Sécurité des systèmes de la robotique médicale

Jérémie Guiochet, Gilles Motet, Bertrand Tondu, Claude Baron

Sécurité des systèmes de la robotique médicale

Jérémie Guiochet

LAAS - CNRS
7 av. du Col. Roche
31077 Toulouse Cedex 4
jeremie.guiochet@laas.fr

Gilles Motet **Bertrand Tondu**
Claude Baron
LESIA - INSA Toulouse
135 av. de Rangueil
31077 Toulouse Cedex 4
{motet,tondu,baron}@insa-toulouse.fr

Résumé : L'utilisation de systèmes robotiques dans le domaine médical, initiée il y a quelques années, pose le problème de la sécurité au sein d'un environnement où l'homme est très présent. La complexité de tels systèmes et le transfert de responsabilités du chirurgien vers le robot conduisent les concepteurs à intégrer dans leurs études des exigences de sûreté de fonctionnement, et notamment un de ses attributs essentiels : la sécurité. Bien que cette discipline soit largement étudiée dans des domaines à sécurité critique comme l'avionique, la spécificité de la robotique médicale nous amène à reconsidérer la notion de risque qui y est associée. En partant de l'effet indésiré, le dommage, on remonte aux causes en considérant les notions de danger, de risque et de sécurité. Cela nous conduit à l'identification des moyens possibles pour gérer le risque associé à l'utilisation de systèmes de la robotique médicale. Les notions introduites sont illustrées par notre expérience issue du développement d'un robot télé-échographe.

Table des matières

1 Introduction

La robotique industrielle essentiellement dédiée à des processus manufacturiers a récemment utilisé la technologie de ses bras robots pour des applications hors de l'usine. Cette « robotique de service », et plus particulièrement sa composante de pointe, la robotique médicale [11, 61], a fortement modifié la problématique de la sécurité des systèmes robotiques. Alors que les problèmes de sécurité des robots industriels relevaient essentiellement de défaillances des systèmes de protection (barrières, grillages, etc.), et que l'opérateur humain ne pénétrait l'espace de travail que pour des opérations de maintenance ou de programmation, la robotique de service nécessite de prendre en compte la proximité physique et l'étroite collaboration entre l'humain et le robot [33]. L'impérieuse exigence de maîtriser la sécurité est d'autant plus urgente que les fonctionnalités et l'autonomie des robots de service ne cessent d'augmenter. Le robot médical Robodoc[1], commercialisé pour effectuer le remplacement de la tête du fémur au niveau de la hanche [57, 7], réalise à l'issue de la planification de l'opération, la découpe et la préparation de la cavité fémorale en totale autonomie. Ainsi, la responsabilité d'actions médicales sont progressivement transférées du praticien vers le robot. Par ailleurs, on assiste aujourd'hui à l'apparition de systèmes de télé-médecine (médecine à distance) permettant la téléopération du robot par le spécialiste se trouvant à une grande distance du patient. Il existe également des systèmes de téléopération sur site, pour lesquelles l'acte du praticien est effectué par l'intermédiaire du robot, permettant au spécialiste d'effectuer des actions plus rapides et plus précises. Dans ce cadre, le système daVinci, illustré figure 1, permet de réaliser une opération minimalement invasive[2] grâce à un système de télécommande des outils, et d'une visualisation en 3 dimensions des images filmées par un endoscope. Le système AESOP [44] permet également de réaliser des opérations minimalement invasives mais en guidant les déplacements d'un endoscope grâce à la voix du praticien. De façon plus générale, plusieurs projets de recherche, sur le modèle de l'arthroscopie[3], visent à améliorer les opérations de chirurgie en miniaturisant les outils et en faisant appel à un guidage par endoscope. Des robots miniatures ou micro-robots pourraient répondre à cette demande, et permettre alors des opérations jusqu'ici impossibles, car trop dangereuses, comme des opérations complexes du cœur ou du cerveau.

Dans ce contexte, les utilisateurs (patients et médecins), mais également les personnes se trouvant dans leur environnement ou les autorités acceptant leur mise sur le marché, peuvent s'interroger à juste titre sur la confiance qui peut être accordée à de tels systèmes. La sécurité, l'un des facteurs de cette confiance, a longtemps été considérée comme une propriété résultant de l'utilisation d'un ensemble de techniques sans qu'il y ait de lien entre elles. Il existe néanmoins aujourd'hui une science de la sécurité, parfois appelée science du danger, science du risque,

[1] ISS Inc, USA, http ://www.robodoc.com

[2] Cette technique opératoire minimise l'accès anatomique par le biais de petites incisions pour insérer un endoscope et des instruments chirurgicaux

[3] Examen d'une cavité articulaire au moyen d'une caméra appelée endoscope permettant par la suite d'effectuer des opérations sans ouvrir comme en chirurgie

FIG. 1 – Système chirurgical daVinci, © [2006] Intuitive Surgical, Inc

ou plus récemment cindynique[4]. Bien que de nombreux domaines s'appuient sur ces sciences pour analyser la sécurité des systèmes, la robotique médicale pose de nouvelles problématiques liées à la sécurité. En effet l'interaction, très forte avec l'humain, ainsi que l'hétérogénéité des disciplines couvertes lors de la conception (informatique, électronique, mécanique, facteur humain) amènent à redéfinir certains concepts et à explorer de nouvelles techniques de conception.

Cet article a pour but de proposer un cadre générique permettant de définir les problèmes relatifs à la sécurité des systèmes de la robotique médicale et également de présenter les principales techniques d'analyse et de conception améliorant la sécurité de tels systèmes. Il est illustré par notre expérience issue du développement d'un robot télé-échographique (TER). Il fonde ses analyses sur le concept d'événement non désiré qu'est le dommage (section 2). À partir de cette notion, et de l'ensemble des normes qui lui sont dédiées, les parties suivantes traitent des causes des dommages (section 3) et des moyens que l'on peut employer pour les traiter (section 4). Nous abordons ensuite la notion d'assurance de la sécurité que l'on peut obtenir grâce à la certification (section 5).

[4]http ://www.cindynics.org

2 Effets non désirés : les dommages

Afin d'analyser le concept de sécurité inhérente aux robots médicaux, il est fondamental de revenir aux notions de base, et de comprendre le mécanisme d'apparition d'un accident. Pour tout système, les effets non désirés sont identifiés par la notion de dommage permettant par la suite de définir les concepts de risque et de sécurité.

2.1 Dommage

2.1.1 Définition

La notion de dommage est commune à de nombreux domaines. Elle est définie de la même façon dans le médical [37], en robotique et au sein des normes génériques comme la CEI 60300 [31]. La norme cadre ISO Guide 51 [38] définit ainsi le dommage :

Dommage	*Blessure physique ou atteinte à la santé des personnes, ou dégât causé aux biens ou à l'environnement*

Il est intéressant de comparer cette définition avec celle de la sécurité fréquemment utilisée en robotique industrielle, définie comme la *prévention de dégâts sur l'humain, le robot et les éléments avec lesquels le robot interagit* [16]. On retrouve deux composantes de la notion de dommage :

- les *personnes*, qui peuvent être les patients, les spécialistes ou les assistants, identifiés ici comme les humains,
- les *biens*, correspondants aux dispositifs médicaux utilisés (le robot lui-même, les outils, les appareils de mesures, etc.).

Cependant, la définition adoptée dans le domaine médical introduit une composante supplémentaire : l'environnement. Ceci est particulièrement important car les tâches des robots médicaux peuvent influer sur l'état de l'environnement : destruction, pollution, contamination, etc. D'une manière générique, il est important de spécifier quelles sont les « parties prenantes »d'un dommage potentiel. Ce concept est présenté dans la norme générique sur le risque, le ISO Guide73 [40]. À titre d'exemple le dommage peut concerner l'intégrité des biens (Ariane 5), des personnes (Therac-25), de l'environnement, ou tout à la fois (Tchernobyl).

2.1.2 Gravité d'un dommage

Pour des systèmes robotiques médicaux, la notion de gravité (*severity* en anglais) est identique à celle de nombreux autres domaines technologiques. Elle évalue la nuisance des dommages. Cependant, les normes relatives aux dispositifs médicaux ne prescrivent aucune échelle de graduation de ces nuisances, et laissent ainsi le choix aux fabricants, à l'opposé d'autres domaines où les niveaux sont prédéfinis (en pétrochimie ou en avionique par exemple). La liste suivante donne un exemple de métrique sur la gravité des dommages sur les seuls humains : catastrophique

(décès d'une ou plusieurs personnes), majeure (blessures ou maladies graves, infirmité permanente), mineure (blessures ou maladies mineures, nécessitant un traitement médical), minime (légères blessures relevant des premiers soins), négligeable (incident n'exigeant aucun traitement médical). Notons que dans cette échelle de mesure, le décès d'une personne est classé comme *catastrophique*, alors que dans d'autres domaines technologiques le niveau catastrophique est réservé à l'occurrence du décès de nombreuses personnes, comme pour les dommages d'origine naturelle (séismes, etc.). Pour les dispositifs médicaux, il est évident que l'enjeu est la santé d'un patient, et que son décès est donc catastrophique. La notion de gravité en fonction du nombre de morts est par conséquent un concept inexistant en médecine. Il existe malgré tout un exemple de dispositif médical, le Therac-25, ayant provoqué plusieurs décès (six) de 1985 à 1987 aux États-Unis, du fait d'une trop forte exposition aux rayons X [48].

2.1.3 Occurrence d'un dommage

En plus de la gravité, un dommage est qualifié par sa fréquence d'occurrence. Dans la norme médicale ISO 14971 [37], la *probabilité d'un dommage* est exprimée en terme d'*occurrence d'un dommage* par un mesure qualitative (fréquent, occasionnel, etc.). Cette norme évoque le fait qu' « une bonne description qualitative est préférable à une inexactitude quantitative ». Ce point de vue a un aspect novateur par rapport aux prescriptions qui ont été faites lors des premières études de sécurité notamment dans le nucléaire où les approximations successives rendaient les résultats numériques inexploitables. L'estimation des probabilités est généralement obtenue selon trois approches : données historiques de situations comparables, techniques d'analyse ou de simulations, jugements d'experts ou de bases de données appropriées. En particulier, en robotique médicale, il n'existe pas de données historiques exploitables. Cette absence peut cependant être palliée en se référant à des données sur des dommages liés aux contrôleurs de robots industriels (notamment auprès d'organisme comme l'INRS[5] en France, l'OSHA[6] et la FDA[7] aux USA, ou le HSE[8] en Angleterre), ou causés par l'utilisation de logiciels dans le milieu médical, ou encore induits par l'utilisation de dispositifs médicaux autres que des robots, etc.

Le choix des niveaux d'occurrence dépend des concepteurs. À titre d'exemple, la liste suivante présente des niveaux de probabilité d'occurrence, généralement utilisés pour une estimation qualitative : fréquente, probable, occasionnelle, rare, improbable, invraisemblable. Dans cette classification utilisée en robotique médicale [25, 43], *fréquente* indique une fréquence d'occurrence du dommage plusieurs fois par an, mais il existe des études où la fréquence est exprimée en fonction d'une heure d'utilisation. La variabilité des échelles de mesure diminue généralement lors de l'estimation du risque global pour l'utilisateur, et l'on retrouve les mêmes niveaux de risque dans différentes études (aspect présenté dans la section suivante).

