ESTIMATION QUANTITATIVE DES RISQUES LIÉS À L'UTILISATION D'UN SYSTÈME LORS DE SA CONCEPTION

Lama Al Bassit, Nicolas Tricot, Leyla Sadeghi, Luc Mathieu

10ème Conférence Francophone de Modélisation, Optimisation et Simulation- MOSIM'14 – 5 au 7 novembre 2014 - Nancy –France « de l'économie linéaire à l'économie circulaire»

ESTIMATION QUANTITATIVE DES RISQUES LIÉS À L'UTILISATION D'UN SYSTÈME LORS DE SA CONCEPTION

L. AL-BASSIT, N. TRICOT, L. SADEGHI

IRSTEA - 1 rue Pierre Gilles de Gennes - 92160 ANTONY Cedex
lama.albassit@irstea.fr, nicolas.tricot@irstea.fr, leyla.sadeghi@irstea.fr

L. MATHIEU

LURPA - 61 avenue du président Wilson - 94235 CACHAN Cedex
luc.mathieu@lurpa.ens-cachan.fr

RÉSUMÉ : *L'estimation des risques liés à l'utilisation d'un système peut être effectuée de manière quantitative en se basant sur des données du type statistiques d'accident. Pour un système nouveau, ces données ne sont pas disponibles. Dans ce cas, l'estimation des risques est basée sur des approches qualitatives. Dans cet article, nous proposons de la quantifier davantage. Cette estimation est basée sur des données issues de la conception du système. La gravité du dommage probable est estimée à partir des paramètres de la conception. L'estimation de la probabilité du dommage fait intervenir une mesure de la qualité de conception du système, utilisant des notions de la conception axiomatique, ainsi que d'autres facteurs liés à l'utilisateur et à l'environnement. En considérant que la valeur du risque se calcule par la multiplication de la gravité et de la probabilité du dommage, nous obtenons une estimation quantitative du risque très peu dépendante de données qualitatives comme l'avis d'experts par exemple.*

MOTS-CLÉS : *Risque, estimation de risque, analyse quantitative des risques, qualité de la conception, conception sécuritaire.*

1 INTRODUCTION

L'analyse du risque, qui est une étape du management du risque, permet principalement d'identifier les risques et de les estimer. Cette analyse des risques est souvent appliquée dans la dernière phase de la conception des systèmes avec l'objectif d'obtenir une attestation de conformité. Cette analyse permet de valoriser les actions menées par les constructeurs afin d'améliorer la sécurité de leurs nouveaux produits et de prouver le respect de la Directive Machine. Pour y parvenir, le constructeur se base généralement sur une approche qualitative dont les résultats varient selon l'appréciation des experts qui ont participé à ce processus. Plusieurs experts peuvent avoir un jugement différent sur la gravité du risque de chute d'une plateforme élevée par exemple.

Enfin, cette analyse des risques liés à un système a l'avantage de fournir une aide à la prise de décision dans le choix des solutions techniques. Elle peut être employée dans toutes les phases de la conception et même après la conception.

Tixier (Tixier et al., 2002) passe en revue 62 méthodes d'analyse des risques utilisées dans le domaine industriel qu'il classifie selon leurs entrées/sorties et sur le type d' approche mise en œuvre (qualitatives ou quantitatives, déterministes ou probabiliste). Aven (Aven, 2008) distingue trois catégories de méthodes d'analyse des risques : l'analyse des risques simplifiée, l'analyse des risques courants et l'analyse des risques basée sur un modèle.

L'analyse des risques simplifiée s'effectue par une procédure informelle, des réunions et brainstormings, et donne une estimation qualitative grossière du risque (risque faible, risque modéré ou risque élevé). L'analyse des risques courants, est une procédure formalisée et basée sur une des méthodes d'analyse de risque industriel du type HAZOP, PRA, IDAR®, etc. Dans cette catégorie de méthode d'analyse, l'estimation des risques est aussi qualitative, même si des valeurs numériques sont parfois utilisées pour exprimer les différents niveaux de risque. Les résultats de ce type d'analyse sont souvent présentés sous la forme d'une matrice (matrice des risques) qui indique le niveau de risque en fonction de la gravité du dommage probable et de la probabilité de l'occurrence de ce dommage. De nombreux travaux scientifiques se sont intéressés à l'établissement et à la quantification de la matrice des risques (Ni et al., 2010 ; Markowski, 2008 ; …). Ces auteurs proposent des extensions arithmétiques de l'approche de la matrice des risques ou encore une matrice des risques utilisant la logique floue.

La troisième catégorie, l'analyse des risques basée sur un modèle, emploie des outils comme l'arbre d'événements ou l'arbre de défaillances pour calculer et estimer le risque. Des résultats quantifiés peuvent être associés à cette analyse en accordant à chaque évènement ou défaillance de base un modèle de probabilité d'occurrence fonction du temps. Les durées de vie des composants du système en sont les données principales. Elles permettent d'estimer la probabilité d'occurrence d'un événement non désiré ou d'un dommage.

Dans cet article nous nous focalisons sur l'étape d'estimation des risques du processus d'analyse des risques et nous adoptons la définition du risque de Lowrance (Aven et al., 2011) que nous trouvons la plus proche de celle définie dans la norme (NF EN ISO

12100, 2010) : « le risque est une mesure de la probabilité et de la sévérité d'un effet néfaste », que nous appelons ici dommage. Une estimation quantitative des risques nécessite donc une estimation de la sévérité (ou gravité) du dommage probable et de la probabilité de ce dommage.

Lors de la conception d'un nouveau système les paramètres et les solutions de conception adoptés introduisent de nouvelles sources de phénomène dangereux. La variation de ces paramètres influence le niveau de risque liée à ces phénomènes.

Notre objectif est de proposer une approche d'estimation des risques basée sur des données issues de la conception du système et le moins possible sur l'avis d'experts afin de fournir une estimation quantifiée des risques liés à l'utilisation future du système.

De nombreux travaux scientifiques se sont intéressés à cette intégration de la sécurité en conception des systèmes. Nous pouvons citer notamment les travaux de (Ghemraoui, 2009) qui propose une catégorisation des risques selon les phases de la conception ainsi que les travaux de (Houssin et Gardoni, 2009) et de (Coulibaly et al., 2008) qui proposent un indicateur de sécurité basé sur les normes de sécurité mais dépendant de l'estimation d'experts.

