



HAL
open science

Analyse de Risques en Robotique: Apports de la Conscience de Situation

Charles Fage, Jean-Marc Salotti

► **To cite this version:**

Charles Fage, Jean-Marc Salotti. Analyse de Risques en Robotique: Apports de la Conscience de Situation. SELF 2021 - 55ème congrès de la Société d'Ergonomie de Langue Française, Jan 2021, Paris / Virtuelle, France. hal-03117894

HAL Id: hal-03117894

<https://inria.hal.science/hal-03117894>

Submitted on 21 Jan 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Analyse de Risques en Robotique : Apports de la Conscience de Situation

Fage, Charles¹² ; Salotti, Jean-Marc¹²

¹École Nationale Supérieure de Cognitique (ENSC), Bordeaux INP
109 Avenue Roul, 33405 TALENCE Cedex

²Équipe-projet Auctus, Centre Inria Bordeaux Sud-Ouest
200 Avenue de la Vieille Tour, 33405 TALENCE Cedex
charles.fage@inria.fr

Résumé. Bien que des normes de conception strictes existent en robotique, l'utilisation des robots dans l'industrie conduit à des accidents impliquant des opérateurs, parfois mortellement. Pour y remédier, nous proposons une nouvelle méthode d'analyse de risques en robotique basée sur le modèle de conscience de situation d'Endsley, et les causes potentielles de son altération appelées « démons ». Une catégorisation des accidents en environnement industriel (base de données INRS) a permis d'identifier l'implication de 3 principaux démons du modèle d'Endsley dans 90% des accidents répertoriés (N=44) : « *tunnélisation de l'attention* », « *représentation mentale erronée* » et « *hors de la boucle* ». Un réseau bayésien est utilisé afin de déterminer des probabilités de risques liés à l'implication de ces démons. En complément, des recommandations spécifiques sont formulées afin d'améliorer la conscience de situation des opérateurs mais également des robots afin de réduire les risques d'accident.

Mots-clés : évaluation du risque ; conscience de situation ; erreur humaine ; robotique

Risks Analysis in Robotics: Insights from Situation Awareness

Abstract. Although strict design standards have been developed for robotics, using robots within industrial environments leads to accidents involving operators, sometimes resulting in fatalities. In order to address this situation, this paper proposes a new risk analysis method for robotics based on the Endsley's situation awareness model, and its demons impeding the situation awareness. Categorizing accidents with robots in industrial environments (INRS database) lead to identifying that 3 specific demons are involved in 90% of reported accidents (N=44): "out-of-the-loop", "errant mental model" and "attentional tunneling". A Bayesian network is used to determine risks probabilities. In addition, specific recommendations are made to improve situation awareness and reduce the risks.

Keywords: risk assessment; situation awareness; human error; robotics

*Ce texte original a été produit dans le cadre du congrès de la Société d'Ergonomie de Langue Française qui s'est tenu à Paris, les 16, 17 et 18 septembre 2020. Il est permis d'en faire une copie papier ou digitale pour un usage pédagogique ou universitaire, en citant la source exacte du document, qui est la suivante :

Fage, C., Salotti, JM. (2020). Analyse de risques en robotique : apports de la conscience de situation. Actes du 55ème Congrès de la SELF, L'activité et ses frontières. Penser et agir sur les transformations de nos sociétés. Paris, 16, 17 et 18 septembre 2020

Aucun usage commercial ne peut en être fait sans l'accord des éditeurs ou archiveurs électroniques. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page.

INTRODUCTION

Les standards de sécurité en robotique fournissent des spécifications strictes pour la conception et l'utilisation de robots en environnement industriel (12,13). Par ailleurs, d'autres standards robotiques ont été développés, et notamment pour prendre en compte les interactions physiques homme-robot (pHRI) (14,15). Cependant, malgré les efforts importants pour améliorer la sécurité des opérateurs, de nombreux accidents sont toujours recensés dans les bases de données, souvent liés à des erreurs humaines (11). Dans la plupart des situations, les robots n'étaient pas conçus pour fonctionner en collaboration étroite avec un opérateur humain, mais une interaction n'était pas requise pour régler le problème inattendu.