[5] Institut National de Recherche et de Sécurité, www.inrs.fr
[6] Occupational Safety and Health Administration, www.osha.gov
[7] Food and Drug Administration, www.fda.gov
[8] Health & Safety Executive, www.hse.gov.uk

Fréquence d'occurrence	Fréquence indicative (par année)	Gravité du dommage				
		1 Catastrophique	2 Majeure	3 Mineure	4 Minime	5 Négligeable
Fréquente	>1	H	H	H	H	I
Probable	$1\text{-}10^{-1}$	H	H	H	I	I
Occasionnelle	$10^{-1}\text{-}10^{-2}$	H	H	I	I	F
Rare	$10^{-2}\text{-}10^{-4}$	H	I	I	F	T
Improbable	$10^{-4}\text{-}10^{-6}$	I	I	F	T	T
Invraisemblable	$<10^{-6}$	I	F	T	T	T

FIG. 2 – Exemple de tableau pour l'estimation du risque

2.2 Notion de Risque

2.2.1 Définition

Afin de rendre compte de l'interaction entre la gravité et l'occurrence d'un dommage, la notion de risque a été introduite. La définition de la norme médicale ISO 14971 [37] est identique à celle de la norme plus générique ISO Guide 51 [38] :

Risque — *Combinaison de la probabilité d'un dommage et de sa gravité*

La notion de risque connait des fluctuations dans sa définition et est parfois présentée comme la probabilité du *danger* (par opposition avec la probabilité d'occurrence du *dommage*) combinée avec la gravité du dommage. C'est notamment le cas dans les versions précédentes des normes médicales sur le risque. Dans le domaine médical, c'est la notion de probabilité du *dommage* qui est aujourd'hui utilisée sans préciser quels événements ont provoqué ce dommage. Les circonstances de l'apparition du dommage associées à la notion de danger seront exposées ultérieurement à la section 3.

Dans le domaine médical, la combinaison n'est pas un simple produit entre probabilité et gravité. En effet, il est possible de n'attribuer qu'une faible pondération à la probabilité. La détermination de la probabilité étant parfois impossible, difficile, ou non vérifiable, un risque sera principalement évalué en fonction de la gravité du dommage potentiel. Cette problématique est développée dans la section 4.3.3

2.2.2 Mesure du risque

Pour quantifier le niveau du risque, les couples [probabilité, gravité] sont comparés. Sur la base des classifications de gravité et probabilité d'occurrence présentées en sections 2.1.2, le tableau de la figure 2 estime le risque suivant quatre niveaux : H (risque fort), I (risque intermédiaire), F (risque faible), et T (risque négligeable).

2.2.3 Risque acceptable

La notion de risque est essentielle pour caractériser la confiance attribuée à un système. En effet, si l'on s'expose à des dommages graves, seule leur faible probabilité d'occurrence nous les font accepter. Nous établissons généralement cet arbitrage en fonction des risques que nous encourrons par ailleurs. La notion de *risque acceptable* [38] est alors définie comme *un risque accepté dans un contexte donné basé sur des valeurs courantes de notre société.*

Les *valeurs courantes de notre société* sont souvent fondées sur des données associées à des phénomènes naturels. Ainsi, on accepte le risque de mourir en prenant l'avion si la probabilité de ce décès par cette cause est identique voire inférieure à la probabilité de décès induit par un séisme ou une crise cardiaque (pour un corps sain). La définition précise par ailleurs que l'acceptabilité est *fonction du contexte.* Ce contexte exprime en particulier l'apport escompté malgré le risque pris. Ainsi, une opération chirurgicale sans robot, a une probabilité non négligeable de conduire à des dommages graves. Mais ces risques sont acceptés en confrontant le bénéfice d'une guérison aux dommages causés par une évolution naturelle de la maladie sans traitement médical.

Le *risque acceptable* est, par conséquent, le résultat d'un équilibre entre l'idéal de la sécurité absolue et des facteurs comme le bénéfice pour les patients, les règles et les conventions de la société concernée. En robotique médicale, le patient sera confronté aux mêmes risques qu'une opération classique, ajoutée de ceux induits par l'utilisation d'un robot. Mais il convient alors de bien identifier les bénéfices que l'ont retire de cette utilisation (gain de temps, moins de perte de sang, etc.). Nous reviendrons sur cette notion dans la partie 4.4 où nous présenterons les moyens pour spécifier un risque acceptable.

2.3 Sécurité

Le concept de sécurité est devenu un des enjeux les plus importants pour de nombreux domaines technologiques. Il est parfois utilisé pour exprimer *l'absence d'accident ou de perte.* Cette définition donne une dimension absolue à la sécurité. Or le domaine médical prouve bien qu'il n'y a qu'une sécurité relative ; il existe toujours un risque résiduel. Par exemple, sur un nombre donné d'opérations chirurgicales, il est établi qu'il existe un certain nombre de rejets, d'infections, ou d'autres complications allant parfois jusqu'au décès du patient. Au regard des bienfaits pour la majorité des patients, la société permet de prendre ce risque. Dans ce contexte, le terme *sécurité* est employé dans le domaine médical pour exprimer un niveau de sécurité atteint en réduisant le risque à un niveau acceptable. La définition de la norme [38] illustre bien cette relativité :

Sécurité _____ *Absence de risque inacceptable*

La sécurité, dans cette optique, est donc un concept lié à une connaissance du niveau de risque accepté. Ainsi, pour beaucoup d'opérations chirurgicales, la gravité et la probabilité des dommages possibles (donc le risque) sont des informations que le praticien transmet aux patients. Ce dernier accepte alors ou non le niveau de risque induit par l'intervention médicale. La décharge que signent alors les patients

(même aujourd'hui pour une simple échographie), permet de protéger juridiquement les docteurs en cas d'apparition du dommage. Il est donc évident que pour une intervention avec un robot, une telle décharge doit comporter les mêmes informations que pour une opération classique, et augmentée des nouveaux risques induits par l'utilisation du robot.

3 Causes : les dangers

3.1 Phénomène dangereux et situation dangereuse

Historiquement, le danger a été défini de différentes manières. Dans la méthode analytique MORT (*Management Oversight and Risk Tree* présentée par [41]), un danger est principalement caractérisé par un transfert d'énergie. De manière similaire, en robotique industrielle, le danger se rapportait à une accumulation d'énergie aboutissant à un accident. Le danger a aussi été défini comme une propriété inhérente d'un objet, d'une substance ou d'un sous-système qui a la capacité de provoquer un dommage. Dans le domaine médical, il est évident que les dangers ne se réduisent pas à un transfert d'énergie ou à une propriété inhérente d'un élément. On peut citer comme exemple le rejet d'un organe transplanté, le développement d'un effet secondaire, ou le fonctionnement irrégulier (voire l'arrêt) d'un pacemaker.

Dans le cadre d'un système automatisé comme un robot médical, il est important de prendre en compte l'état dans lequel le système se trouve et les conditions d'environnement pour définir un danger. Ces considérations apparaissent dans la définition donnée pour les systèmes informatiques par [48], où le danger (*hazard* en anglais) est défini par « un état ou un ensemble de conditions d'un système (ou d'un objet), qui, couplés avec d'autres conditions de l'environnement du système (ou de l'objet), mèneront inévitablement à un accident ».

Les normes récentes définissent le danger comme « source potentielle de dommage ». Cette définition diffère de la précédente en posant une condition de potentialité sur l'aboutissement à un dommage. La notion de source est dans ce cadre ambiguë et peut être interprétée de différentes manières. Il est en effet parfois difficile de faire la différence entre le danger, ses causes ou ses effets. Par exemple la norme [37] fournit des listes de dangers communs aux dispositifs médicaux pour aider le concepteur à les identifier, et l'on peut retrouver dans ces listes à la fois des effets et des causes. C'est en cela que le terme *source* reste vague et peut désigner par exemple une défaillance, une faute ou une erreur dans la terminologie de la sûreté de fonctionnement [4]. Le concept de *source* ne souligne pas non plus le fait que c'est une combinaison de circonstances qui peuvent aboutir à un dommage.

Les disparités entre les définitions précédentes du danger ont été réduites avec la publication de la dernière version de la norme sur la gestion du risque pour les dispositifs médicaux [37]. Le terme de *phénomène dangereux* a été substitué au terme de *danger* et la notion de *situation dangereuse* a été introduite.

Phénomène dangereux *Source potentielle de dommage*

On regroupe sous cette appellation l'ensemble des sources et des facteurs pouvant contribuer à la création d'un dommage. L'annexe D de la norme [37] fournit

un ensemble « d'exemples de phénomènes dangereux possibles et des facteurs qui y contribuent ». La classification présentée ne met pas en valeur les différents concepts que nous venons d'introduire, et il est possible de trouver à un même niveau de classification des défaillances, leurs causes, des types génériques de sources de dommages, des propriétés inhérentes à des substances, etc. Le propos de cette norme n'est pas de donner une catégorisation basée sur la terminologie du risque, mais de fournir une liste permettant éventuellement aux concepteurs de trouver des phénomènes dangereux ou des facteurs qui y contribuent, qui n'auraient pas été identifiés. On y trouve des termes génériques comme par exemple des attributs de l'énergie tels que l'électricité, la chaleur, la force mécanique, le rayonnement et dans le même temps des causes de ces transferts énergétiques comme les pièces mobiles, les mouvements intempestifs, les masses suspendues, etc. [37, p.22]. À partir de cette liste, nous proposons des classes de phénomènes dangereux pour les systèmes de la robotique médicale :

- propriétés inhérentes dangereuses (un bord tranchant, une substance toxique, etc.) ;
- états dangereux du sous-système (axes en mouvement, masse suspendue, etc.) ;
- défaillances des composants matériels ou logiciels ;
- erreurs humaines ;
- événements inconnus liés à l'environnement ouvert.

Ces sources potentielles de dommage peuvent être combinées, et également induire suivant la situation un risque fort ou nul. En effet un bord tranchant n'induit aucun risque s'il reste isolé de tout contact physique. Le concept de situation dangereuse permet alors de spécifier une situation dans laquelle un phénomène dangereux induit un risque non négligeable :

Situation dangereuse	*Situation dans laquelle des personnes, des biens ou l'environnement sont exposés à un ou plusieurs phénomènes dangereux*

Pour les systèmes de la robotique médicale, comme pour de nombreux systèmes technologiques, le concept de scénario est inclus dans la notion de situation. Un scénario décrit les événements et les états du système provoquant un comportement du système. Dans le cas d'une situation dangereuse, il est important de décrire le scénario d'utilisation qui est fondamental pour un robot médical. À titre d'exemple, les risques induits par les mêmes phénomènes dangereux au cours des différentes phases d'utilisation d'un robot médical (installation du patient, planification de l'opération, approche de l'outil, opération médicale, etc.) peuvent avoir des valeurs très différentes.

