol. 46, 221-229, 2008.

[Houssin et Coulibaly, 2011] Houssin R., Coulibaly A., "An approach to solve contradiction problems for the safety integration in innovative design process", Computers in Industry, Vol. 62, 398–406, 2011.

[INRS, 2006] INRS, "Sécurité des machines et des équipements de travail - Moyens de protection contre risque mécaniques", 2006.

[Juglaret, 2012] Juglaret F., "Indicateurs et Tableaux de Bord pour la prévention des risques en Santé-Sécurité au Travail", *Thèse de Doctorat*, CRC, Mines-ParisTech, *Soutenue le* 17 décembre 2012.

[Kamsu Goguemn et al., 2008] Kamsu Foguem B., Coudert T., Béler C., Geneste L., "Knowledge formalization in experience feedback processes: An ontology-based approach", Computers in Industry, Vol. 59, 694-710, 2008.

[Karnas, 2011] Karnas G., " Psychologie du travail", 3rd edition, 2011. ISBN : 978-2-13-058849-8

[Kjellén, 2000] Kjellén U., "Prevention of accidents through experience feedback", Taylor & Francis, 2000.

[Kleiven, 2007] Kleiven S., "A *Parametric Study* of *Energy Absorbing Foams* for *Head Injury Prevention*", The 20th International Technical Conference on the Enhanced Safety of Vehicles Conference (ESV), Lyon, France, June 18–21, 2007.

[LaPlaca et al., 2007] LaPlaca M.C., Simon C.M., Prado G.R., Cullen D.K, "CNS injury biomechanics and experimental models", Weber & Maas (Eds.) Progress in Brain Research, Vol. 161, 2007.

[Licht et al., 2005] Licht D. M., Polzella D. J., "Human factors, ergonomics, and human factors engineering: an analysis of Definitions", Harry G. Armstrong Aerospace Medical Research Laboratory, U.S.A, 2005.

[Lo et Helander. 2007] Lo S., Helander M.G., "Use of axiomatic design principles for analysing the complexity of human-machine systems", *Theoretical Issues in Ergonomics Science*, Vol. 8, 147-169, 2007.

[Ilevbare et al., 2013] Ilevbare I.M., Probert D., Phaal R., "A review of TRIZ, and its benefits and challenges in practice", Technovation, Vol. 33, 30–37, 2013.

[Marhavilas et al., 2011] Marhavilas P.K., Koulouriotis D., Gemeni V., "Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000-2009", Journal of Loss Prevention in the Process Industries, Vol. 24, 477-523, 2011.

[Marsot, 2005] Marsot J., "QFD: A methodological tool for integration of ergonomics at the design stage", Applied *Ergonomics*, Vol. 36, 185-192, 2005.

[Mazouni, 2008] Mazouni M.H., "Pour une Meilleure Approche du Management des Risques : De la Modélisation Ontologique du Processus Accidentel au Système Interactif d'Aide à la Décision", *Thèse de Doctorat*,

Nancy-université, Soutenue le 13 Novembre 2, 2004.

[Mili, 2009] Mili A., "Vers des méthodes fiables de contrôle des procédés par la maîtrise du risque: Contribution à la fiabilisation des méthodes de process control d'une unité de Recherche et de Production de circuits semi-conducteurs ", *Thèse de Doctorat,* L'Institut polytechnique de Grenoble, *Soutenue le* 21 octobre 2009.

[Moehrle, 2005] Moehrle M.G., "What is TRIZ? From Conceptual Basics to a Framework for Research", Creativity and Innovation Management, Vol.14, Number 1, 2005.

[M2OS, 2009] Groupe de travail Mangement, Méthodes, Outils, Standards (M2OS), "Fiches méthodes", IMdR, 2009.

[Neboit et al, 1990] Neboit M., Guillermain H., Fadier E. "De l'analyse des systèmes à l'analyse de l'interaction opérateur x tâche: proposition méthodologique", Facteurs humains de la fiabilité dans les systèmes complexes, Octarès-Entreprise. 1990.

[Øien, 2001a] Øien K., "Risk indicators as a tool for risk control", Reliability Engineering and System Safety, Vol. 74, 129-145, 2001.

[Øien, 2001b] Øien K., "A framework for the establishment of organizational risk indicators", Reliability Engineering and System Safety, Vol. 74, 147-167, 2001.

[Øien, 2011a] Øien K., Utne I.B., Herrera, I.A., "Building Safety indicators: Part1- Theoretical foundation", Safety Science, Vol. 49, 148–161, 2011.

[Øien, 2011b] Øien K., Utne I.B., Tinmannsvik R.K., Massaiu S., "Building Safety indicators: Part 2 – Application, practices and results", Safety Science. Vol. 49,162–171, 2011.