Plusieurs méthodes d'analyse de la fiabilité humaine ont été proposées pour analyser les causes et conséquences des erreurs humaines, en robotique mais aussi dans d'autres domaines, tels que l'aéronautique, dans lesquels les interactions système-opérateur sont très importantes (4,5,6,9,17). Ces méthodes, basées par exemple sur des méthodologies HFACS (Human Factors Analysis and Classification System - 4) ou sur un modèle computationnel (17), permettent de quantifier des probabilités d'erreurs humaines et fournissent donc une évaluation de ces probabilités (ou Probability Risk Assessment – PRA). Néanmoins, comme la plupart des accidents surviennent dans un contexte spécifique avec différents outils et différents postes de travail, il est difficile de généraliser les causes de l'accident et fournir des recommandations utiles pour la conception et les scénarios d'utilisation de nouveaux systèmes (2). Dans le domaine des interactions homme-robot cognitives, de nombreuses études soulignent le manque de référentiel commun et des représentations partagées entre l'opérateur et le robot (3,24). Ces facteurs contribuent à une dégradation du niveau de conscience de situation (Situation Awareness – SA) ; la SA est un élément critique dans la réduction des risques (6,7,18,20,23). Pour déterminer une PRA, nous proposons ici d'analyser tous les accidents impliquant un robot dans la base de données INRS en termes de facteurs de SA et estimer les probabilités de risques en fonction du potentiel impact de ces facteurs, comme suggéré dans une précédente étude dans le domaine de l'aéronautique (21). Endsley propose un modèle général de SA, en lui associant 8 grands types d'altération - communément appelés « démons » - qui peuvent être utilisés pour analyser ces accidents (6).

Ce modèle est présenté dans la Section 2 du document. Quarante-deux accidents robotiques ont été extraits de la base de données INRS. Parmi ces 42 accidents, 3 ont été retenus pour être analysés et discutés en détails en Section 3 du document avec une attention particulière portée sur la présence et la nature des démons impactant la SA. L'intégralité de la base est ensuite analysée : les résultats statistiques sont rapportés. La Section 4 présente la méthode PRA : les probabilités conditionnelles peuvent être estimées dans le but de construire un réseau Bayésien, qui représente un outil standard de la PRA (1,9,10,17,19). En conclusion, nous proposons des perspectives de recherche ainsi que des recommandations pratiques.

MODÈLE DE CONSCIENCE DE SITUATION

Selon Endsley, la SA est définie comme la perception des éléments dans l'environnement et des événements par rapport au temps et à l'espace, la compréhension de leur sens, et la projection de leur statut futur (6). Dans ce modèle, huit facteurs potentiels de détérioration de la SA sont définis : il s'agit des démons du modèle, appelés dans ce papier démons de SA (6,7).

1. Une erreur de « **tunnélisation de l'attention** » (ou *attentional tunnelling*) est observée quand un opérateur présente une focalisation importante de son attention sur un problème spécifique, qui s'accompagne d'une faible attention pour les autres paramètres importants qui doivent être pris en compte pour que la tâche soit accomplie avec succès.
2. Un « **modèle mental erroné** » (ou *errant mental model*) peut être la cause d'une erreur humaine lorsque l'opérateur a une mauvaise interprétation de la situation courante du fait d'inférences inappropriées par rapport à ses observations.
3. Une erreur « **hors de la boucle** » (ou *out-of-the-loop*) se présente lorsqu'un système autonome conduit une tâche complexe et redonne soudainement le contrôle à l'opérateur, qui ne suivait pas la tâche et donc incapable d'en connaître le statut courant.
4. Une erreur de « **complexité** » (ou *complexity creep*) est observée lorsqu'un problème survient et qu'un nombre trop grand de systèmes sont impliqués, de telle sorte que l'opérateur n'est pas en capacité de comprendre la situation et donc de trouver une solution.
5. Une « **saillance mal-placée** » (ou *misplaced saliency*) peut être observée si l'interface du système est conçue pour maximiser la perception et l'attention de l'opérateur sur un dispositif particulier, alors même que son attention devrait être portée sur d'autres dispositifs ou appareils.
6. Une « **overdose de données** » (ou *data overload*) survient lorsqu'un trop grand nombre d'informations doit être géré – dans leur réglage ou leur prise en compte – dans un contexte nécessitant une grande attention ou des contraintes temporelles fortes.
7. Un « **piège de mémoire requise** » (ou *requisite memory trap*) se présente lorsque de trop nombreuses sous-tâches doivent être effectuées par l'opérateur et que celui-ci en oublie une.
8. Une « **charge mentale, anxiété, fatigue et stress** » excessive (ou *workload, anxiety, fatigue, stress*) peut avoir un impact direct sur la performance et contribuer à une erreur humaine.