3.2 Événement dommageable

Le terme d'*événement dommageable* est défini dans la norme [38] comme :

Événement dommageable	*Événement déclencheur qui fait passer de la situation dangereuse au dommage*

Ce concept n'est pas repris dans les normes dédiées aux dispositifs médicaux. En revanche, il s'avère intéressant pour une application robotique. Il permet en effet de spécifier l'événement qui fait passer le système socio-technique (système incluant les humains et la technologie) d'une situation dangereuse à un dommage spécifique. En robotique médicale, de tels événements sont principalement des interactions entre l'outil du robot et une partie du corps du patient (coupure, arrachement, étirement, brûlure, etc.) dont résulte un dommage (saignements, destruction de liaisons, destruction de fonctionnalités, perforation, etc.).

3.3 Accident et incident

Les analyses de sécurité utilisent deux notions importantes, pourtant absentes de la norme médicale [37], mais qui apparaissent dans la majorité de la littérature sur le domaine. On définit ainsi la notion d'accident en s'inspirant de la définition proposée par [48] :

Accident	*Événement non désiré et d'occurrence non prévue résultant en un niveau de dommage spécifié*

Cette notion repose sur celle de l'événement dommageable. Dans le cas d'un accident, l'événement dommageable produit un dommage de gravité non nulle ou non négligeable. À l'opposé, un événement dommageable produisant un dommage de gravité nulle ou négligeable (en général dû à des circonstances extraordinaires, on peut alors parler de *chance*) produira ce que l'on définit par un *incident*.

Incident	*Événement qui ne conduit pas à des pertes, mais qui a le potentiel de créer des dommages en d'autres circonstances*

Ainsi, un mouvement intempestif d'un bras de robot qui ne touche pas d'humains (ni de biens) alors que ceux-ci se trouvaient dans son espace de travail, est un incident s'il n'y a aucun dommage.

3.4 Exemple d'utilisation des notions liées au risque

En prenant l'exemple d'une coupure (événement dommageable), la figure 3 illustre les notions introduites et notamment le fait qu'une situation dangereuse conduira à un dommage s'il existe un événement dommageable. Sur cet exemple nous faisons également apparaître le concept de scénario d'utilisation, qui combiné avec un phénomène dangereux conduit à une situation dangereuse. Cet exemple n'illustre que le cas de l'accident mais on pourrait également représenter le fait que l'on aboutit à un incident.

4 Moyens : la gestion du risque

Les concepts associés aux dommages et à leurs sources étant définis, il convient de gérer le risque des dommages afin de garantir l'absence de risque inacceptable,

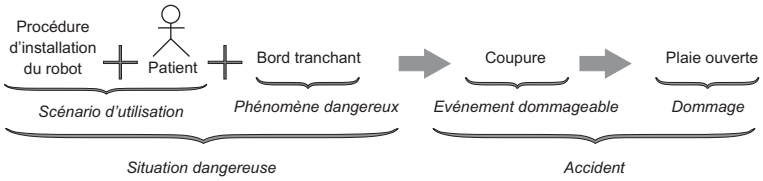

FIG. 3 – Exemple illustrant la terminologie

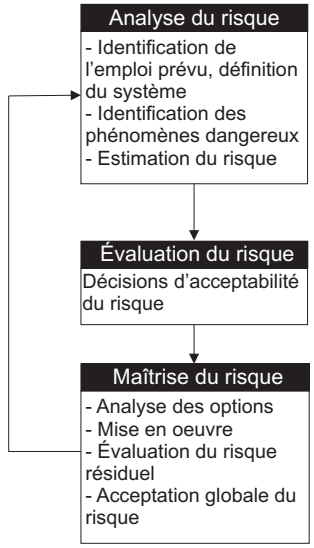

FIG. 4 – Activités de la gestion des risques, figure tirée de la norme [37]

c'est-à-dire la sécurité. La figure 4 donne une représentation schématique des principales étapes du processus de gestion des risques.

4.1 Vue d'ensemble

Ce processus correspond à celui présenté dans la norme ISO 14971 [37] tiré de la norme générique ISO Guide 51 [38]. Avant de détailler chaque étape de ce processus dans les sections 4.3, 4.4 et 4.5, nous abordons la question essentielle des facteurs humains au sein de la gestion du risque pour les systèmes de la robotique médicale (section 4.2).

4.2 Intégration des facteurs humains dans la gestion du risque

La présence d'humains dans l'environnement des systèmes de la robotique de service et en particulier de la robotique médicale, en fait des systèmes dits *socio-techniques*. La sécurité de tels systèmes ne dépend pas uniquement de la défaillance de ses composants. En effet, l'humain ne peut être réduit à un simple composant

ayant un taux de défaillance. Il peut, par exemple, stopper le système en cas de défaillance et finir une opération chirurgicale de manière classique. Son rôle dans l'utilisation du système est une composante particulière qu'il convient d'analyser. Ainsi, aujourd'hui, la sécurité est généralement obtenue par une analyse des facteurs de risque principalement dus aux défaillances, mais aussi par une analyse des *facteurs humains*.

4.2.1 Facteurs humains en robotique et en médical

Dans le milieu industriel, les facteurs humains sont pris en compte au sein du processus de développement. Mais bien que ce domaine d'étude cristallise de nombreuses recherches, il est encore difficile de trouver dans les processus de développement des robots médicaux, des éléments y faisant référence. La différence de langage entre ingénieurs de développement et spécialistes du domaine cognitif est sans doute une des raisons de ce problème. On peut noter, par exemple, l'abandon d'un projet de norme, la CEI 300-3-8, mentionnée dans la norme ISO 60300 [31], qui devait traiter de l'appréciation de la fiabilité humaine.

Dans le domaine de la robotique beaucoup d'études portent sur des aspects très techniques liés aux interactions entre humains et robots du point de vue des ordres envoyés au robot. Par exemple, différents modes de téléopération comme le retour d'effort ou la commande par la voix sont étudiés. Si l'on retrouve dans le domaine médical quelques applications de ces recherches (endoscope guidés par la voix dans AESOP [44]), les facteurs humains concernent principalement l'étude de l'erreur humaine, sujet largement abordé par les sciences cognitives [58].

4.2.2 Processus de gestion du risque et analyse des facteurs humains

Plusieurs approches existent pour exprimer les interactions entre l'analyse de la sécurité (correspondant à la gestion du risque) et l'analyse des facteurs humains. [46, p65-66] classent les moyens pour la sûreté de fonctionnement des systèmes socio-techniques suivant quatre activités. La sécurité, en tant qu'attribut de la sûreté de fonctionnement, est ainsi augmentée par ces moyens. Les aspects de la sécurité liés aux facteurs humains utilisent ici la notion d'erreur humaine pour la classification de ces activités :

- La *prévention des erreurs humaines* a trait principalement à la recherche d'une répartition des tâches entre humains et technologie qui permette de confier aux humains des fonctions et des tâches homogènes et cohérentes.
- La *prévision des erreurs humaines* concerne les méthodes pour estimer la présence, la création et les conséquences des erreurs humaines.
- L'*élimination des causes d'erreurs humaines* concerne la réduction des causes d'erreurs en mettant l'humain en situation réelle ou en simulation.
- La *tolérance aux erreurs humaines* concerne l'introduction de mécanismes permettant au système socio-technique de continuer sa fonction en dépit des erreurs.

Cette classification permet, grâce à la terminologie utilisée, de donner une vision claire des moyens disponibles concernant les facteurs humains. Mais elle n'indique

aucun enchaînement d'étapes et aucune interaction avec l'analyse des risques.

[10] exposent les étapes de la conception d'un système en mettant en parallèle les étapes et les interactions entre trois domaines : le processus de développement, l'analyse de la sécurité et l'analyse des facteurs humains. Leurs travaux font apparaître des redondances ou des activités communes à l'analyse de la sécurité et à l'analyse des facteurs humains mais conservent la séparation entre ces deux domaines. De plus, il est intéressant de noter que dans un ouvrage de référence sur la sécurité des systèmes comme celui de N. Leveson [48], la notion de facteurs humains n'est pas utilisée, et que seule l'erreur humaine est mentionnée.

Dans [20], les auteurs proposent, pour le développement de dispositifs médicaux, d'introduire les facteurs humains dans un processus de gestion du risque. Une approche identique se retrouve dans un rapport du HSE [30], où il est proposé d'inclure les facteurs humains à la norme IEC 61508 [32] dédiée aux dispositifs électriques, électroniques et programmables relatifs à la sécurité. C'est dans la continuité de ces deux propositions que nous aborderons les facteurs humains par la suite. Pour chaque étape de la gestion du risque présentée dans cette section, des éléments spécifiques aux facteurs humains et à la robotique médicale seront présentés.

4.3 Analyse du risque

L'analyse du risque est définie [40] comme :

Analyse du risque	*Utilisation systématique d'informations pour identifier les sources de dommages et estimer les risques*

Première étape de l'actuelle approche de la gestion du risque, elle en constituait la seule dans les normes précédentes. Elle constitue également le point de départ des processus d'analyse de la sécurité (*Safety Assessment Process*) dans de nombreux domaines [56], et influe directement le processus de développement. Lors de la conception d'un système de robot médical, le processus d'analyse du risque est parallèle au processus de développement avec lequel des informations sont continuellement échangées. Il repose sur des descriptions du système provenant du processus de développement et impose certaines modifications (conception, utilisation, etc.). Cela implique notamment que ce processus comme tout processus actuel de développement, soit itératif, continu et incrémental, et n'intervienne donc pas seulement en début de fabrication ou à des étapes fixes du développement, mais tout au long du cycle de vie du système. [48] attribue ainsi deux finalités majeures à une analyse du risque : la participation au processus de développement et la production d'informations en vue de la certification. Aujourd'hui les règles de la certification imposent la présence d'une analyse du risque dans le processus de développement (voir section 5).

L'analyse du risque est mise en œuvre par trois activités que nous détaillerons par la suite : la définition du système et de l'utilisation prévue, l'identification des phénomènes dangereux, et l'estimation du risque.

4.3.1 Définition du système et de l'utilisation prévue

Cette étape a pour but de fournir une base pour l'identification des phénomènes dangereux en produisant les éléments suivants : une description générale, une définition des frontières du système et une description de ses interfaces, une définition de l'environnement, une description des flux d'énergie, de matières et d'informations aux travers des limites du système, et une définition des fonctions couvertes par l'analyse du risque.

La norme ISO 14971 [37] met en valeur les facteurs humains sans les nommer. Il est par exemple conseillé de « décrire l'environnement d'utilisation du dispositif, de définir qui se charge de l'installation du dispositif, et si le patient peut contrôler le dispositif médical ou influer sur son utilisation ». Ces considérations soulignent la nécessité d'effectuer une allocation des tâches entre les différents humains et le dispositif, en fonction des performances humaines. Cette norme aborde ce dernier point en évoquant l'importance des facteurs tels que « l'utilisateur prévu, ses capacités physiques et mentales, ses compétences et sa formation ». L'analyse de la tâche et l'allocation de la charge de travail sont des activités que l'on trouve dans la littérature sur les facteurs humains, mais qui n'apparaissent pas explicitement dans les normes actuelles dédiées au risque.