Dans un premier temps, nous présentons dans cet article les notions relatives au risque, les éléments qui interviennent dans son estimation ainsi que les liens entre les risques et le processus de la conception. Dans un second temps, nous détaillons les arguments provenant de l'analyse de la conception qui ont conduit à notre proposition pour l'estimation des risques. Nous nous intéressons ensuite (section 3) à l'estimation de la gravité du dommage probable en nous basant sur les paramètres de conception. La section 4 s'intéresse à la probabilité d'occurrence du dommage et identifie les éléments qui la lient à la qualité de la conception du système, au profil de l'utilisateur futur et aux caractéristiques de son environnement d'évolution. La partie suivante (section 5) présente l'applicabilité et l'intérêt de la démarche proposée pour la prise de décision lors de la conception d'un système. La dernière partie (section 6) présente deux cas d'étude relatifs à deux types d'accident impliquant une machine forestière.

2 RISQUES ET PROCESSUS DE CONCEPTION

2.1 Estimation normalisée du risque

La norme (NF EN ISO 12100, 2010) considère que le risque est « *la combinaison de la probabilité d'un dommage et de la gravité de ce dommage* ». Selon cette norme la probabilité d'occurrence du dommage est fonction de trois éléments : « *l'Exposition de la ou des personnes au phénomène dangereux* », « *l'Occurrence d'un événement dangereux* » et « *la Possibilité d'éviter ou de limiter le dommage* ». Pour quantifier la probabilité d'occurrence du dommage il sera, donc, nécessaire de quantifier les trois éléments ci-dessous:

1) L'exposition au phénomène dangereux qui est fonction du temps d'exposition. Dans notre cas, nous prenons l'hypothèse que le système ne nécessite qu'un seul utilisateur pour fonctionner et nous nous intéressons à calculer le risque vis-à-vis de celui-ci. Dans le cas de co-activité (plusieurs opérateurs), l'exposition sera fonction de la somme des temps d'exposition des opérateurs.

2) L'occurrence d'un événement dangereux. Selon la norme, l'occurrence d'un événement dangereux peut être d'origine technique ou humaine.

3) La possibilité d'éviter ou de limiter le dommage. Selon la norme, cette possibilité est basée essentiellement sur l'humain, son expérience, sa conscience du risque, son habilité à réagir pour éviter le dommage, etc. L'environnement, la zone de travail et la nature d'apparition du dommage ont aussi une influence sur la possibilité d'éviter le dommage.

Les paramètres permettant la quantification de l'occurrence d'un événement dangereux ainsi que la possibilité à éviter ou à limiter le dommage sont de deux types: les facteurs techniques liés au système et les facteurs liés à l'humain et à l'environnement.

Par la suite, nous quantifions l'influence des facteurs techniques sur la probabilité d'occurrence d'un évènement dangereux en nous basant sur des données liées à la qualité de la conception du système et à sa fiabilité. L'influence des facteurs liés à l'humain et à l'environnement est liée la probabilité d'occurrence d'un évènement dangereux. Une note est ainsi attribuée à chaque profil d'utilisateur et d'environnement.

2.2 Expression mathématique du risque

L'un des résultats intéressants de l'estimation des risques est d'avoir une classification des risques. Celle-ci permet aux acteurs du projet de conception d'avoir un ordre de priorité des risques à traiter et à réduire. Une matrice des risques permet de situer chaque risque en fonction de sa gravité et sa probabilité d'occurrence et, donc, d'identifier si c'est un risque faible, modéré ou élevé (figure 1). Cette matrice convient lorsque la gravité et la probabilité d'occurrence sont données par des valeurs discrètes mais dans le cas où elles peuvent être quantifiées avec des valeurs continues une représentation graphique semble plus intéressante.

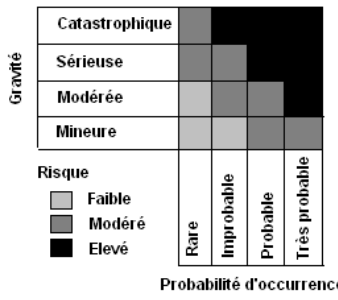


Figure 1 : Exemple d'une matrice des risques

Une des formulations mathématiques les plus utilisées pour exprimer quantitativement le risque est la suivante (Ni et al., 2010) :

Risque = gravité x probabilité d'occurrence.

Avec cette formulation, des événements ayant le même niveau de risque se retrouvent sur la même courbe hyperbolique (figure 2).

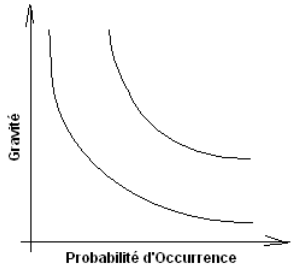


Figure 2: Représentation graphique du risque

Dans notre cas le risque, *R*, sera calculé en multipliant deux valeurs : la première exprime la gravité, *G*, du dommage et la deuxième, *P*, exprime la probabilité d'occurrence de ce dommage. Sa valeur sera donc comprise entre 0 et 1 et sera obtenue à partir de trois facteurs : *E* traduisant le niveau d'exposition au phénomène dangereux, *Q* exprimant l'influence de la qualité de la conception et *H* représentant l'influence du profil de l'utilisateur et de l'environnement. Ainsi :

$$R = G \times P \qquad avec\ P=f(E, Q, H)$$

2.3 Catégorisation des risques selon les étapes de la conception

Selon (Ghemraoui, 2009) et (Ghemraoui et al., 2009), les risques liés à l'utilisation d'un système peuvent être distingués en trois catégories. Cette catégorisation est fonction de l'étape de la conception qui a fait introduire l'origine du phénomène dangereux cause du risque. En se basant sur les étapes de la conception définies dans l'approche systématique de (Pahl et al, 2007) c'est-à-dire la conception conceptuelle, la conception architecturale et la conception détaillée, trois types de risque sont identifiés :

1) Les risques liés aux choix faits en phase de conception conceptuelle nommés par la suite « Risques d'accident ». La conception conceptuelle est l'étape qui permet de définir le concept du système et le rôle principal de l'utilisateur vis-à-vis de ce dernier. Les phénomènes dangereux introduits à ce niveau sont liés essentiellement à l'énergie (l'énergie qui alimente, qui circule dans, qui s'accumule, qui se crée par ou se dégage du système). La gravité de ces risques est très importante.