Les démons proposés par Endsley sont très généraux. D'une manière ou d'une autre, chaque erreur humaine peut être interprétée comme résultant de l'occurrence d'un ou plusieurs de ces 8 démons. Le réseau bayésien proposé a donc pour nœuds les 8 démons ainsi qu'un nœud « erreur humaine ». Les arcs de ce réseau sont les 8 liens causaux entre chaque nœud démon et le nœud erreur humaine.

ANALYSE DES ACCIDENTS

Méthode

Les statistiques seraient utiles pour calculer les probabilités conditionnelles. Cependant, même si certains accidents de robotique ont été signalés, aucun n'a été analysé du point de vue de la dégradation de la SA et de l'observation des démons de la SA. Un effort important doit donc être fait pour mieux comprendre les liens entre les erreurs humaines et les démons de la SA. La base INRS comporte de nombreux accidents de robotique dans des contextes différents mais avec des circonstances d'exploitation similaires.

Il est proposé ici d'analyser les accidents de robotique de la base de données de l'INRS (Institut National de Recherche et de Sécurité) [11]. Cette base de données n'étant pas dédiée à la robotique, la première étape consiste à appliquer un filtre afin de sélectionner tous les accidents liés à l'utilisation d'un robot. En utilisant le mot-clé « robot », 55 accidents sont sélectionnés. Cependant, après un examen minutieux, 11 accidents doivent être éliminés, et ce pour deux raisons. Premièrement, certains accidents ne sont pas suffisamment documentés pour déterminer la cause ou le contexte de l'accident et le rapport n'est pas exploitable. Deuxièmement, un robot fonctionne parfois dans un environnement complexe et dangereux et la classification de l'accident dans le domaine robotique est ainsi discutable. Par exemple, un robot peut être utilisé en conjonction avec une presse, des outils de coupe ou des boîtes lourdes. Si l'opérateur travaille à la maintenance du robot et est blessé par un objet qui fait partie de la tâche robotique, nous proposons de conserver l'accident dans la liste. En revanche, si le lien entre le robot et l'accident n'est que la prochaine étape de la tâche, il n'y a aucune raison de conserver cet accident dans la liste.

Suite à l'application de ce processus de filtrage, 44 accidents ont été retenus. Ces derniers ont ensuite été analysés et pour chacun d'eux, un ou plusieurs démons de la SA ont été identifiés comme causes profondes. Nous proposons d'illustrer la méthode par l'analyse de trois rapports d'accident dans lesquels différents dans lesquels différents démons de la SA sont impliqués. Les trois accidents sont désignés par les lettres A, B, C dans les paragraphes suivants et leur description est directement tirée de la base de données de l'INRS.

Accident A

L'accident s'est déroulé comme suit : l'entreprise vient d'acquérir deux ensembles de production, composés d'une presse et d'un bras robotisé qui transfère les pièces du moule dans une boîte en polystyrène. Lorsque le robot est défaillant, l'opérateur doit faire le tour de la presse pour intervenir sur le robot. Il doit ensuite retourner au pupitre pour remettre la presse en marche. La victime, un chef d'équipe de 29 ans, a neutralisé le contacteur. Lors de l'accident, l'opérateur a remarqué que la presse s'était arrêtée. Il a appelé le chef d'équipe et ce dernier entre son buste dans l'espace de travail du robot pour constater le dysfonctionnement. Il doit remuer une cassettes lorsque le robot revient vers lui, lui tapant mortellement la tête contre le montant de la machine. Le risque avait été repéré sur le document de sécurité. La

victime avait signé la fiche de poste interdisant d'effectuer cette opération.

Nous proposons de considérer ici la présence de deux démons de la SA. Tout d'abord, en supposant que la victime essaie toujours d'avoir un comportement cohérent, le « **modèle mental erroné** » semble être l'un des principaux démons impliqués dans la mauvaise SA de l'individu. Une représentation mentale erronée possible, qui pourrait être commune à de nombreux opérateurs, est de croire qu'un robot immobile est arrêté et ne bougera pas sans déclencher un bouton de démarrage. En effet, dans des situations ordinaires, un robot est activé en appuyant un bouton et il est arrêté en appuyant sur un autre : un robot immobile peut donc être considéré comme arrêté par un opérateur. Ensuite, l'autre démon de la SA probablement impliqué dans cette estimation incorrecte de l'état du robot est le syndrome « **hors de la boucle** ». Dans le cas présent, le contrôle n'a pas été explicitement rendu à l'opérateur, mais un humain devait faire quelque chose pour la poursuite de la tâche. Ici, le problème est qu'aucune information du robot n'expliquait l'état du robot et le fait qu'il pouvait continuer et suivre les étapes suivantes de sa tâche : l'opérateur est donc en-dehors de la boucle perception-action du robot.