Alors que pour les robots industriels la tâche était entièrement réalisée soit par l'humain soit par le robot, le problème se pose différemment en robotique médicale. En effet, pour une même tâche, le spécialiste et le robot peuvent collaborer avec différents degrés d'interaction. Pour le développement de ces nouvelles applications, l'aspect d'analyse de la tâche avec prise en compte du comportement humain est devenu une étape complexe. Les codes du domaine médical et la complexité des tâches, telle qu'une opération chirurgicale, en font un travail délicat rendant indispensable une collaboration étroite entre ingénieurs et spécialistes du domaine médical.

Il est important de noter qu'aujourd'hui cette étape de l'analyse du risque est de plus en plus fortement liée à la modélisation du système, et donc à l'utilisation de langages de modélisation. L'hétérogénéité des systèmes de la robotique médicale (composants mécaniques, électroniques, informatiques, humains) conduisent à choisir des langages de haut niveau d'abstraction permettant de modéliser le système dans son ensemble. Un exemple d'une telle approche est donnée dans [24] où UML (*Unified Modeling Language*) est utilisé pour le développement d'un robot télééchographe.

4.3.2 Identification des phénomènes dangereux

L'étape d'identification des phénomènes dangereux connus et prévisibles est basée sur la définition du système obtenue précédemment. De nombreuses activités peuvent être utiles à l'identification des dangers dans des systèmes technologiques comme les robots médicaux telles que (liste non exhaustive) : la consultation des bases de données sur les expériences, les rapports sur les accidents et les incidents, l'utilisation de listes comme celle de la norme ISO 14971 [37], l'examen des sources et des transferts d'énergie, l'estimation des matières dangereuses (sub-

Composant	Modes de défaillance	Cause	A. Effet local B. Effet sur le système	Evaluation du risque			A. Moyens de détection possibles B. Solutions
				Occurrence	Gravité	Risque	
Contrôleur du robot	Figé	Interblocage du programme ou du système d'exploitation	A. Envoie commande constante B. Mouvement bloqué en un point	F	1	H	A. Système externe type watchdog B. Réinitialisation et Alerte utilisateur

FIG. 5 – Exemple de tableau de l'AMDEC

stances, rayons, systèmes de pression, etc.), la consultation des analyses de risque d'autres dispositifs, les sessions de *brainstorming*, la consultation d'experts, l'examen des interactions entre le patient, le robot et le spécialiste, et l'utilisation de techniques d'analyse.

Les techniques d'analyse partent soit de phénomènes dangereux, pour en déduire des situations dangereuses et des événements dommageables (on parle alors de techniques inductives ou *forward*), soit exploitent des dommages et des événements dommageables pour identifier les situations puis les phénomènes dangereux (analyses déductives ou *backward*). Parmi les techniques les plus utilisées en robotique, [17] retient l'AMDEC[9] (Analyse des Modes de Défaillance et de leurs Effets et de leur Criticité) comme technique *forward* et l'analyse des arbres de fautes[10] comme technique *backward*. Bien que les exemples d'utilisation de ces méthodes [42, 66] soient orientés vers des robots industriels, elles sont largement applicables aux robots médicaux [27, 28, 45]. Ces deux techniques souvent utilisées conjointement, sont aussi préconisées pour l'analyse du risque dans le domaine médical [37]. Ces méthodes sont particulièrement adaptées aux dispositifs médicaux car il est possible d'inclure certains aspects liés aux facteurs humains comme l'erreur humaine, et aussi de mélanger les différents domaines que sont la mécanique, l'électronique, et l'informatique, présents dans la réalisation d'un système robotique.

La figure 5 illustre l'utilisation d'un tableau pour l'AMDEC en ne prenant en compte que l'un des modes de défaillance pour le contrôleur de robot télééchographe TER [64] que nous avons développé. Il existe en effet d'autres modes de défaillance de ce composant comme la coupure (toutes les sorties nulles) qui peut être due à une chute de tension, ou encore le cas où les sorties deviennent aléatoires du fait d'un dépassement de mémoire ou d'un pointeur *fou* du programme. Le mode de défaillance analysé sur cet exemple est un contrôleur bloqué dans un état quelconque et ne donnant plus signe d'activité ; on utilise alors le terme de *figé*. La cause principale identifiée est l'interblocage entre tâches, ou une mauvaise gestion des ressources du système d'exploitation. On exprime également les effets, ainsi qu'une estimation du risque suivant les niveaux présentés dans le tableau de la figure 2. La solution envisagée pour maîtriser ce risque est l'utilisation d'un système de protection du type *watchdog* ou chien de garde.

[9] Ou FMECA, *Failure Modes, Effects and Critically Analysis*
[10] Ou FTA, *Fault Tree Analysis*

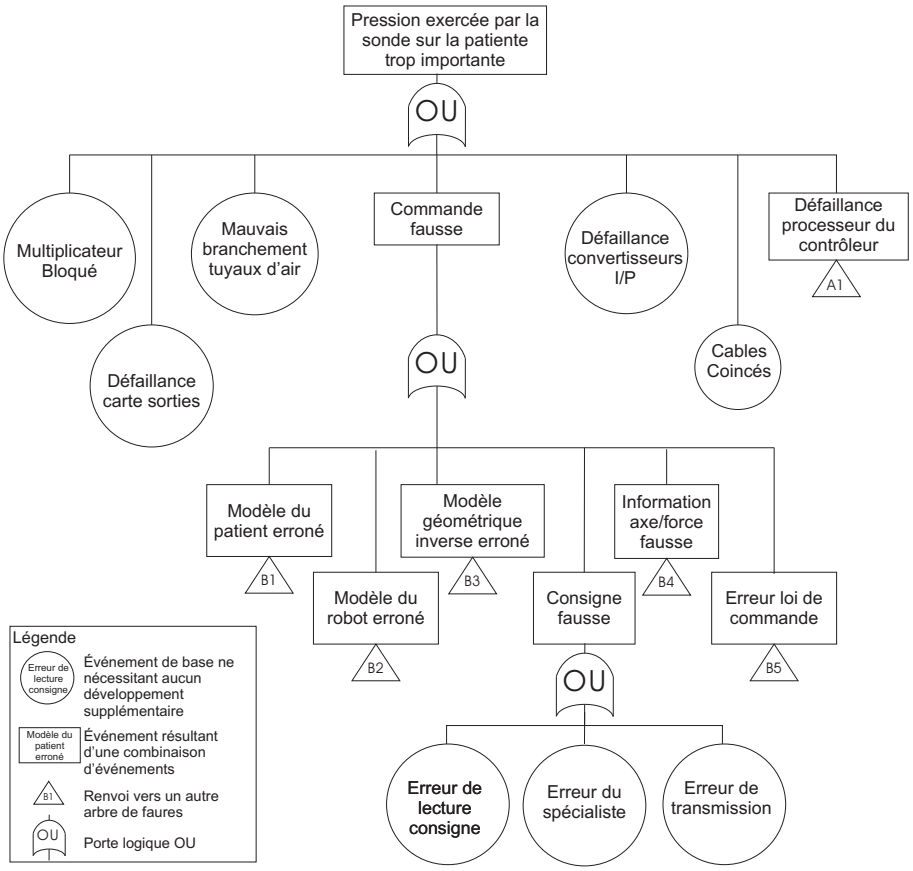

FIG. 6 – Exemple d'arbre de fautes

La figure 6 représente un arbre de fautes pour l'événement racine « *Pression exercée trop importante* »dans le cadre du robot TER pour l'échographie. Certaines particularités du système, comme l'utilisation de nouveaux actionneurs, les muscles artificiels fonctionnant avec de l'air comprimé, introduisent des événements dommageables liés à l'utilisation d'air (mauvais branchements des tuyaux d'air, défaillance des convertisseurs Intensité / Pression, etc.). Une analyse du risque plus détaillée incluant l'utilisation de ces techniques est présentée dans [24].

Parmi les points essentiels de cette étape de l'analyse du risque, il convient de noter l'importance de l'erreur humaine en tant que phénomène dangereux. Il est aujourd'hui devenu évident que ce thème est un des enjeux majeurs de la gestion du risque. Des domaines autres que la robotique médicale, comme l'avionique où l'erreur humaine est responsable de 70% des accidents, ou comme l'accident de Chernobyl, démontrent la nécessité d'intégrer cette problématique. Au sein de ce domaine d'étude un aspect important concerne les problèmes d'utilisation des interfaces homme-machine. Un des cas classiques illustrant cet aspect dans le domaine médical, est celui du Therac-25, évoqué précédemment (cf. section 2.1.2) présenté dans de nombreuses analyses [19][48, Annexe A]. Certains des accidents ont été provoqués par des séquences non prévues de manipulation par les utilisateurs. Ces derniers n'ont forcé ou désactivé aucune fonctionnalité, et les modifications pour bloquer les erreurs ont été introduites par la suite.

L'étude de l'erreur humaine est un domaine à la frontière des sciences cognitives [58, 47], et difficilement intégrée par les concepteurs. Comme exposé en 4.3.2, la complexité de cette discipline a souvent mené à l'utilisation de *checklists* et de règles de conception. Cependant ces moyens ne sont pas suffisants pour de nombreux systèmes et plus particulièrement pour les systèmes innovants. Face à cette problématique, les ingénieurs ont donc développé des heuristiques et des techniques comme THERP (*Technique for Human Error Rate Prediction*, développée par Swain au Sandia National Laboratories) permettant d'aider les concepteurs à adapter la tâche à l'humain.

4.3.3 Estimation du risque

D'après la définition fournie dans la section 2.2 le risque est fonction de la probabilité du dommage potentiel considéré. Cependant, en pratique cette estimation ne peut être faite sans calculer la probabilité des situations induisant ce dommage. On obtient alors de ces définitions les formules suivantes :

$$R_{dommage_k} = P_{dommage_k} \times C_{dommage_k}$$

$$\text{où } P_{dommage_k} = \sum_{toute\ situation_i\ induisant\ le\ dommage_k} P_{situation_i}$$

où $R_{dommage_k}$ est le risque de dommage k, $P_{dommage_k}$ est la probabilité d'occurrence du dommage k, et $P_{situation_i}$ la probabilité d'occurrence de la situation i.

L'estimation consiste donc à identifier la gravité des dommages et la probabilité des situations dangereuses conduisant à ce dommage. Le risque global est ensuite calculé à partir de ces données. Différentes approches existent pour exprimer le calcul du risque. Des versions précédentes de normes du domaine médical

[37] indiquaient que le risque pour chaque « phénomène dangereux »(et non situation dangereuse) devait être être calculé. Dans la norme IEC 61508 [32, Partie 5 - Annexe D], le terme utilisé est la probabilité de « l'événement dangereux ». L'estimation d'un risque, et notamment de sa probabilité, est donc une activité difficile à généraliser. La définition basée sur la situation dangereuse semble cependant englober ces différentes approches. Dans le cas du développement de système de la robotique médicale, cela permet d'identifier clairement qu'un dommage potentiel est lié à un scénario d'utilisation.