2) Les risques liés aux choix faits en phase de conception architecturale appelés « Risques ergonomiques ». La conception architecturale est l'étape qui permet de définir l'architecture du système et de dimensionner et sélectionner ses différents composants ou matériaux ainsi que de fixer ses modes et procédures d'utilisation. Les phénomènes dangereux introduits à ce niveau sont liés :

- à des dimensions et des emplacements incompatibles avec les mesures anthropométriques ;
- à des défauts d'alignement ou de dimensionnement introduisant des vibrations et des bruits ;
- à des paramètres physiques ne respectant pas les principes d'ergonomie comme des masses, des forces, des niveaux de luminosité, etc. ;
- à des choix non optimaux des composants, des matériaux ou des dimensions des pièces menant à leur usure, ou à leur détérioration ou à leur défaillance ;
- à des modes de fonctionnement incompatibles avec les capacités mentales ou physiques de l'humain.

3) Les risques liés aux choix faits en phase de conception détaillées nommés « Risques résiduels ». La conception détaillée est l'étape qui permet de finaliser la conception du système en fixant les caractéristiques non fonctionnelles des composants (dimensions, formes, propriétés de surface, matériaux, etc.) ainsi que les différentes finitions. Les origines des phénomènes dangereux introduits à ce niveau sont donc liées à ces choix de finition (présence d'arêtes vives, de surfaces rugueuses en contact avec l'utilisateur, etc.).

2.4 Lien entre risques, couplages et qualité de conception

Selon la conception axiomatique (Suh, 2001), une bonne conception assure l'indépendance entre les exigences fonctionnelles du système conçu. La conception axiomatique décrit la conception en tant que mappage entre quatre domaines : le domaine client, le domaine fonctionnel, le domaine physique et le domaine de processus. L'indépendance entre les exigences fonctionnelles se vérifie en analysant l'équation de la conception. Cette équation est une représentation mathématique du mappage entre le domaine fonctionnel, comportant les exigences fonctionnelles, et le domaine physique, comportant les paramètres de conception. Soit $\{FR\}$ le vecteur des exigences fonctionnelles et $\{DP\}$ le vecteur des paramètres de conception, l'équation de la conception s'écrit de la façon suivante :

$$\{FR\} = [A]\{DP\}$$

où $[A]$ est la matrice de conception. Une conception assurant l'indépendance des exigences fonctionnelles, donc non-couplée, correspond à une matrice de conception diagonale. Une conception ayant une matrice triangulaire est considérée acceptable et appelée une conception découplée. Dans tous les autres cas, la conception est dite couplée. Ainsi, une matrice de conception rectangulaire et ayant un nombre d'exigences fonctionnelles supérieur au nombre de paramètres de conception correspond à une conception couplée.

Certains travaux de recherche comme (Helander, 2007), (Suh, 2007), (Lo and Helander, 2007) et (Ghemraoui, 2009) insistent sur le lien entre, d'un côté, la sécurité et l'ergonomie d'un système et, de l'autre, le non couplage des exigences fonctionnelles du système. En effet, le couplage est un des aspects de complexité du système

qui rend son comportement difficilement prédictible, (Wiering and Stassen, 1993), et difficilement maîtrisable par l'utilisateur d'où le risque lié à son utilisation.
Un autre aspect qui rend le comportement du système non prévisible est lié à la défaillance du système ou de ses composants. L'amélioration de la fiabilité du système permet donc également de minimiser le risque lié à son utilisation.
De notre point de vue, une conception de bonne qualité minimise le risque. L'évaluation de la qualité de la conception fera, par conséquent, intervenir le nombre de couplages dans le système ainsi que sa durée de vie.
En projetant les problèmes de défaillance dans la matrice de conception, nous déduisons qu'une défaillance d'un composant du système peut se traduire par la non-assurance d'une des exigences fonctionnelles et donc par une augmentation du nombre de couplages. La qualité de la conception augmente donc en minimisant le nombre de couplages et en maximisant le temps avant défaillance ; défaillance augmentant de fait le nombre de couplages.

3 QUANTIFICATION DE LA GRAVITÉ DU DOMMAGE

La gravité du dommage probable causé par un système est fonction de ses paramètres physiques. Elle est proportionnelle à l'incompatibilité entre les caractéristiques humaines et les paramètres physiques du système. La gravité d'un risque de chute d'une plateforme élevée est fonction de la hauteur de chute, donc de l'énergie cinétique du corps lors de l'impact. La gravité d'un risque du au bruit est proportionnelle au niveau de bruit ou au rapport entre le niveau de bruit et le niveau seuil supporté par l'humain.
D'autres facteurs peuvent également influencer la gravité mais ceux-ci sont souvent liés à l'humain ou à l'environnement. Dans l'exemple de la chute d'une plateforme, l'état de santé de la personne et la nature du sol où l'impact aura lieu auront une influence sur la gravité du dommage.
Cependant, nous cherchons ici à quantifier l'apport du système dans la détermination du niveau de la gravité.
Pour y parvenir, nous avons besoin d'identifier le paramètre physique en lien avec le risque et sa valeur maximale, p_{Sys}, ainsi que la valeur seuil de ce paramètre supportée par l'humain, p_{seuil}.
L'expression mathématique adoptée pour calculer la gravité donne une valeur adimensionnelle qui vaut 0 lorsque p_{Sys} est égale ou inférieure à p_{seuil} et qui augmente avec l'augmentation du rapport p_{Sys}/p_{seuil} :

$$G = \begin{cases} \dfrac{\left| p_{Sys} - p_{seuil} \right|}{p_{seuil}} & Si\ p_{Sys} \geq p_{seuil} \\ 0 & Si\ p_{Sys} < p_{seuil} \end{cases}$$