Accident B

L'accident s'est produit dans une usine métallurgique. Il s'est déroulé comme suit : la victime - 30 ans, ouvrier sur presse - travaille sur une presse à injecter de puissance 1500 T, installée il y a trois mois. La presse en marche est alimentée par un robot qui puise le métal en fusion dans un four à l'aide d'une louche. L'ensemble presse et robot est vérifié périodiquement par l'équipe de maintenance, qui a signalé la nécessité de mettre en place des protecteurs au niveau du robot de transfert du métal du four à la presse. Lors de l'installation du nouveau robot et de la louche, les grilles et la porte interdisant l'accès au robot ont été installées. Par contre, les contacteurs électriques de sécurité n'ont pas été montés : l'accès au robot en marche est donc possible. Le jour de l'accident, la victime vérifie le graissage du piston de la presse. Pour cela, elle arrête le robot et la louche en commandant le bouton d'arrêt au tableau électrique. Au cours de cette opération, la victime s'est trompée de bouton. Croyant intervenir robot arrêté, elle a ouvert la porte et s'est trouvée sur la trajectoire de la louche : elle a été percutée par celle-ci pleine de liquide en fusion. Brûlée au dos et à la main gauche, la victime a été hospitalisée.

Plusieurs erreurs ont été commises et des procédures inappropriées ont été suivies. L'organisation du travail et la définition des règles de sécurité doivent être modifiées. Pour cet accident, un démon de la SA évident a eu un impact décisif : la « **saillance mal placée** ». L'interface contrôlant le robot et la louche n'était en effet pas assez claire pour la victime, qui a cru que le robot était arrêté alors qu'il ne l'était pas. Sans plus de détails, il est difficile de déterminer quels boutons étaient trompeurs et avaient une saillance inappropriée. Pour autant, la conclusion du rapport est suffisante pour dire que l'interface était trompeuse et qu'aucune autre raison n'est nécessaire pour expliquer le comportement de la victime.

Ce genre d'accident ne se produit pas très souvent, mais la conception d'une interface claire et simple

pour contrôler des systèmes complexes a été soulignée dans de nombreuses études [6].

Accident C

L'accident s'est produit dans une usine produisant de la céramique. Il s'est déroulé comme suit : la victime, 31 ans, cariste, poussait des boîtes de carrelage sur le convoyeur à l'intérieur de la zone d'évolution d'un robot de palettisation, dans l'atelier de conditionnement. Le robot a heurté violemment la victime à la jambe gauche, occasionnant une double fracture du tibia et du péroné.

Ce type d'accident est relativement fréquent. L'espace de travail du robot est toujours une zone dangereuse. La victime a probablement remarqué que le robot était en marche, mais a décidé de pénétrer dans la zone sans l'arrêter. On ne sait pas si la personne était fatiguée, stressée par une charge de travail élevée ou si elle voulait finir rapidement. Quelle que soit la raison exacte de sa présence, il était certainement possible d'éviter le bras du robot, à condition que l'opérateur soit toujours attentif aux mouvements du robot. Cependant, alors que la victime poussait des boîtes sur le convoyeur, l'attention a été dirigée vers un autre système et l'accident s'est produit. Le démon de « **tunnélisation de l'attention** » est donc ici impliqué pour diminuer la SA de l'opérateur.

D'autres remarques importantes peuvent être faites :

- Premièrement, il était en fait possible d'entrer dans la zone du robot sans avertissement et le robot n'était pas équipé de détecteurs de présence humaine. Ceci est incompatible avec les normes habituelles. Une autre organisation du travail est nécessaire pour une exploitation sûre du robot palettiseur.
- Deuxièmement, une fois de plus, aucune information n'est fournie à l'opérateur concernant l'état actuel et les états futurs du robot. Si le robot travaille dans une petite zone et se rend soudainement à un autre endroit sans avertissement, l'opérateur se trouve dans une sorte de situation « hors de la boucle ». Cependant, il est difficile d'impliquer ici le syndrome « hors de la boucle », car la victime ne faisait pas fonctionner le robot, il s'agissait simplement d'une situation de co-travail. Même si un avertissement du robot aurait pu permettre d'éviter l'accident, l'opérateur ne s'attendait à aucune information et la raison principale de l'accident est la présence de la victime dans une zone interdite.