La principale difficulté provient du calcul de la probabilité d'occurrence d'un dommage. Comme cela a été évoqué précédemment (voir section 2.1.3) il est difficile voir impossible d'estimer quantitativement cette grandeur. Toute étude débute généralement par une estimation qualitative et lorsque cela est possible, elle est complétée par une étude quantitative. Dans les systèmes complexes comme les robots médicaux (mélangeant des aspects mécaniques, électroniques, informatiques et humains), il est naturel de se poser la question de la faisabilité et de la valeur d'une estimation quantitative. En particulier, il est impossible d'obtenir des données quantitatives ou qualitatives sur des probabilités de défaillance des composants logiciels. La méthode, utilisée actuellement dans de nombreux domaines et présentée dans plusieurs normes pour pallier cette méconnaissance ([39, 49, 18, 32]), est de donner au sous-système logiciel un niveau d'intégrité de sécurité à atteindre. Pour déterminer ce niveau d'intégrité à atteindre, les analyses se basent sur une analyse du risque du système global, et détermine alors l'impact sur la sécurité des défaillances des composants logiciels. Une seconde étape consiste à utiliser des techniques de développement différentes suivant le niveau d'intégrité déterminé. En définitive, plus ce niveau est élevé et plus le sous-système logiciel doit être intègre, et donc exempt de défaillances catastrophiques. La figure 7 donne un exemple de ces niveaux dans deux normes dédiées au développement de systèmes critiques militaires [49] et avionique [18]. Bien que ce concept soit très largement répandu dans les systèmes critiques, il est encore absent des travaux sur les logiciels de la robotique médicale.

4.4 Évaluation du risque

L'activité d'évaluation du risque concerne les prises de décisions d'acceptabilité du risque évoquées précédemment (cf. 2.2.3). Une première étape de l'évaluation consiste à isoler les dangers dont le risque estimé n'est pas suffisamment faible. Pour cela, les risques acceptés en raison de leur faible niveau ne sont pas étudiés. Par exemple, il est possible de décider que seuls les dangers induisant un risque de niveau T ou F de la figure 2 ne nécessiteront pas de réduction. En l'état actuel des choses, la détermination d'un niveau de risque acceptable est réalisée en utilisant les niveaux de risque acceptable de dispositifs médicaux déjà en service et ceux d'actes médicaux réalisés sans l'intervention d'un robot.

La deuxième étape consiste en l'étude des risques de niveau trop élevé, et dont la réduction est réalisable. Dans cette situation, il convient de réduire le risque au niveau aussi faible que raisonnablement praticable. Ce concept présenté sur la figure 8), se nomme ALARP (*As Low As Reasonably Practicable*). Cette figure

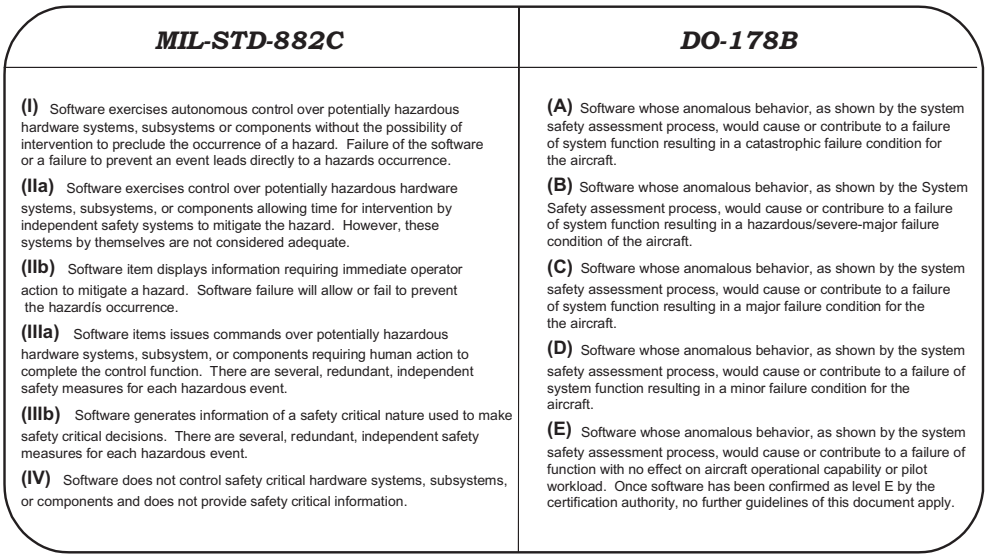

FIG. 7 – Comparaison entre les niveaux d'intégrité de deux normes logicielles [49, 18]
Le texte des normes est donné ici en version originale car il n'existe pas de version française, ni de correspondance normalisée pour la traduction de certains termes techniques

illustre les différents paliers d'acceptabilité du risque. Les concepts de protection et prévention présents sur cette figure seront expliqués ultérieurement.

Une fois le risque ramené en zone ALARP, la problématique risque encouru contre bénéfice et coût de réduction se pose. La figure 9 illustre ce principe pour la zone dite *tolérable*. Lorsqu'un risque se situe en zone ALARP, il est jugé tolérable si le bénéfice retiré et le coût important de réduction du risque justifient la prise de risque.

Cette balance entre risques et bénéfices, est sans doute la notion la plus controversée du processus de gestion des risques, puisqu'elle se base sur des concepts liés aux valeurs de la société concernée. En effet, comme cela a été présenté en partie 2.2.3, le risque est accepté dans un contexte donné, basé sur des valeurs courantes de notre société. Ce qui n'est pas explicite dans ces normes, est qu'un risque est acceptable d'une part parce qu'il se situe dans une limite comparable avec d'autres systèmes, mais surtout parce que la société est prête à l'accepter au regard des bénéfices qu'elle peut en tirer.

Dans le domaine des dispositifs médicaux - dont font partie les robots médicaux - la problématique intègre d'autres éléments. Ces robots qui assistent aujourd'hui les spécialistes réalisent généralement des tâches qui existaient auparavant[11]. Ainsi l'acceptabilité du risque peut se mesurer en comparant l'acte médical utilisant le robot, avec l'acte sans le robot. Une étude sur plusieurs années présentée par [6], compare

[11] Des applications permettant de réaliser de nouvelles opérations sont encore au stade de concept.

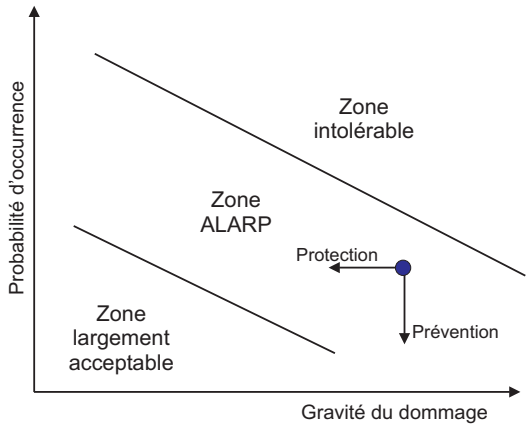

FIG. 8 – Exemple de diagramme des niveaux d'acceptabilité du risque et de la zone ALARP

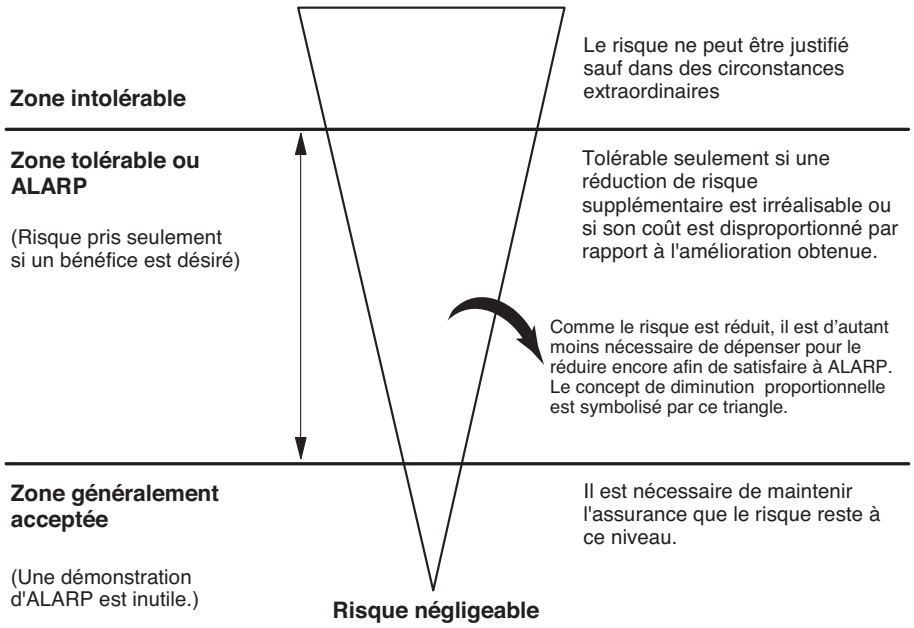

FIG. 9 – Illustration de l'acceptabilité du risque en fonction du coût, tiré de [29], et repris dans la norme [32]

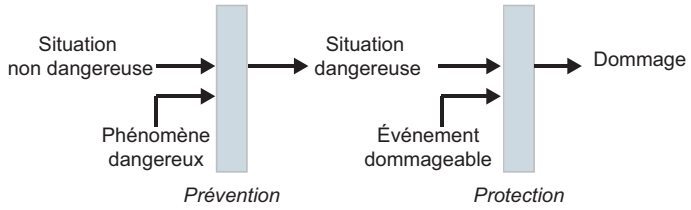

FIG. 10 – Prévention et protection vues comme des barrières de sécurité

les résultats des opérations du remplacement de la hanche par Robodoc avec ceux d'une équipe sans dispositif robotique. Les performances du robot ont été évaluées ainsi que les risques encourus puisqu'aucune opération n'a conduit a des dommages. Une autre comparaison entre un robot chirurgical et une équipe médicale classique est présentée par [59]. Cet article fournit uniquement des résultats en terme de performance de l'opération, mais il en ressort que la réalisation des tâches médicales s'est effectuée sans dommage. Pour les futures applications robotiques qui permettront d'effectuer des tâches jusqu'alors impossibles, la problématique de l'acceptabilité des risques sera plus complexe. En effet, l'absence de comparaison avec des opérations uniquement réalisées par l'humain, empêche de fixer les niveaux de risque acceptable. Le processus sera alors le même que pour des nouvelles opérations chirurgicales ; c'est le corps médical et la société qui prendront la décision de faire les essais cliniques et d'accepter un risque non nul.