Pour un risque d'accident (voir §2.3), l'énergie a été identifiée comme le paramètre physique du système entrainant le dommage. Pour les risques liés au manque d'ergonomie, ce paramètre peut être une dimension (liée à un poste de travail, par exemple), un niveau de bruit, de luminosité, de concentration de poussière, etc. Pour un risque d'usage, le paramètre du système en lien avec le risque peut être une contrainte, une rugosité, etc. Les valeurs seuils supportées par l'humain concernant les risques liés à l'ergonomie sont disponibles dans les normes de sécurité (l'EN 1005-3 donne les limites des forces recommandées pour l'utilisation des machines, l'EN ISO 11064-4 s'intéresse à l'agencement et au dimensionnement du poste de travail, l'ISO 8995-1 : 2002 donne les exigences d'éclairage pour les lieux de travail, …) mais pas les valeurs seuils des différents types d'énergie supportée par l'humain ni les valeurs seuils des paramètres liés au risques d'usage. Cependant, certaines études réalisées en biomécanique s'intéressent à ces aspects, comme par exemple (LaPlaca et al., 2007) qui propose un modèle des lésions cérébrales en fonction de la charge mécanique causant le dommage ou encore (Kleiven, 2007) qui s'intéresse aux critères de blessure à la tête et à l'influence de la vitesse et de l'accélération.
Dans le cas des risques liés au manque d'ergonomie, et contrairement aux risques d'accident, la durée de l'exposition au phénomène dangereux peut influencer le niveau de gravité du dommage. Ce facteur sera pris en compte lors de la quantification de la probabilité d'occurrence et donc de manière indirecte dans la quantification du risque.

4 PROBABILITÉ D'OCCURRENCE DU DOMMAGE ET ANALYSE DE LA CONCEPTION

Comme nous avons déjà vu dans la partie 2.2, la probabilité d'occurrence du dommage sera déterminée en fonction de l'exposition au phénomène dangereux, de la qualité de la conception et du profil de l'utilisateur et de l'environnement.
Nous remarquons ici que l'influence de l'exposition sur la probabilité d'occurrence de l'événement dangereux, n'est pas de même nature que l'influence de la qualité de la conception ou de l'humain et de l'environnement. Effectivement, un temps d'exposition nul élimine la probabilité d'occurrence du dommage mais une bonne conception ou un type d'utilisateur particulier (formé et expérimenté) ne fait que la minimiser.

4.1 Exposition au phénomène dangereux

Nous exprimons l'influence de l'exposition au phénomène dangereux sur la probabilité d'occurrence de dommage par le facteur *E* qui donne le rapport entre le temps d'exposition prévu au phénomène dangereux pendant un cycle de travail, t_{exp}, et la durée de ce cycle t_{cycle} :

$$E = \frac{t_{\exp}}{t_{cycle}}$$

Le facteur *E* exprime la probabilité d'exposition au phénomène dangereux. Il peut varier entre 0 et 1. La valeur 0 correspond à un temps d'exposition nul et donc à une probabilité d'exposition nulle.
Le cycle de travail à prendre en compte varie selon la phase à risque dans l'utilisation du système. Pour un risque identifié en phase d'utilisation normale, la durée du cycle peut correspondre au nombre d'heures de travail quotidien sur la machine. Pour un risque identifié en phase de maintenance par exemple, la durée du cycle peut correspondre à la durée totale de la phase de maintenance.
Le temps d'exposition au phénomène dangereux pour un système en conception est une valeur qui sera estimée en se basant sur la conception proposée et sur la mesure du temps de réalisation des tâches similaires sur des systèmes existants.

4.2 Probabilité d'occurrence du dommage et qualité de la conception

Comme présenté dans la partie 2.3, la probabilité d'occurrence du dommage lors de l'utilisation du système augmente avec la diminution de la qualité de la conception du système. Nous considérons qu'un système dont la conception est de bonne qualité est un système ne comportant pas de couplage dans sa matrice de conception et est un système fiable (durée de vie maximale).
Pour prendre en compte les deux points précédents, nous définissons les deux facteurs C et F. C donne le niveau de couplage dans le système et F donne le niveau de non fiabilité du système ou sa probabilité de défaillance.

4.2.1 Niveau de couplage dans le système

Une analyse d'un système existant ou faite durant sa conception permet d'établir son équation de conception et donc sa matrice de conception. Dans le cas où cette matrice est diagonale ou triangulaire, le niveau de couplage dans le système, *C*, est considéré nul. Dans le cas contraire, le niveau de couplage se calcule grâce au nombre de cellules de la matrice montrant des couplages, $N_{couplages}$, et au nombre d'exigences fonctionnelles identifiées, n_{FR}. Une cellule de la matrice de conception montre un couplage dans deux cas :

- si elle n'est pas sur la diagonale principale de la matrice et différente de zéro, ou
- si elle est à la fois sur la diagonale principale de la matrice et égale à zéro. Le niveau de couplage sera donné par la relation suivante :

$$C = \begin{cases} 0 & Si\ [A]\ triangulaire \\ \dfrac{N_{couplages}}{(n_{FR})^2} & Si\ non \end{cases}$$

Avec cette expression le niveau de couplage du système prend des valeurs comprises entre 0, pour une conception non couplée ou découplée et 1 pour une conception ayant un maximum de couplages.

4.2.2 Probabilité de défaillance du système

Nous considérons que le niveau de fiabilité du système se détermine par le rapport entre la durée de vie avant défaillance du système ou de la partie du système responsable du risque, d_{Sys}, et la durée de vie maximale du système fixé dans son cahier des charges, d_{Max}. *F* sera donc donné par l'expression suivante :

$$F = \begin{cases} 0 & Si\ d_{Sys} \geq d_{Max} \\ 1 - \dfrac{d_{Sys}}{d_{Max}} & Si\ d_{Sys} < d_{Max} \end{cases}$$

F peut varier de 0 pour une défaillance improbable pendant la durée de vie du système à 1 pour un système défaillant dès le premier instant de son utilisation.
La durée de vie avant défaillance d'un nouveau système sera estimée à partir des connaissances sur les durées de vie des composants, des pièces et solutions de conception déjà utilisés dans des systèmes existants.