Statistiques

La même méthode d'analyse a été appliquée aux 44 accidents afin d'en déduire des statistiques. Les résultats sont présentés dans le Tableau 1.

Tunnélisation	Modèle mental erroné	Hors de la boucle	Complexité
13	16	21	6
Saillance mal placée	Overdose de données	Piège de mémoire requise	Charge mentale, anxiété, fatigue, stress
4	0	0	3

Tableau 1. Classification du nombre d'accidents de la base INRS par type de démon de Endsley.

Plusieurs remarques :

- Premièrement, il y a souvent un manque d'information concernant la fatigue, la charge de travail ou le stress de la victime le jour de l'accident. Il y a donc une sous-estimation de l'occurrence du démon de la SA associé.
- Selon notre interprétation de tous les accidents, les démons de « **piège de mémoire requise** » et « **overdose de données** » ne sont jamais impliqués. Le premier a été introduit par Endsley pour tenir compte de la limite de la mémoire à court terme de l'homme [6]. Lorsqu'une longue liste de sous-tâches est requise, un opérateur humain oublie parfois l'une d'entre elles. Ce problème est bien connu pour l'atterrissage, dans le domaine de l'aviation. En revanche, dans le domaine de la robotique, de telles exigences sont rares. Il n'est donc pas surprenant que ce démon de la SA ne soit jamais impliqué dans les accidents signalés. Concernant le démon « **overdose de données** », celui-ci est également peu commun car il est souvent rencontré dans le domaine de la visualisation de données lorsque trop d'informations sont présentées à la fois.
- Pour tous les accidents, au moins un démon de la SA a été identifié comme un facteur important.
- Le démon « **hors de la boucle** » a été identifié dans **48% des causes d'accidents**. Comme expliqué précédemment pour l'accident A, la raison de la classification « hors de la boucle » est basée sur l'observation que la victime n'était pas consciente de l'état exact du robot et croyait à tort qu'il était arrêté ou sur le point de commencer un mouvement spécial.

Un autre résultat important est le nombre de fois qu'une action interdite a été entreprise. Selon notre analyse, 25 accidents se sont produits alors que la victime ou une autre personne n'a pas suivi la procédure de sécurité. Ce résultat suggère que les normes de conception des nouveaux systèmes robotiques ne sont pas suffisantes.

ÉVALUATION DE LA PROBABILITÉ DU RISQUE

Les mesures statistiques de l'implication des démons de SA dans les accidents ne sont pas suffisantes pour inférer une évaluation fine de la probabilité du risque (PRA) pour une application donnée.

En effet, d'une part nous ne connaissons pas le nombre d'accidents rapportées au nombre d'heures passées par un opérateur près d'un robot, et d'autre part, le risque est très dépendant du type de robot, de l'environnement et de la tâche considérée. Pour déterminer les risques, nous proposons la méthode suivante :

1. Premièrement, **lister toutes les erreurs humaines possibles** et leur potentiel impact (approche standard).
2. Pour chacun des 8 démons de SA, **déterminer la liste des erreurs humaines** qui pourraient en être la conséquence directe. Chaque erreur humaine listée à l'étape 1 devrait alors être associée avec un ou plusieurs démons de SA.
3. Pour chaque paire (i.e. erreur possible – démon(s) de SA), **fournir une estimation** de la probabilité d'occurrence.

4. **Additionner ces estimations** pour calculer la probabilité d'erreurs humaines associée à chaque démon de SA.

Une remarque peut être faite sur l'étape 3 de cette méthode – l'estimation de la probabilité d'occurrence – qui est très difficile à réaliser. Pour une tâche spécifique dans un contexte spécifique, les risques spécifiques sont évidemment connus, et généralement pris en compte. En revanche, dans la plupart des cas, les PRA sont calculées par des experts en Facteurs Humains selon une approche empirique. Les estimations sont basées sur des représentations mentales des risques. Les statistiques que nous avons fournies apparaissent alors très importantes pour aider les experts à construire des représentations plus appropriées des liens entre démon de SA et erreurs humaines.