4.5 Maîtrise des risques des systèmes de la robotique médicale

4.5.1 Principes généraux

La maîtrise du risque a pour objectif de réduire les risques. Deux approches sont généralement présentées : la *protection* qui vise à réduire la gravité du dommage et la *prévention* dont l'objectif est de réduire la probabilité d'occurrence du dommage. Ces concepts sont illustrés sur la figure 8 présentée précédemment. Ces termes sont souvent utilisés dans des dispositifs simples comme par exemple la mise en place d'extincteurs d'incendie dans des zones à risque (moyen de protection) et de panneaux d'interdiction de faire du feu (moyen de prévention). Mais pour des systèmes technologiques plus complexes comme les robots médicaux, la séparation entre ces deux concepts est moins évidente. Nous préférerons alors utiliser les termes de *protection contre les événements dommageables*, et de *prévention des situations dangereuses* en nous référant aux définitions données dans la section 3. La notion d'événement potentiellement dommageable permet d'inclure à la fois les événements dommageable, mais aussi les phénomènes dangereux et les situations dangereuses. Ces deux techniques de réduction du risque peuvent être vues comme des barrières de sécurité à différents niveaux de la chaîne causes/conséquences, depuis une situation dangereuse (incluant des phénomènes dangereux), jusqu'au dommage. Cette approche est illustrée par la figure 10.

Nous présentons dans cette section un état de l'art des techniques utilisées en

robotique médicale en abordant celles relevant de la prévention (section 4.5.2) puis celles concernant la protection (4.5.3). Les solutions technologiques présentées dans cette section sont en fait des patrons (ou *patterns* en anglais) de sécurité, puisqu'elles représentent des solutions connues à des problèmes particuliers dans un contexte donné. Il est évidemment très difficile de faire état de l'ensemble des techniques de maîtrise du risque en robotique médicale, et encore plus de les catégoriser. Cependant, la proposition qui est faite dans cette section permet de regrouper les principales techniques émergentes.

Signalons au préalable que les robots médicaux comme le robot échographe Hippocrate [14] ou le robot chirurgical Robodoc [7] ont souvent été réalisés à partir de robots industriels. Dans ce contexte les solutions techniques permettant d'augmenter la sécurité des robots ont été conservées voire améliorées. Les spécificités des tâches de la robotique médicale ont cependant amené les concepteurs à des solutions propres à chaque application (robotique de réhabilitation, robotique chirurgicale, etc.). Sur la base de ce constat, [12] présente des solutions technologiques et des principes sur lesquels peuvent se baser les concepteurs de tels systèmes. Ces solutions sont issues des exigences non fonctionnelles du système et de l'analyse du risque. Ainsi, toute utilisation d'une technique de maîtrise du risque doit trouver sa justification dans les résultats de l'analyse du risque. C'est cette approche qui est illustrée par [34] où, afin de réduire le risque de choc entre un robot et un humain, un indice de danger est calculé par le rapport entre la force possible produite par le robot et la force maximale que tolère un humain. En se basant sur l'identification et la quantification de ce danger, les auteurs proposent alors des solutions de conception et de contrôle logiciel des mouvements permettant de réduire ce danger.

4.5.2 Prévention des situations dangereuses

L'objectif des techniques de prévention est de réduire la probabilité d'occurrence de situations dangereuses, à travers des choix de conception, d'utilisation, ou de technologies de mise en oeuvre. Nous proposons de classer ces techniques de prévention suivant deux catégories :

- les techniques d'évitement des fautes permettant de garantir la réalisation effective des exigences fonctionnelles dont le non-respect engendrerait des situations dangereuses ;
- des choix de limitation de performances qui permettent en cas de faute ou non de réduire l'occurrence de situations dangereuses.

4.5.2.1 Évitement des fautes

La garantie de la réalisation effective des exigences fonctionnelles est un objectif complexe à atteindre, voire impossible pour des systèmes complexes comme les robots médicaux. Cependant, il existe un grand nombre de techniques utilisables pour le développement de robots médicaux déjà expérimentées dans des secteurs à sécurité critique comme le nucléaire, l'avionique, le ferroviaire, l'aéronautique, etc. Une classification de ces techniques de sûreté de fonctionnement est présentée dans [4], et notamment dans les deux catégories d'évitement des fautes : la prévention des

fautes et l'élimination des fautes. La prévention des fautes concerne principalement les techniques de développement de logiciel (langages de modélisation, processus de développement, etc.), et l'élimination des fautes s'appuie sur des techniques de test, de validation et de vérification. Nous ne nous référerons ici qu'aux principales techniques qui ont déjà été appliquées dans des systèmes de la robotique médicale ou dont l'utilisation est fortement dépendante des spécificités de ce domaine.

Évitement des fautes logicielles des contrôleurs de robot

Les contrôleurs de robots ont aujourd'hui atteint la complexité de nombreux systèmes informatisés. Les logiciels des robots médicaux sont d'autant plus complexes puisque les concepteurs explorent aujourd'hui de nouvelles architectures, capteurs, actionneurs, etc. Pour les directives européennes sur les dispositifs médicaux (incluant donc les robots médicaux), exposées ultérieurement dans la section 5, le logiciel est considéré comme un des éléments du dispositif médical, et doit être traité de la même manière que les autres composants au niveau de l'analyse du risque. Mais il n'existe pas encore de norme dédiée au logiciel médical qui serait analogue à la norme avionique DO178B [18] où sont recommandées des techniques de développement logiciel en fonction du niveau de criticité du logiciel. La seule recommandation que l'on peut extraire des directives est de suivre un système qualité de type ISO 9000, appliqué au logiciel médical comme cela est présenté dans [9]. Toutes ces techniques de prévention et d'élimination de fautes sont présentées dans des ouvrages comme [46, 22], mais tant qu'il n'existera pas de cadre normatif pour la réduction du risque des logiciels médicaux, le développement et l'utilisation de ces techniques seront fortement limités.

Évitement des fautes matérielles

Les fautes matérielles sur les robots industriels sont nombreuses et principalement dues aux capteurs et aux actionneurs, et leur occurrence peut mener à des situations dangereuses. Les premiers robots médicaux descendants directs de ces systèmes ont tout naturellement hérité de cette spécificité. Par exemple, la précision du mouvement articulaire d'un robot médical est une exigence fonctionnelle dont la dégradation constitue un phénomène dangereux pouvant engendrer des dommages. C'est le cas pour un robot pratiquant une opération au moyen d'un scalpel. Il existe aujourd'hui un ensemble d'actionneurs (principalement des moteurs électriques AC, DC, et pas-à-pas), qui ont des modes et des taux de défaillances connus et généralement fournis par les fabricants. La solution la plus commune à la maîtrise de ces défaillances est un programme de maintenance périodique préventive, qui s'applique à tous les composants matériels du système robotique et notamment à tout ce qui a trait aux articulations des robots. Au niveau des actionneurs, le choix des concepteurs s'est principalement porté sur les moteurs pas à pas, plus précis que les autres moteurs. En dehors des modes de défaillances des actionneurs, un des phénomènes qui dégrade la précision au niveau de l'articulation est le *backlash* (contre-mouvement dû au jeu des articulations sur un changement

de sens). Ce mode est réduit par le principe de transmission harmonique[12] (roues en forme d'ellipses). Dans le cadre du robot neuro-chirurgical Minerva, l'équipe de recherche a mis au point une solution dérivée de ce principe [23] ce qui a permis d'obtenir des écarts de positions bien inférieurs à ceux d'origine.

Une des solutions les plus utilisées pour éviter les fautes matérielles en opération est de maîtriser les étapes de mise sous tension et d'arrêt des systèmes robotiques. À la manière d'un décollage, ou d'une opération délicate dans une centrale nucléaire, il convient à la mise en route de tester les parties critiques et vérifier le bon état de marche du système. Cette activité qui s'effectue en général à l'initialisation, doit se faire avant le placement du patient pour qu'il soit protégé en cas de dysfonctionnement. Ceci permet d'identifier des capteurs ou des actionneurs défectueux mais également de détecter des anomalies dans les parties informatisées. À titre d'exemple, dans un système de robot chirurgical [45], les étapes essentielles des vérifications à la mise en route d'un robot médical concernent les tests de la mémoire et du processeur par le BIOS, les tests du *checksum* du code exécutable et des fichiers utilisés, les tests interactifs des capteurs et des actionneurs, et les tests des circuits d'arrêt.

Évitement des erreurs humaines

Les erreurs humaines sont dans les systèmes à sécurité critique, la cause de nombreuses catastrophes. Par extension, il est naturel de penser que les systèmes de la robotique médicale vont être confrontés au même problème. Ce vaste domaine d'étude relève de différentes disciplines, et se trouve au croisement de l'analyse des facteurs humains, des sciences cognitives et de la théorie des systèmes comme cela a été présenté dans la section 4.2. Une fois les erreurs identifiées, l'évitement est réalisé par la mise en place de choix de conception des interfaces ou du système, et des modifications d'utilisation ou des exigences. Une sous- branche importante de ce domaine est l'étude des interactions humain-ordinateur. Dans le cadre de la robotique médicale, les interfaces fournissent au spécialiste des informations sur l'état du système mais surtout les données essentielles relatives à la tâche (par exemple une image pour une opération chirurgicale ou pour une échographie). En cela, la qualité des informations sur l'état du système délivrées à l'opérateur, est une garantie de la bonne exécution de la tâche, et ainsi de la sécurité. De plus, le spécialiste utilisant un robot médical conserve sa responsabilité de médecin mais devient responsable du contrôle de la tâche, comme l'est un opérateur pour un robot industriel. Plusieurs problèmes se posent alors, et notamment l'analyse des erreurs humaines liées aux interfaces, les choix des messages d'alerte, les informations affichées, etc. Le risque est alors augmenté par la difficulté du praticien à percevoir l'état exact du patient et du robot, par exemple à travers une profusion d'informations mises à disposition sur des écrans.

Comme présenté en section 4.3.2, l'aspect cognitif de ces études étant complexe et éloigné des sciences de l'ingénieur, le choix est souvent fait de suivre des directives sous forme de listes de règles de conception, encore appelées « bonnes

[12] ou *harmonic drive*, produit d'une division de Quincy Technologies, Inc., USA.

pratiques »concernant principalement les interfaces humain machine. Cependant ces moyens sont insuffisants pour de nombreux systèmes et plus particulièrement pour les systèmes innovants. Ils ne donnent pas la solution exacte au problème lié à l'application mais une façon d'orienter la solution, et à ce titre ils ne garantissent pas la sécurité du système. Les interfaces suivent donc, comme pour tout composant du système, un cycle de vie itératif avec notamment une étape d'analyse du risque lié aux facteurs humains.

Parmi les erreurs humaines, il faut mentionner les actions non prévues des utilisateurs. Ainsi, dans de nombreuses applications médicales il est important que les mouvements du patient soient maîtrisés. Cet aspect inhérent à toute opération (robotisée ou non) est plus critique en robotique car les réactions du système face à un déplacement non prévu du patient sont difficiles à estimer. Une approche consiste à bloquer le patient, ou les membres critiques, au moyen de structures plastiques comme cela est présenté dans [53]. Les auteurs présentent également des phases plus ou moins critiques lors de l'opération robotisée (guidage d'une aiguille pour une injection très précise) et en déduisent différents modes opératoires du robot notamment en terme de vitesse de déplacement.