4.2.3 Qualité de la conception

Une mauvaise qualité de conception est donc liée à la présence de couplages ou de défaillances dans le système. La probabilité d'une mauvaise qualité de conception, *Q*, sera donnée par l'expression suivante :

$$Q = C + F - C \times F$$

La valeur de *Q* est comprise entre 0, pour une conception de bonne qualité, fiable et ne présentant pas de couplages, et 1, pour une conception de mauvaise qualité due à la présence d'un nombre maximal de couplages (*C=1)* ou à un système défaillant (*F=1)*.

4.3 Profil de l'utilisateur et probabilité d'occurrence du dommage

Les « qualités » de l'utilisateur (son expérience, sa formation quant à l'utilisation du système et aux risques liés à son utilisation, ses capacités physiques, sa rapidité de réaction, …) jouent un rôle positif dans la minimisation de la probabilité d'occurrence du dommage ou dans l'évitement de ce dommage. L'environnement peut également influencer la probabilité d'occurrence du dommage. Un environnement présentant des événements ou des variations non prévisibles ou non maîtrisables augmente la probabilité d'occurrence du dommage (présence d'obstacles imprévisibles devant un système mobile ou variations non contrôlables dans la luminosité influençant le niveau de visibilité de l'utilisateur par exemple).
Les paramètres liés à l'humain et à l'environnement pouvant influencer la probabilité d'occurrence du dom-

mage sont très nombreux. Nous proposons de simplifier ces paramètres en considérant des profils d'utilisateur et d'environnement. Ces profils sont, en général, prévus dans le cahier des charges du système lors de la conception.

Nous identifions trois types d'utilisateur :

- L'utilisateur professionnel ayant des connaissances techniques et une expérience technique ;
- L'utilisateur non professionnel représentant la majorité des utilisateurs adultes n'ayant pas suivi de formation sur l'utilisation du système ;
- L'utilisateur aux capacités limitées regroupant les utilisateurs incapables physiquement d'utiliser le système.

Nous proposons de pondérer ces profils selon leur influence sur la probabilité d'occurrence du dommage. Ainsi, nous attribuons 0,25 à un utilisateur professionnel, 0,5 à un utilisateur non professionnel et 0,75 à un utilisateur aux capacités limitées.

Concernant l'environnement, nous identifions deux types d'environnement que nous appelons :

- Environnement parfait où tous les événements et les variations dans cet environnement sont prévisibles et contrôlables. Cela peut être le cas d'un milieu fermé où tous les paramètres (luminosité, température, humidité, présence potentielle d'objet, présence potentielle d'autres personnes, etc.) sont prévisibles et contrôlables. Nous attribuons à cet environnement la valeur 0.

- Environnement difficile où les événements et les variations sont non prévisibles et non contrôlables. Cela peut être le cas d'un environnement naturel par exemple. Nous attribuons à cet environnement la valeur 1.

Soit h_u la valeur attribuée au paramètre lié à l'utilisateur et *he* la valeur du paramètre lié l'environnement. L'influence de ces deux éléments, utilisateur et environnement, sur la probabilité d'occurrence du dommage, *H*, sera donnée par l'équation suivante :

$$H = h_u + h_e - h_u \times h_e$$

La valeur de *H* est de 1 si l'environnement est difficile. Elle est au minimum de 0,25 lorsque l'utilisateur est professionnel et que l'environnement est parfait.

5 CALCUL DU RISQUE ET PRISE DE DÉCISION

La probabilité d'occurrence du dommage, *P*, est fonction des trois valeurs obtenues correspondantes à l'exposition *E*, la qualité de conception *Q* et le profil de l'utilisateur et le type d'environnement *H*. Comme nous avons déjà signalé, la probabilité du dommage peut être éliminée en annulant le temps d'exposition au phénomène dangereux (*E=0)* mais l'amélioration de la qualité de la conception, ou le changement de profil des utilisateurs seul ne suffisent pas à éliminer la probabilité de l'accident. Par conséquent, nous exprimons la probabilité d'occurrence du dommage par l'équation suivante :

$$P = E \times \left(Q + H - Q \times H\right)$$

La probabilité d'occurrence du dommage, *P*, varie entre 0, pour une exposition nulle, et 1, pour une exposition permanente, avec un système dont la qualité de conception est mauvaise et évoluant dans un environnement difficile.

Finalement, il suffit de reprendre l'équation liant *R*, *G* et *P* pour calculer le risque, *R* :

$$R = G \times P$$

La quantification des risques liés à l'utilisation d'un système permet, d'une part, de classifier ces risques, d'identifier les risques les plus importants et de choisir quels risques traiter en premier lieu. D'autre part, la quantification de l'ensemble des risques permet de déterminer le rang du système et de juger sa réponse, ou satisfaction, à une exigence fonctionnelle liée à la sécurité. Elle permet ainsi de comparer deux systèmes ou deux solutions de conception entre elles afin de déterminer la plus sécuritaire. Elle permet enfin d'identifier, lors de la conception du système, les paramètres physiques à optimiser pour rendre la conception plus sécuritaire.

6 CAS D'ÉTUDE : CALCUL DU RISQUE LIÉ À LA DÉCHIQUETEUSE FORESTIÈRE

L'application choisie pour la validation de notre proposition concerne l'estimation de risques liés à l'utilisation d'une déchiqueteuse forestière. Les déchiqueteuses forestières (figure 3), aussi appelés broyeurs-déchiqueteuses de branches, sont des machines utilisées pour réduire le volume du bois provenant des opérations d'élagage d'arbres et arbustes. Elles déchiquettent ces végétaux et les transforment en petits morceaux pour être composté ou utilisé comme une source d'énergie (plaquettes forestières). De nombreux phénomènes dangereux liés à l'utilisation de ce type de machines ont été identifiés suite à l'étude de rapports d'accident, à des rencontres et discussion avec des utilisateurs et à l'observation de la machine en situation de travail.