La PRA qui découle de cette méthode est un réseau Bayésien comportant des nœuds « cause » associés aux démons de SA et des nœuds « conséquence » associés aux erreurs humaines. Les probabilités conditionnelles peuvent être aisément calculées si un seul démon de SA est impliqué. À l'inverse, l'implication de plusieurs démons de SA en même temps est un problème difficile à résoudre. Dans la base de données INRS, **au moins 10 accidents** sur les 44 peuvent être considérés comme une **variation de l'accident A** (présenté dans la Section 3) impliquant les mêmes démons de SA : **« modèle mental erroné »** et **« hors de la boucle »**. Plusieurs démons de SA sont donc souvent impliqués simultanément. Si fournir une PRA pour un démon de SA unique est déjà complexe, fournir une PRA lorsque deux ou plus démons de SA sont impliqués en même temps est un grand défi, dû au grand nombre de combinaisons possibles. Afin d'estimer les distributions de probabilité et compte tenu de l'indépendance des démons de SA les uns par rapport aux autres, il est ici possible d'utiliser le modèle Noisy-Or (16, 17, 19, 21). Voir l'équation (1) pour l'équation du modèle Noisy-Or.

$$P(\overline{SA}/X_1 \dots X_n) = 1 - \prod_{i=1}^n (1 - P(\overline{SA}/X_i)) \quad (1)$$

Dans le formalisme proposé ci-dessus, X_1 à X_n sont 8 variables booléennes associées à l'observation des 8 démons de SA. \overline{SA} est utilisé pour exprimer une SA détériorée menant à une erreur humaine. Si les démons de SA sont indépendants les uns des autres, il n'est pas nécessaire de déterminer les probabilités conditionnelles complexes avec plusieurs variables. La probabilité peut être inférée directement comme le produit des probabilités conditionnelles élémentaires.

Dans tous les cas, l'hypothèse de l'indépendance des démons de SA n'est pas réaliste. Parmi les 8 démons, le démon **« charge mentale, anxiété, fatigue et stress »** est singulier. En effet, il n'est pas lié directement au déclenchement d'une erreur humaine en particulier. Il s'agit plutôt d'un démon facilitant l'expression d'un autre démon, tel que la **« tunnélisation de l'attention »**, le **« modèle mental erroné »** ou encore le **« piège de mémoire requise »**. **Nous proposons alors de considérer que seulement 7 démons de SA sont indépendants.** Le démon **« charge mentale, anxiété, fatigue et stress »** est donc retiré du réseau bayésien, mais il doit être pris en compte dans la probabilité des autres démons SA.

Prenons comme exemple applicatif la cellule robotique de l'accident A. Supposons que l'accident le plus redouté soit lié à une intervention humaine dans la cellule, alors que le robot n'est pas mis hors tension comme l'exige la procédure. Le démon « hors de la boucle » (HB) et le démon « modèle mental erroné » (ME) sont jugés causes possibles induisant un tel comportement (C), selon les probabilités suivantes :

- $P(C/HB) = 0.0001$

- $P(C/ME) = 0.0002$

On en déduit donc la probabilité d'observer C :

$$P(C) = 1 - \left(1 - P\left(\frac{C}{HB}\right)\right) - \left(1 - P\left(\frac{C}{ME}\right)\right) \approx 0.0003$$

DISCUSSION

Le travail présenté ici repose sur une analyse méthodique d'une base de données d'accidents en environnement industriel. Les potentielles erreurs humaines y sont étudiées sous le prisme des démons de SA d'Endsley.

Tout d'abord, le fait d'analyser des rapports d'accidents représente une limite au présent travail. En effet, il est très difficile – et dangereux – de faire des inférences sur les comportements des opérateurs sur la seule base du recueil non exhaustif d'un enquêteur. En revanche, ces rapports d'accidents représentent une base de travail d'analyse qui cherche des pistes pour évaluer la probabilité de risque, avec une grille d'analyse novatrice pour le domaine de la robotique (e.g. pour le domaine maritime : 25)). La réflexion du présent travail repose sur l'identification de potentiels démons de SA dans la survenue de l'accident, à un niveau conceptuel donc. Dans ce contexte, les présentations détaillées de la base INRS constituent de facto une base sérieuse pour ancrer la réflexion sur des informations réelles.