4.5.2.2 Prévention par la limitation des performances

Limitation logicielle de la vitesse des actionneurs

Le principe de limitation logicielle de la vitesse est déjà utilisé dans la robotique industrielle. Par exemple, lorsqu'un opérateur doit effectuer une tâche de maintenance ou programmer une nouvelle tâche robotique, la vitesse des mouvements peut être limitée à 20 cm/s. Cette valeur que l'on peut retrouver dans plusieurs études et dans certaines normes robotiques industrielles (comme par exemple la norme américaine ANSI/RIA R15.06-1999) ne convient pas aux applications de la robotique de service. Sa valeur a été fixée en fonction du temps de réponse de l'humain face à une défaillance. Pour des applications de robotique médicale cette valeur doit être adaptée en fonction de l'application et elle se situe évidemment pour de nombreuses applications bien en dessous de 20cm/s. Face à la variété des applications de la robotique médicale, il est évident qu'il est complexe d'envisager une norme commune pour la vitesse de déplacement du robot. Par exemple il est difficile de définir une vitesse commune à des opérations aussi différentes qu'une chirurgie invasise ou un examen échographique. Cependant, les vitesses de déplacement doivent être justifiées par une analyse du risque. C'est ce travail qui a été réalisé lors du développement d'un robot médical effectuant des injections précises [53]. Les auteurs ont en effet grâce à une analyse du risque défini des états du système plus ou moins critiques, et limité la vitesse en fonction de ces états.

Architecture mécanique

Certaines architectures permettent de prévenir certains risques de contact entre les humains et le robot. En effet, s'il existe des architectures lourdes, volumineuses, et rigides, d'autres sont étudiées pour leur légèreté, leur faible occupa-

tion et leur souplesse. Ainsi, à l'opposé d'Hippocrate [14], un bras manipulateur pour l'échographie basé sur un robot industriel, le projet TER [64], propose une structure dite parallèle restreignant l'amplitude, la force et la vitesse des mouvements. De plus, cette structure permet en cas de coupure d'alimentation en air, de n'exercer plus aucune pression sur la patiente car les actionneurs du robot étant des muscles artificiels se détendent en absence d'air. Les robots médicaux sont construits aujourd'hui pour intervenir sur de très petits espaces de travail, et des choix spécifiques au niveau de l'architecture contribuent également à respecter cette contrainte. Ainsi, pour une tâche très spécialisée, il est conseillé de réduire le nombre d'articulations. Ceci réduit alors le nombre de défaillances possibles et limite l'encombrement. Le robot neuro-chirurgical Minerva [23] possède seulement trois articulations (une translation et deux rotations). À l'opposé, un robot multitâche travaillant dans un milieu hostile possédera un plus grand nombre de degrés de liberté, éventuellement redondants. En complément à cette restriction, certains robots sont équipés de butées mécaniques très contraignantes (la rotation de Minerva est limitée à 30 degrés). Dans un autre domaine que la chirurgie, le robot médical de réhabilitation Tou [8], est dit intrinsèquement sûr grâce à sa structure molle. Il est constitué de six modules cylindriques en caoutchouc mousse. Le mouvement du bras est produit par la déformation adéquate de chaque module par des fils métalliques internes. L'angle de la déformation est limité à 30 degrés pour prévenir les irréversibilités de mouvement et les hystérésis excessifs. Des pliures plus importantes peuvent apparaître lorsque des forces extérieures agissent sur le robot. Si le guidage d'une telle architecture n'est pas précis, en revanche les caractéristiques de souplesse laissent supposer que dans un cadre humain de réhabilitation ce robot ne présente pas les risques de chocs habituels. Il faut noter tout de même que pour des applications de chirurgie, avec des exigences de précision importantes, il est impossible aujourd'hui d'utiliser une telle approche.

Souplesse des mouvements

La plupart des accidents de la robotique industrielle sont liés à l'énergie cinétique importante développée par des robots rapides, lourds et rigides. Pour prévenir ces dommages que l'on pourrait retrouver dans la robotique médicale, deux approches sont possibles. La première consiste à développer des contrôleurs combinant un contrôle en position et en force. Cette approche, nommée *compliance active*[13] est basée sur l'utilisation d'algorithmes implantés dans le contrôleur. À l'opposé, la *compliance passive* est l'utilisation de structures matérielles montées sur le poignet du robot. L'utilisation de poignets, ou plus généralement d'articulations, compliants permet de se rapprocher de la souplesse de l'homme. Le M.I.A. (*Mechanical Impedance Adjuster*) présenté dans l'article de [51], se compose principalement d'un ajusteur d'impédance (afin de régler la souplesse) et d'un entraînement d'articulation (pour transmettre le mouvement). La compliance consiste à régler un ressort directement joint à l'axe de l'articulation. La compliance passive peut également

[13] *Compliance* est un anglicisme que l'on trouve parfois traduit par *complaisance*, ou plus simplement par *souplesse*

FIG. 11 – Détail d'une articulation actionnée par des muscles artificiels de McKibben

être obtenue sans structure matérielle supplémentaire à l'actionneur. En effet, il est possible d'obtenir une compliance naturelle de l'actionneur. Les muscles artificiels décrits par [62] offrent une compliance très comparable aux articulations humaines (un exemple d'articulation est présenté figure 11). Ils contribuent ainsi à la sécurité intrinsèque du robot. Ils ont été utilisés pour le développement du robot télé-échographe TER [64] mais aussi dans le cadre de bras manipulateurs comme le robot ISAC[14] pour la réhabilitation des personnes âgées ou handicapées.

4.5.3 Protection contre les événements dommageables

Malgré l'utilisation de techniques de prévention des situations dangereuses, il est impossible de toutes les éviter. Il est donc nécessaire de concevoir des systèmes capables de se protéger malgré l'occurrence de situations dangereuses et d'événements dommageables. Beaucoup de techniques de protection consistent à détecter l'occurrence d'événements potentiellement dommageables et à y réagir, ou à masquer leurs effets. Ces événements peuvent provenir des humains (patient et praticien) ; leur détection sera abordée à la section 4.5.3.1. Les défaillances du robot constituent le second type d'événement qui doit être détecté (section 4.5.3.2). Un traitement classique dans le domaine de la sécurité robotique consiste à effectuer un arrêt d'urgence permettant une reprise du contrôle par un opérateur humain, mais d'autres moyens de traitement seront également présentés dans la section 4.5.3.3. Pour des événements plus complexes à détecter, nous présenterons un axe de recherche et des solutions possibles dans la section 4.5.3.4.

[14] Intelligent Soft Arm Control, http ://shogun.vuse.vanderbilt.edu/CIS/IRL/Projects/isaac.html

4.5.3.1 Détection des situations dangereuses dues à l'environnement humain

La principale source de danger pour la robotique industrielle est la présence de l'humain dans la zone de travail lors des opérations de maintenance. L'INRS [36] présente un ensemble des moyens de détection de l'humain dans cette zone, à proximité et au contact. Cependant, pour les applications de la robotique médicale, la tâche s'effectue en collaboration avec l'humain rendant certaines de ces solutions inadaptées. En dehors des dangers liés au domaine médical (nature biologique, liés à l'environnement, etc.), le danger principal est un déplacement du robot provoquant un dommage humain. Au niveau de la structure, même du robot il est possible d'utiliser des matériaux couvrant le robot et permettant de mesurer la force de contact ou la pression exercée en tout point [67]. Notons que parmi les solutions pour limiter la gravité des chocs, on doit également citer l'emploi de matières visco-élastiques [52].

Les capteurs d'effort permettent aussi de détecter une pression trop importante sur le patient et de modifier l'état du robot. Ainsi, en cas de dépassement d'une force maximale mesurée sur l'effecteur, le robot échographe Hippocrate [14], se débraye et le spécialiste peut déplacer manuellement le bras pour le mettre dans une position non dangereuse.

De nombreux systèmes robotiques utilisent aujourd'hui le retour d'effort en tant que variable de rétroaction en associant des capteurs de forces à l'effecteur ou aux articulations. Bien que cette technique soit étudiée depuis plusieurs années, elle est encore peu présente en robotique médicale, du fait notamment que le calcul de cette commande qualifiée d'*hybride* soit complexe, et que les données des capteurs de force soient difficiles à interpréter en termes de dommages sur l'homme. Dans le cas d'un robot chirurgical, il est très difficile lors d'une opération de mesurer l'ensemble des efforts sur l'outil chirurgical. L'emploi d'actionneurs compliants, présentés précédemment (cf. section 4.5.2.2), améliore la sécurité sans recours à un calcul de force. Il apparaît comme une solution préventive d'avenir pour un geste médical plus sûr.

L'occurrence de situations dangereuses peut aussi être due au praticien. Celui-ci peut interrompre inopinément l'opération, par exemple du fait d'une incapacité temporaire à la superviser. Pour détecter cette situation dangereuse, des dispositifs obligent l'opérateur humain à maintenir constamment un interrupteur dans une même position lors des mouvements du robot. Ce principe que l'on retrouve dans de nombreux systèmes de la robotique industrielle, est nommé interrupteur homme-mort ou DMS (*Dead Man Switch*). Il a été également utilisé pour des robots médicaux comme Acrobot (robot chirurgical orthopédique [13]) sous forme de *gâchette* ou sous forme de pédale comme sur le robot échographe Hippocrate [14].

4.5.3.2 Détection des défaillances du robot

Les défaillances du robot médical constituent des phénomènes dangereux qui doivent être détectés et traités en tant qu'événements potentiellement dommageables. En phase opérationnelle, la détection d'erreur est généralement mise en

œuvre par des techniques de redondance. La redondance structurelle consiste à multiplier les composants matériels du robot comme les actionneurs, les capteurs, les cartes contrôleur, etc. Les données produites par ces composants peuvent ensuite être comparées et certains composants écartés en raison d'une défaillance détectée. Cette technique de protection, utilisée dans les systèmes à sécurité critique comme l'avionique est aujourd'hui employée en robotique [45]. Par exemple, le robot chirurgical Robodoc possède pour chaque articulation deux codeurs incrémentaux (données de position), et les données sont comparées à tout instant par deux processeurs [7].

La redondance fonctionnelle est un autre type de redondance qui permet d'effectuer une même fonction mais avec une conception différente. Ainsi, il est possible de retrouver une donnée de vitesse avec des capteurs de vitesse mais aussi depuis des données de position et d'accélération du mouvement. La redondance peut aussi s'effectuer à un niveau de conception plus élevé. [45] présentent une application d'un patron de sécurité, l'utilisation d'un *double canal* à un robot chirurgical. Ce système est composé de deux canaux de traitement informatique, symétriques mais de conceptions différentes. Tout comme la redondance structurelle, cette technique est en général limitée par les coûts, l'espace, la consommation d'énergie et la complexité du système.

4.5.3.3 Arrêt d'urgence et arrêt contrôlé

Après la détection d'événements potentiellement dommageables, le système doit les traiter pour s'affranchir de tout dommage potentiel. Il se pose alors la question de la mise en état sûr qui peut être très problématique dans certaines applications de la robotique médicale.