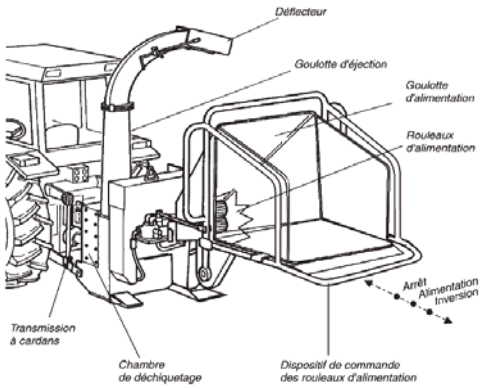


Figure 3: Principaux composants de la déchiqueteuse forestière [source: fiche sécurité machines agricoles et forestières -Irstea]

Une analyse de la conception de la machine a été réalisée (Al Bassit and Tricot, 2013). Elle a permis d'établir l'équation de la conception de cette machine et d'identifier les principaux couplages entre ses fonctionnalités.
Les phénomènes dangereux liés à l'utilisation de cette machine sont variés: le happement par les rouleaux d'alimentation, une coupure par le rotor de déchiquetage, une projection de coupeaux de bois venant de la chambre de déchiquetage, des dommages auditifs dus au bruit de la machine, des postures dangereuses dues à la hauteur de la goulotte, l'exposition aux poussières de bois, des blessures aux mains et aux doigts lors du changement des couteaux, etc.
Dans la suite, nous avons sélectionné deux de ces phénomènes dangereux pour appliquer la démarche d'estimation quantitative du risque.

6.1 Happement par les rouleaux d'alimentation

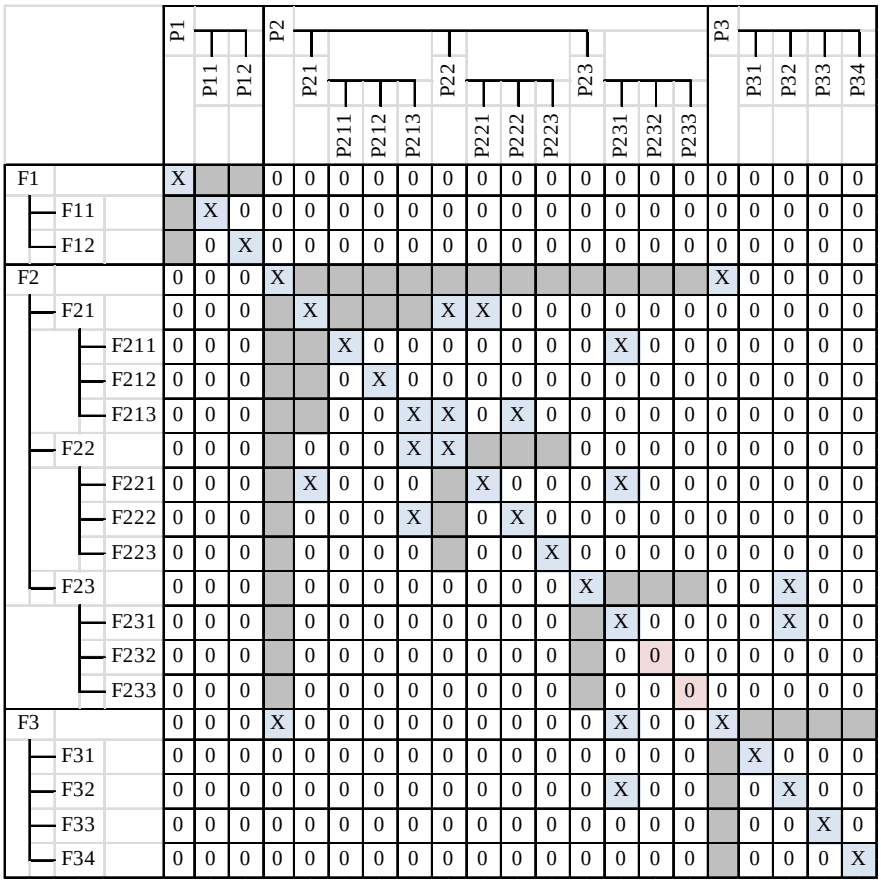
Le happement par les rouleaux d'alimentation correspond à l'accident grave type lié à l'utilisation de ces machines. Il est généralement suivi par des coupures par les lames du rotor de déchiquetage.

Gravité du dommage probable
Le paramètre du système en lien avec le risque de happement, est l'énergie (ou la puissance) des rouleaux d'alimentation. Il est donc nécessaire de connaitre la valeur numérique de la puissance des rouleaux et d'avoir la puissance maximale supportée par l'humain n'entrainant pas son happement. Pour notre application nous adopterons une valeur estimée de manière approximative. Des essais sur mannequins permettraient d'obtenir cette puissance seuil supporté par l'humain.
La vitesse linéaire d'un point de la surface du rouleau d'alimentation de la déchiqueteuse étudiée est de 1,15 m/s. La puissance du rouleau est 10 fois moins importante que la puissance moteur. Selon le constructeur, la puissance du moteur de notre déchiqueteuse est de 20 kW. La puissance au niveau des rouleaux est donc de 2 kW et la force de traction du rouleau est de 1739,1 N. Nous estimons que la puissance seuil supportée par l'humain correspond à une force de traction de 100 N allant à une vitesse de 0,2 m/s donc de 20W. Ces résultats numériques nous permettent de déterminer que $p_{sys}/p_{seuil} = 100$ et donc que la valeur de la gravité sera : $G = (p_{sys}-p_{seuil})/p_{seuil} = 99$.

Probabilité d'occurrence du dommage
- Exposition : le risque de happement est identifié en phase d'alimentation de la machine. Pendant un chantier d'élagage de 8 heures, la déchiqueteuse fonctionne pendant moins de 3 heures. Nous estimons que le temps total de présence de l'utilisateur en face du système d'alimentation en fonctionnement est de 1/10 du temps de fonctionnement du système. Donc l'exposition vaut $E = 0,1$.
- Qualité de conception
La matrice de conception obtenue suite à l'analyse de la conception du système (figure 4) présente 17 couplages pour 21 exigences fonctionnelles. Le niveau de couplage est par conséquent : $C = 17/(21)^2 = 0,038$.
La durée de vie maximale d'une déchiqueteuse est de 10 à 12 ans selon le cahier des charges de ces machines. La durée de vie du système d'alimentation de notre déchiqueteuse qui est constituée essentiellement de pièces mécaniques et motorisés par un moteur hydraulique est équivalente à la durée de vie maximale. Le système étudié est donc considéré fiable et $F = 0$.
La probabilité d'une mauvaise qualité de conception est donc de $Q = C+F- C.F = 0,038$.
- Influence de l'environnement et de l'utilisateur sur la probabilité d'occurrence du dommage
L'utilisation d'une déchiqueteuse forestière nécessite une formation préalable. De plus, ces machines sont destinées à des professionnels. Les déchiqueteuses fonctionnent dans des milieux ouverts où aucun contrôle des paramètres ambiants (humidité, température, etc.) n'est possible. L'influence du profil de l'utilisateur et le type d'environnement sera donc :
$H = h_u + h_e - h_u.h_e = 0,25+1-(0,25x1) = 1$.