[Pahl et Beitz, 2007] Pahl G., Beitz W., Feldhusen J., Grote K.-H., "Engineering design: A systematic approach", 3rd edition Berlin: Springer- Verlag, 2007.

[Polet, 2002] Polet P., "Modélisation des franchissements de barrières pour l'analyse des risques des systèmes homme-machines", *Thèse de Doctorat,* Université de Valenciennes et du Hainaut-Cambrésis, 2002.

[Pomian et al., 1997] Pomian J.L., Pradère T., Gaillard I., Ingénierie et ergonomie. Eléments d'ergonomie à l'usage des projets industriels, Cépadués-éditions, Toulouse, 1997.

[Popovi et Vasić, 2008] Popović V., Vasić B., "Review of Hazard Analysis Methods and Their Basic Characteristics", Faculty of Mechanical Engineering Transactions, Vol. 36(4), 181-187, 2008.

[Rakoto et al., 2002] Rakoto H., Clermont P., Geneste L., "Le Retour d'Expérience : un processus socio-technique. 1er Colloque du Groupe de Travail Gestion des Compétences et des Connaissances en Génie Industriel : vers l'articulation entre Compétences et Connaissances – Nantes", France, novembre 2002.

[Rakoto, 2004] Rakoto H., "Intégration du Retour d'Expérience dans les processus industriels Application à Alstom Transport", *Thèse de Doctorat,* Ecole Nationale d'Ingénieurs de Tarbes, Soutenue le 15 octobre 2004.

[Sadeghi et al., 2012a] Sadeghi L., Mathieu L., Tricot N., Al Bassit L., "Using a modeling language for a better integration of human safety at the early design

phase based on experience feedback analysis", International Conference of Agricultural Engineering CIGR-AgEng, July 8-12, 2012.

[Sadeghi et al., 2012b] Sadeghi L., Mathieu L., Tricot N., Al Bassit L., "Intégration systématique des contraintes normatives au cours de processus de conception d'une machine ", 18ème congrès de maîtrise des risques et de sûreté de fonctionnement, Lambda-Mu 18, October 16-18, 2012.

[Sadeghi et al., 2013a] Sadeghi L., Mathieu L., Tricot N., Al Bassit L., Ghemraoui R., "Towards Design for Safety Part1: Functional Reverse Engineering Driven by Axiomatic Design". International Conference on Axiomatic Design, 7th ICAD, Worcester, June 27-28, 2013.

[Sadeghi et al., 2013b] Sadeghi L., Mathieu, L., Tricot, N., Al Bassit L., Ghemraoui R., Towards Design for Safety Part2: Functional Re-Engineering using Axiomatic Design and FMEA. International Conference on Axiomatic Design, 7th ICAD, Worcester, June 27-28, 2013.

[Sallaou, 2008] Sallaou M., "Taxonomie des connaissances et exploitation en conception préliminaire: application à un système éolien"*, Thèse de Doctorat, Ecole Nationale Supérieure d'Arts et Métiers , Soutenue le* 24 Septembre 2008.

[Scaravetti, 2004] Scaravetti D., "Formalisation préalable d'un problème de conception, pour l'aide à la décision en conception préliminaire", *Thèse de Doctorat, ENSAM Bordeaux, soutenue le 3 Décembre*, 2004.

[Seguy, 2008] Seguy A., " Décision collaborative dans les systèmes distribués *:* application à la e-maintenance*", Thèse de Doctorat, Université de Toulouse, Soutenue le* 5 décembre 2008.

[Shahrokhi, 2006] Shahrokhi M., "Intégration d'un modèle de situation de travail pour l'aide à la formation et à la simulation lors de la conception et l'industrialisation de systèmes", *Thèse de Doctorat, Ecole Centrale de Nantes, Soutenue le* 5 décembre 2006.

[Shahrokhi et Bernard, 2006] Shahrokhi, M., Bernard, A., "Barrier analysis through industrial design processes", *Ergo IA*, 2006.

[Sienou, 2009] Sienou A., "Proposition d'un cadre métholodogique pour le management intégré des risques et des processus d'entreprise", *Thèse de Doctorat, Université de Toulouse, Soutenue* le 2 juin 2009.

[Sklet, 2006] Sklet S., "Safety barriers: Definition, classification and performance", *Journal of loss prevention in the process industries*, Vol.**19,** 494-506, 2006.

[Souchkov, 2008] Souchkov V., " A Brief history of TRIZ", Posted in the Web Site of CGI Training & Consulting, may 2008.

[Suh, 1990] Suh N., "The principles of design", Oxford University press, 1990.

[Suh, 2001] Suh N., "Axiomatic Design: Advances and Applications", Oxford University Press, 2001.

[Suh, 2005] Suh N., "Complexity in engineering. *Annals of the CIRP"*, Vol. **54,** 46-63, 2005.