Ensuite, le présent travail met en lumière certaines erreurs humaines, contournant parfois les dispositifs de sécurité. Bien que les opérateurs de robots sachent qu'il est obligatoire d'éteindre le robot avant d'entrer dans son espace de travail, ils oublient parfois ou négligent délibérément de suivre la procédure appropriée. Autrement dit, un problème a été rencontré et ils essaient de le résoudre d'eux-mêmes au détriment de leur propre sécurité. **Dans 11% des accidents étudiés** dans la base de données INRS, **un opérateur a décidé d'entrer dans l'espace de travail du robot** pour résoudre un problème sans s'assurer que le robot avait été mis à l'arrêt. Un des démons de SA identifié dans ces situations était le **« modèle mental erroné »**. La victime avait la représentation d'un robot immobile comme étant à l'arrêt.

Enfin, le démon **« hors de la boucle »** est impliqué dans **48% des accidents étudiés**. Le robot est généralement programmé pour opérer dans un mode autonome, mais les interactions sont tout de même requises pour le paramétrage ou la maintenance du robot. Dans chaque cas d'accident, la victime n'était pas consciente du statut du robot et n'était donc pas capable d'en prédire les états futurs. Ce problème est bien connu dans la communauté Human Robot Interaction (HRI) et des recommandations existent pour des interactions efficaces et sûres entre humain et robot (15).

CONCLUSION ET RECOMMANDATIONS

Le présent article propose une nouvelle approche de l'évaluation de la probabilité de risque appliquée à la robotique en environnement industriel. La première contribution porte sur l'analyse de la base de données d'accidents INRS au regard du modèle de SA et de ses démons. Ces statistiques d'accidents et leur interprétation en termes de démons de SA peuvent aider les experts à mieux comprendre les risques associés aux erreurs humaines. La deuxième contribution tient au réseau bayésien qui peut être construit pour représenter les risques associés à une SA détériorée et donc des erreurs humaines. Sur la base de ces contributions, plusieurs recommandations peuvent être formulées pour réduire les risques :

- Pour éviter, ou réduire, une potentielle mauvaise représentation, des informations explicites devraient être fournies aux opérateurs sur le statut du robot (éteint, à l'arrêt, attendant une action, etc.). Aux modalités « classiques » (e.g. alarmes sonores, témoins lumineux), la réflexion pourrait ajouter des modalités du mouvement, en faisant levier sur les degrés de liberté offerts par la robotique. Par exemple, un mode spécifique « vivant » pourrait être implémenté sous forme de mouvements lents et répétitifs, à la manière d'une respiration, pour signaler que le robot est dans l'attente d'une interaction.
- Concernant les normes ISO, les spécifications n'existent pas pour les robots qui ne possèdent pas un mode collaboratif. Notre recommandation concerne donc l'extension des standards de robotique collaborative à l'ensemble des robots.

Pour conclure, l'étude de ces accidents a montré qu'ils surviennent dans un environnement complexe, dans lequel le robot n'est qu'une petite partie d'un système et que les humains présents ne sont pas forcément des opérateurs robotique ou des coéquipiers pour le robot. Dans ces environnements complexes, des solutions *ad hoc* sont implémentées, et les estimations de risques sont approximées. Nous voyons un argument supplémentaire pour analyser les erreurs humaines potentielles au regard des démons de SA, qui sont la seule source commune d'erreurs à travers l'ensemble des cas.

BIBLIOGRAPHIE

1. Baoping, C., Yonghong, L., Yunwei, Z., Qian, F., Zengkai L. and Xiaojie, T. (2013). "A dynamic Bayesian networks modeling of human factors on offshore blowouts", in *Journal of Loss Prevention in the Process Industries*, Vol. 26 No. 4, July 2013, pp. 639-649.
2. Baxter, P., Kennedy, J., Senft, E., Lemaignan, S., Belpaeme, T. (2016). From Characterising Three Years of HRI to Methodology and Reporting Recommendations, *proceedings of the 11th ACM/IEEE*