La probabilité d'occurrence du dommage sera donc :
$P = E.(Q+H-Q.H) = 0,1$.

La valeur numérique attribuée au risque de happement par les rouleaux d'alimentation sera donc $R = G \times P = 9,9$.



	P1	P11	P12	P2	P21	P211	P212	P213	P22	P221	P222	P223	P23	P231	P232	P233	P3	P31	P32	P33	P34
F1	X			0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F11		X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F12		0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F2	0	0	0	X													X	0	0	0	0
F21	0	0	0		X				X	X	0	0	0	0	0	0	0	0	0	0	0
F211	0	0	0			X	0	0	0	0	0	0	0	X	0	0	0	0	0	0	0
F212	0	0	0			0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F213	0	0	0			0	0	X	X	0	X	0	0	0	0	0	0	0	0	0	0
F22	0	0	0		0	0	0	X	X				0	0	0	0	0	0	0	0	0
F221	0	0	0		X	0	0	0		X	0	0	0	X	0	0	0	0	0	0	0
F222	0	0	0		0	0	0	X		0	X	0	0	0	0	0	0	0	0	0	0
F223	0	0	0		0	0	0	0		0	0	X	0	0	0	0	0	0	0	0	0
F23	0	0	0		0	0	0	0	0	0	0	0	X				0	0	X	0	0
F231	0	0	0		0	0	0	0	0	0	0	0		X	0	0	0	0	X	0	0
F232	0	0	0		0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0
F233	0	0	0		0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0
F3	0	0	0	X	0	0	0	0	0	0	0	0	0	X	0	0	X				
F31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		X	0	0	0
F32	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0		0	X	0	0
F33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	X	0
F34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	X

Figure 4: Aperçu de la matrice de conception d'une déchiqueteuse forestière

6.2 Postures dangereuses dues à la hauteur de la goulotte

Manipuler des branches posées au sol pour les disposer dans la goulotte d'alimentation de la machine est une activité entrainant rapidement des TMS (Troubles Musculo-Squelettiques).

Gravité du dommage

L'opérateur alimentant la déchiqueteuse est amené à soulever et à déplacer des branches et des troncs qui peuvent peser plus de 50 kg. Avoir une goulotte d'alimentation à hauteur de la hanche, au niveau où l'opérateur bloque les branches qu'il manipule rend le travail plus ergonomique. La norme sur l'ergonomie NF X35-109 : 2011, intitulé « *manutention manuelle de charge pour soulever, déplacer et pousser/tirer »*, définit une hauteur de chargement de 0,75 m à 1,10 m comme condition acceptable pour la position des mains de l'opérateur lors de la prise/dépose d'une charge. Pour une déchiqueteuse ayant une goulotte de 0,4 m de hauteur, le risque sur l'opérateur lié à l'utilisation de cette déchiqueteuse sera quantifié avec la démarche proposée.
G = (0,75-0,4) / 0,75 = 0,47

Probabilité d'occurrence du dommage

- Exposition : la durée de pose des branches dans la goulotte est considérée égale à 1 seconde. La fréquence de la pose de branches dans la goulotte est estimée à 2 fois par minute pour une durée totale de déchiquetage de 2 heures. D'où l'exposition vaut :
E = (1x120x2) / (2x3600) = 0,033.
- Qualité de la conception et Influence de l'environnement et de l'utilisateur sur la probabilité d'occurrence du dommage
Ces deux facteurs sont identiques à l'exemple précédant.
La valeur de la probabilité d'occurrence du dommage sera donc P = 0,025.
La valeur du risque sera égale à :
$R = G$ x P = 0,011.

Ces résultats montrent donc que le risque lié aux postures dangereuses est bien inférieur au risque de happement. Il en est de même pour sa gravité qui est bien inférieure pour le risque lié aux postures dangereuses.

6.3 Happement par les rouleaux d'alimentation pour une solution de conception alternative

Le happement par les rouleaux d'alimentation a été identifié comme entrainant un risque élevé pour l'opérateur. Des solutions de conception ont été proposées pour éliminer ou réduire ce risque. L'un des principes de solution proposés consiste à rajouter dans la goulotte d'alimentation un système de tapis ameneur combiné à un rouleau presseur permettant d'assurer l'amenage des branches jusqu'aux rouleaux d'alimentation (Figure 5). Ce principe permet de dissocier les phases d'amenage des branchages et de déchiquetage. La phase d'amenage

se fait rouleau d'alimentation à l'arrêt et rouleau presseur en position haute. La phase de déchiquetage est déclenchée par l'opérateur en utilisant une commande à action maintenue. Il met ainsi en marche le convoyeur et le rouleau d'alimentation ; le rouleau presseur étant en appui sur les branches.

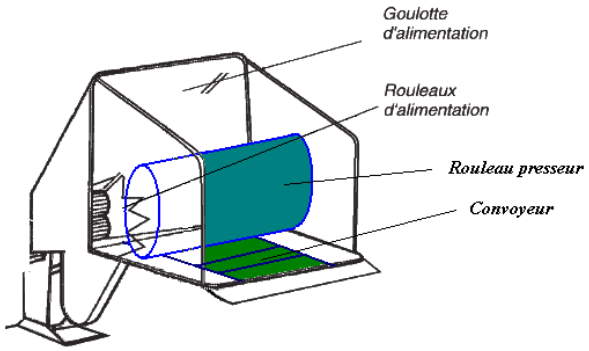


Figure 5: Solution de conception d'une déchiqueteuse à convoyeur et rouleau presseur

Gravité du dommage

Par rapport à la machine actuelle (voir §6.1) L'estimation de la gravité du happement par les rouleaux d'alimentation ne change pas, donc G=99.