[Tang et al, 2010] Tang D., Zhu R., Chen X., Zang T., Xu X., "Functional Reverse Engineering for Recreation Design", *Proceedings of the 6th CIRP-*

Sponsored International Conference on Digital Enterprise Technology, 2010.

[Urbanic et al., 2008] Urbanic R. J., ElMaraghy H. A., ElMaraghy. W. H., "A reverse engineering methodology for rotary components from point cloud data", *Int J Adv Manuf Technol*, Vol. 37, 1146 – 1167, 2008.

[Yannou, 2008] Yannou B., "Le FAST, Mode d'emploi", *Ecole Centrale Paris*, le 25 avril 2008.

[Yang et Zhang, 2000] Yang K., Zhang H., "A comparison of TRIZ and Axiomatic Design", *TRIZ Journal*, Août 2000.

[Zhang et al., 2004] Zhang Z., Chaali A., Vanderhaegen F., "A comparative study on prediction of human operator violation using neural networks ", International Conference on Systems, Man and Cybernetics October 10-13 2004.

[Zlotin et al., 2000] Zlotin B., Zusman A., Kaplan L., Visnepolschi S., Proseanic V., Malkin, S., "TRIZ Beyond Technology: The Theory and Practice of Applying TRIZ to Non-Technical Areas", Ideation international Inc., Michigan, February, 2000.

Aide à la décision pour l'intégration de la sécurité au plus tôt en phase de conception-Approche innovante de reconception de machines agricoles

Résumé : Les travaux de recherche exposés dans ce mémoire se positionnent dans le domaine de la conception sécuritaire. Cette thèse s'intéresse plus particulièrement à rendre opérationnelle la méthode IRAD (Innovative Risk Assessment Design), qui intègre la sécurité de manière systématique tout au long du processus de conception. Dans cet objectif, nous proposons dans un premier temps de formaliser un type de retour d'expérience (les rapports d'accident) qui détaille les faits liés aux éléments d'une situation de travail et à des événements qui ont mené à un accident. Ensuite, nous proposons deux démarches complémentaires de reconception sécuritaire: une démarche d'ingénierie inverse fonctionnelle pour la sécurité (FRES) et une démarche de réingénierie fonctionnelle pour la sécurité (FR2ES). FRES permet d'extraire les connaissances à la fois sur l'accident et sur la conception du système impliqué dans l'accident. Elle permet ensuite d'évaluer le niveau de sécurité du système par l'estimation d'un indicateur de sécurité dépendant notamment du type de risque identifié. Cet indicateur est utilisé comme paramètre d'aide à la décision lors de la phase de reconception du système. La deuxième démarche, FR2ES, permet de définir les objectifs de sécurité liés à chaque phase de la conception dans le but d'éliminer ou de réduire un risque donné. Les solutions les plus sécuritaires possibles sont ensuite obtenues d'une part en intégrant ces objectifs de sécurité dans le processus de reconception et d'autre part à l'aide de l'indicateur de sécurité appliqué aux solutions proposées. Enfin, l'applicabilité de ces démarches a été démontrée sur deux types de liaisons tracteurs-outils, l'arbre de transmission à cardans et la liaison trois points ; systèmes permettant d'atteler les outils aux tracteurs et de les motoriser.

Mots-clés : conception sécuritaire, retour d'expérience, aide à la décision, ingénierie inverse fonctionnelle, indicateur de sécurité, réingénierie fonctionnelle, liaison tracteurs-outils.

Decision support for safety integration at the earliest design phases - Innovative approach to redesigning of agricultural machinery

Abstract: The research presented in this thesis is positioned in the field of design for safety. This thesis is particularly interested in operationalizing the IRAD (Innovative Risk Assessment Design) method, which integrates safety systematically throughout the design process. For this purpose, in first step, we propose to formalize a type of experience feedback (accident reports) detailing the facts relating to the elements of a working situation and the events that led to an accident. In the next step, we propose two complementary approaches to redesign for safety: functional reverse engineering for safety (FRES) and functional re-engineering for safety (FR2ES). FRES is used to extract knowledge on both the accident and the design of the system involved in the accident. This approach allows assessing the safety level of the system by estimating a safety indicator depending on the type of identified risk. This indicator is used as a parameter for decision support during the redesign of the system. FR2ES defines the safety objectives related to each phase of the design in order to eliminate or reduce a given risk. The safest solutions are then obtained, on the one hand, by incorporating these safety objectives in the redesign process and, on the other hand, by using the safety indicator applied to the proposed solutions. Finally, the applicability of these approaches is demonstrated on two types of tractor-implement hitches: the power take off shaft and the three point hitch systems.

Keywords: Design for safety, experience feedback, decision support, functional reverse engineering, safety indicator, functional reengineering, tractor-implement hitches.