3. Burke, J.L., Murphy, R.R., Coovert, M.D. and Riddle, D.L. (2004). Moonlight in Miami: Field study of human robot interaction in the context of an urban search and rescue disaster response training exercise, *Human Computer Interactions*, vol. 19 (1/2), pp. 85-116.
4. Chappell, S., Detwiler, C., Holcomb, K., Hackworth, C., Boquet, A., & Wiegmann, D. A. (2017). Human error and commercial aviation accidents: an analysis using the human factors analysis and classification system. In *Human error in aviation* (pp. 73-88). Routledge.
5. Dhillon, B. S. (1991). *Robot Reliability and Safety* © Springer-Verlag New York, Inc 1991.
6. Endsley, M. R. and Garland, D.J. (2000). *Situation awareness analysis and measurement*, Mahwah, NJ: Lawrence Erlbaum, 2000.
7. Endsley, M. R. and Jones, D. J. (2016), *Designing for situation awareness: An approach to user-centered design* (2nd ed.), London: Taylor & Francis, 2016.
8. Goodrich, M. A. and Schultz, A. C. (2007). "Human-Robot Interaction: A Survey", *Foundations and Trends in Human-Computer Interaction* Vol. 1 (3), pp. 203-275.
9. Groth, K. and Mosleh, A. "Development and Use of a Bayesian Network to Estimate Human Error Probability", *proceedings of the International Topical Meeting on Probabilistic Safety Assessment and Analysis* Wilmington, NC, USA, March 13-17, 2011.
10. Groth, K. M. and Mosleh, A. (2012). "Deriving causal Bayesian networks from human reliability analysis data: a methodology and example mode", *Journal of Risk Reliability*, vol. 226 (4), pp. 361-79.
11. INRS: Institut National de Recherche et de Sécurité (France), Epicea Database, reports of accidents, <http://www.inrs.fr/publications/bdd/epicea/recherche.html>
12. ISO: International Organization for Standardization ISO12100:2010. Safety of Machinery – General principles for design – Risk assessment and risk reduction. http://www.iso.org/iso/home/store/catalogue_detail.html?csnumber=51528.
13. ISO: International Organization for Standardization ISO10218-2011, *Robots and Robotic Devices, Safety Requirements for Industrial Robots*.
14. ISO: International Organization for Standardization ISO13855-2010, *Safety of Machinery – Positioning of Safeguards With Respect to the Approach Speeds of Parts of the Human Body*.
15. ISO: ISO/TS 15066-2016, *Robots and robotic devices — Collaborative robots*.
16. Lemmer, J. F. and Gossing, D. E. "Recursive Noisy OR—A Rule for Estimating Complex Probabilistic Interactions", in *IEEE Transactions on Cybernetics*, Vol. 34 No. 6, January 2005, pp. 2252 – 2261.
17. Mkrtchyan, L. and Podofilini, V. N. "Bayesian belief networks for human reliability analysis: A review of applications and gaps", in *Reliability Engineering & System Safety*, Vol. 139, 2015, pp. 1-16.
18. Paletta, L., Dini, A., Murko, C., Yahyanejad, S., Schwarz, M., Lodron, G., Ladstätter, S., Paar, G., Velik, R. (2017). Towards Real-time Probabilistic Evaluation of Situation Awareness from Human Gaze in Human-Robot Interaction, *Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction*, Vienna, Austria, March 06 - 09, 2017.
19. Pearl, J. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann, 1988.
20. Riley, J.M., Strater, L.D., Chappell, S.L., Connors, E.S., Endsley, M.R. (2010). Situation Awareness in Human-Robot Interaction: Challenges and User Interface Requirements, *proceedings of the conference on Human-Robot Interactions in Future Military Operations*, pp. 171-192.
21. Salotti, J.M. "Noisy-Or nodes for conditioning models", in Lecture Notes in *Artificial Intelligence*, Vol. 6226, pp. 458-467, Springer, from "Simulation of Adaptive Behaviors", (SAB 2010), Paris, 24-28 August, 2010.
22. Salotti, M.R. Bayesian Network for the Prediction of Situation Awareness Errors, *International Journal on Human Factors Modeling and Simulation*, Special Issue on: *Quantifying Human Factors Towards Analytical Human-in-the-Loop*, January 2018.
23. Sarter M.R., and Woods, D. D. "Situation awareness: A critical but ill-defined phenomenon", *The International Journal of Aviation Psychology*, Vol. 1, No. 1, 1991, pp. 45-57.
24. Stubbs, J.K., Hinds, P.J., Wettergreen, D. 2007. Autonomy and common ground in human robot interaction: A field study, *IEEE Intelligent Systems*, vol. 22(2), pp. 42-50.
25. Stratmann, T.C., & Boll, S. (2016). Demon hunt-the role of endsley's demons of situation awareness in maritime accidents. In *Human-Centered and Error-Resilient Systems Development*. pp. 203-212, Springer, Cham.