Probabilité d'occurrence du dommage

- Exposition : grâce à ce principe de solution, l'opérateur n'est plus exposé aux rouleaux d'alimentation en rotation. En phase de chargement les rouleaux sont à l'arrêt et en phase de déchiquetage l'opérateur se trouve dans une zone de sécurité. Le temps d'exposition est donc nul *E=0*

- Qualité de la conception :

La matrice de conception de cette nouvelle conception présente 18 couplages pour 24 exigences fonctionnelles. Par conséquent, le niveau de couplage est : $C=n/m^2=0.031$

Concernant la fiabilité, nous considérons que l'ajout d'un convoyeur actionné par un moteur hydraulique, d'un rouleau presseur et de vérins hydrauliques n'entraîne pas que la durée de vie du système devienne inférieure à la durée de vie maximale définie dans le cahier des charges, donc F=0.

La probabilité d'une mauvaise qualité de conception est donc de Q=C+F-C.F=0.031.

- Influence de l'environnement et de l'utilisateur sur la probabilité d'occurrence du dommage.

Avec cette solution, leur influence est identique (voir §6.1), donc *H=1*.

La probabilité d'occurrence du dommage pour ce principe de solution sera *P=E. (Q+H-Q.H)=0*.

En conséquence, la valeur numérique attribuée au risque de happement par les rouleaux d'alimentation sera nulle : *R=GxP=0.*

La solution de conception proposée permet donc d'éliminer le risque de happement par les rouleaux d'alimentation.

7 CONCLUSION

Dans cet article, nous proposons une démarche d'estimation quantitative du risque lié à l'utilisation d'un système. Cette démarche fait intervenir des éléments de la conception pour la quantification du risque. La gravité du dommage probable correspond à l'incompatibilité entre les paramètres du système et les caractéristiques de l'humain. Cette incompatibilité se détermine par le rapport entre la valeur du paramètre du système en lien avec le phénomène dangereux et une valeur seuil supportée par l'humain du paramètre correspondant. La probabilité d'occurrence du dommage fait intervenir une mesure de la qualité de conception du système. La qualité de conception du système est fonction du niveau de couplage du système ainsi que de sa fiabilité.

La démarche proposée permet d'évaluer les risques et de les classer. Il permet également de donner au concepteur des éléments-clés pour l'améliorer la sécurité en phase de conception. La principale critique pouvant être faite à la méthode proposée est que l'estimation quantitative du risque reste dépendante de l'avis d'experts, notamment en ce qui concerne l'estimation du temps d'exposition au phénomène dangereux. Notre objectif futur est de proposer une quantification du risque objective s'affranchissant totalement de l'avis d'experts.

REFERENCES

Al Bassit, L. and N. Tricot, 2013. *Amélioration de la sécurité de la déchiqueteuse forestière*, Rapport d'étude, Irstea.

Aven, T., 2008. *Risk Analysis: Assessing Uncertainties beyond Expected Values and Probabilities*, Wiley.

Aven, T., O. Renn and E. A. Rosa, 2011. On the ontological status of the concept of risk, *Safety Science*, 49, p. 1074-1079.

Coulibaly, A., R. Houssin, B. Mutel, 2008. Maintainability and safety indicators at design stage for mechanical products, *Computer in Industry*, 59, p. 438-449.

Ghemraoui, R., L. Mathieu and N. Tricot, 2009. Design method for systematic safety integration, *CIRP Annals – Manufacturing Technology*, 58, p. 161-164.

Ghemraoui, 2009. *Méthodologie de conception innovante integrant la sécurité des utilisateurs: application aux liaisons tracteur-outils*, Thèse de doctorat, ENS Cachan.

Helander, M., 2007. Using design equations to identify sources of complexity in human-machine interaction, *Theoretical Issues in Ergonomics Science*, 8 (2), p. 123-146.

Houssin, R. and M. Gardoni, 2009. Software Framework for the Approach: Computer Aided Safety Integration in Design Process (CASID), Journal of Advanced Manufacturing Systems, 08(01), P. 27-45.

Kleiven, S., 2007. A parametric study of energy absorbing foams for head injury prevention. *Proc.*

ESV 2007, 20th Enhanced Safety of Vehicles Conference, France

LaPlaca, M.C., C.M. Simon, G.R. Prado and D.K. Cullen, 2007. CNS injury biomechanics and experimental models, *Progress in Brain Research*, (161), Weber &Maas (Eds.), P. 13-26.

Lo, S. and M. Helander, 2007. Use of axiomatic design principles for analysing the complexity of human-machine systems, *Theoretical Issues in Ergonomics Science*, 8(2), P. 147-169.

Markowski, A. S. and M. S. Mannan, 2008. Fuzzy risk matrix, *Journal of Hazardous Materials*, 159, p. 152-157.

Melvin, J.W. and H.V. Deo, 2002. Axiomatically Designed Robustness, *American Supplier Institute 19th Annual Taguchi Methods Symposium*, San Diego, CA.

NF EN ISO 12100, 2010. *Sécurité des machines : Principes généraux de conception – Appréciation du risque et réduction du risque*. AFNOR.

NF X35-109, 2011. *Manutention manuelle de charge pour soulever, déplacer et pousser/tirer*. AFNOR.

Ni, H., A. Chen and N. Chen, 2010. Some extentions on risk matrix approach, *Safety Science*, 48, p. 1269-1278.

Pahl, G., W. Beitz, J. Feldhusen and K.-H. Grote, 2007, *Engineering Design : A Systematic Approach*, Springer.

Suh, N.P., 2001. *Axiomatic Design : Advances and Applications*, Oxford University Press.

Suh, N.P., 2007. Ergonomics, axiomatic design and complexity theory, *Theoretical issues in ergonomics*, 8(2), p. 101-121.

Tixier, J., G. Dusserre, O. Salvi and D. Gaston, 2002. Review of 62 risk analysis methodologies of industrial plants, *Jornal of Loss Prevention in the Process Industries*, 15, p. 291-303.

Wieringa, P.A. and H.G. Stassen, 1993. Assessment of complexity, *Verification and Validation of Complex Systems : Human Factors Issues*, J.A. Wise, V.D. Hopkin and P. Stager (Eds.), p. 173-180. Springer-Verlag.