Si la détection est réalisée par le contrôleur de robot, c'est le logiciel qui enclenchera une procédure de traitement. Cependant, dans les applications d'aujourd'hui, la détection et le traitement pour la sécurité sont généralement réalisées sans traitement informatique. Le plus classique est l'arrêt d'urgence généralement déclenché par l'opérateur humain. Pour les robots industriels par exemple, l'appellation *arrêt d'urgence* n'est valide que si le circuit est dit « figé »[36], ce qui veut dire sans aucun traitement informatique. Ces systèmes sont généralement doublés par des boutons poussoirs directement reliés aux sources d'énergie.

Une fois l'arrêt d'urgence activé, différents systèmes de blocage des articulations peuvent être intégrés. [65] utilisent des systèmes de freins débrayables électromagnétiques que l'on trouve sur des robots industriels commercialisés, comme le Mitsubishi MoveMaster (bras manipulateur à 6 axes), couplés à des moteurs électriques. Il existe aussi des systèmes de freins utilisés par [55], qui s'enclenchent lors des coupures d'énergie. Le robot Wendy [50] possède un système fonctionnant sans logiciel qui permet d'enclencher des freins électromagnétiques si le bras dépasse une vitesse limite. [15] présente le mécanisme de plusieurs systèmes, notamment le concept de Transmission Continûment Variable utilisé par Cobot[15], et le système de roue libre utilisé par le robot Padyc [63]. Ce système est mis en œuvre par un ensemble de

[15] http ://othello.mech.nwu.edu/~peshkin/cobot/index.html

billes qui se coincent dans des cavités, bloquant alors seulement dans un sens la rotation d'une bague extérieure. Prévu à la base pour une restriction de l'espace de travail du robot (le geste chirurgical est alors contraint), il est possible de l'utiliser pour un blocage en cas d'arrêt d'urgence.

Il ne convient cependant pas toujours d'utiliser des systèmes de blocage des articulations. En effet, en cas de panne, l'arrêt pourrait s'avérer dangereux dans certaines circonstances. Certains sites robotisés utilisent ainsi des systèmes hydrauliques secondaires pour des robots manipulant des charges très lourdes. En cas de défaillance, cette installation prend le relais et redescend doucement le bras chargé sur la plate-forme robotique. Dans le cas du robot télé-échographe TER, les choix de conception ont permis d'adopter un arrêt d'urgence sans blocage ou frein. La sonde, maintenue par quatre câbles, repose sur le ventre de la patiente, et ces câbles sont actionnés par des muscles artificiels de McKibben qui se rétractent lorsque la pression d'air augmente. Ils permettent ainsi de déplacer l'anneau où se trouve la sonde. Le fait de couper toute alimentation d'air, détend les quatre muscles, et la pression sur le ventre de la patiente devient nulle. Dans ce cas particulier, l'arrêt d'urgence est très simple et place directement le système dans un état sûr. Cet exemple montre que des corrélations existent entre les choix d'architecture, les choix des actionneurs et la sécurité. Cet aspect constitue une prospective importante de recherche.

Un autre arrêt que l'on peut dériver des robots industriels est l'*arrêt contrôlé* [60]. À l'opposé de l'arrêt d'urgence, l'arrêt contrôlé permet de conserver le robot sous le contrôle du système de commande. Il équivaut à un état de pause dans lequel le système se met dans l'attente d'une instruction supplémentaire. Cependant, le choix entre arrêt d'urgence (où l'on coupe les moyens énergétiques des actionneurs) et arrêt contrôlé (les actionneurs sont encore alimentés) doit résulter d'une analyse du risque exprimant très clairement les conséquences et les risques induit par ces deux arrêts.

4.5.3.4 Dispositifs externes de sécurité

De nombreux systèmes à sécurité critique intègrent un sous-système permettant de vérifier en temps réel des propriétés de sécurité du système global [21]. Cette technique de protection apparaît sous de nombreuses appellations : *external monitoring system*, *safety-related subsystem*, *safeguard*, *protective system*, *safety supervisor*, *safety bag*, etc. Elle s'appuie sur le principe de la diversification en distinguant deux chaînes de traitement : une chaîne fonctionnelle et une chaîne de contrôle. La première est dédiée à la réalisation des fonctions du système, et la seconde est destinée au contrôle de la première. La chaîne de contrôle est constituée par un ensemble d'assertions exécutables déduites des propriétés de sécurité que le système doit respecter pour éviter les dommages. Peu de systèmes robotiques, et encore moins en robotique médicale, ont utilisé cette approche que l'on retrouve cependant dans de nombreux domaines [26].

Dans le domaine de la robotique de service, en contact avec l'humain, [5] expose un système avec une carte principale, des cartes contrôleurs pour chaque articulation, et une carte sécurité divisée elle-même en deux modules : un module de

contrôle de la carte principale, et un module de contrôle des cartes contrôleurs des articulations. Les informations sont donc analysées et comparées par différents modules. En cas de détection de défaillance, le processeur doit appliquer une politique de sécurité qui peut être le recouvrement d'information (on effectue un retour en arrière sur les données sauvegardées), ou même la réinitialisation du système. Dans la même démarche, [35] présente un système de ce type mais intégré entre la couche décisionnelle et la couche fonctionnelle d'un contrôleur de robot mobile évoluant en milieu humain. Ce dispositif, nommé contrôleur d'exécution, vérifie la cohérence des requêtes transmises par le superviseur vers la couche fonctionnelle mais également des flots de données échangés entre les modules fonctionnels.

5 Assurance de la sécurité : la certification

La certification a pour but de fournir à un client la garantie qu'un produit est conforme à sa spécification et notamment en terme de sécurité. Dans notre cas, les spécifications de sécurité sont au centre du problème. Cette certification est généralement délivrée par un organisme tiers comme G-MED[16] dans le domaine médical, qui depuis quelques années se penche sur le cas des robots médicaux. Cette section présente de manière synthétique comment les systèmes de la robotique médicale se trouvent confrontés à la certification.

5.1 Certification et risque

Bien qu'une analyse du risque ne puisse suffir à l'obtention d'une certification, elle constitue néanmoins le cœur des principales exigences actuelles en terme de certification. Afin d'harmoniser et d'assurer un haut niveau de sécurité, trois directives européennes, [1], [2], et [3], couvrent l'ensemble des équipements médicaux. Ces directives définissent un dispositif réglementaire pour la certification (marquage CE obligatoire) et expriment les exigences essentielles de sécurité. Il existe à un niveau plus technique, un ensemble de normes dédiées aux dispositifs médicaux qui concernent des aspects plus applicatifs, et la manière de mettre en œuvre les exigences des directives. Il est cependant important de noter que dès ces premières directives de très haut niveau conceptuel, l'accent est mis sur l'analyse du risque. La directive [2] l'exprime ainsi dans la première des exigences essentielles :

> *« Les dispositifs médicaux doivent être conçus et fabriqués de telle manière que leur utilisation ne compromette pas l'état clinique et la sécurité des patients ni la sécurité et la santé des utilisateurs,[...], étant entendu que les risques éventuels liés à leur utilisation constituent des risques acceptables au regard du bienfait apporté au client ».*

Comme pour la définition de la sécurité, il ressort de cette directive une valeur relative de la prise de risque faisant référence à la notion d'acceptabilité reliée aux bénéfices fournis. Ainsi, l'importance des étapes d'analyse et d'évaluation du risque apparaît clairement pour tout dispositif médical. De plus, l'organisme de

[16] http ://www.gmed.fr/

certification doit pouvoir accéder aux données et aux résultats de l'analyse du risque.

5.2 Classification des dispositifs médicaux

Le processus de certification fait appel à plusieurs étapes entièrement dépendantes de la classe à laquelle appartient le dispositif. La classification se fait en fonction du type d'interaction avec le patient. On peut résumer ces classes à [2] :

- classe I : dispositifs non invasifs ;
- classe IIa : dispositifs actifs échangeant de l'énergie ;
- classe IIb : dispositifs actifs échangeant de l'énergie potentiellement dangereuse ;
- classe III : dispositifs implantables ou dispositifs invasifs à long terme.

La plupart des robots médicaux appartiennent à la catégorie IIa et IIb. La classe III concerne les dispositifs en rapport avec le cœur ou le système nerveux, qui pour la plupart sont implantés dans le corps humain (comme les *pacemaker*). Les robots chirurgicaux comme Robodoc appartiennent à la classe IIb ainsi que les robots non invasifs mais utilisant une énergie ionisante (un robot échographe par exemple). Cette classification exprime un niveau d'interaction avec le patient sans préciser explicitement le niveau de risque correspondant. La notion de défaillance n'est pas abordée dans cette classification. Il est intéressant de noter que dans un domaine comme l'avionique, la norme logicielle DO178B [18] fait référence à l'*effet de la défaillance* d'un élément pour la classification (catastrophique, dangereux, majeur, mineur, aucun effet). Cette référence fait défaut dans les systèmes médicaux où tout est centré sur l'humain et la proximité du dispositif, sans attribuer directement un niveau de risque à chaque classe. En effet, une défaillance d'un dispositif de la classe III peut avoir un effet moins grave qu'une défaillance d'un dispositif de la classe IIb. Les notions de défaillance et d'effet ne sont abordées que dans les normes sur la gestion du risque. La différence d'approche entre l'avionique et le médical tient au fait que ce dernier domaine aborde depuis peu la notion de système, et de ce fait ne possède encore que des normes de haut niveau. En devenant plus techniques, les normes du domaine médical devraient permettre d'exprimer les raisons d'une telle classification.

5.3 Processus de certification

Dans le cadre d'une étude de la sécurité, et en vue de la certification, il est obligatoire de classer le dispositif comme présenté dans la section précédente. En fonction de la classe du dispositif, la procédure de preuve de conformité devient plus contraignante. En effet, pour un dispositif de classe I, seule une auto-déclaration du fabricant est nécessaire. Pour des dispositifs comme les robots médicaux (classe IIa et IIb), il est exigé un examen complet de conception. Cela consiste à fournir à l'organisme de certification, une trace (un dossier) contenant l'ensemble des informations sur le processus qualité qui a été appliqué (en général de type ISO 9000), les informations sur la gestion des risques, et les informations sur la conception

même du dispositif. Cette procédure, qui met l'accent sur le processus de conception plutôt que sur le produit lui-même, est commune à de nombreux domaines. Il apparaît néanmoins dans le domaine médical une absence de normes ou de guides relatifs à la production du dossier de certification. Dans le domaine des transports, on retrouve au contraire cette notion dans la rédaction des *safety cases* [56], qui ne trouvent pas leur équivalent dans le médical. Il existe cependant des normes pour guider le fabricant dans l'application du processus qualité, comme par exemple la norme [54] qui exprime les particularités de l'utilisation de l'ISO 9003 à la conception d'un dispositif médical. On retrouve alors des éléments comme le *dossier de gestion des risques* et d'autres dossiers relatifs au processus. Les relations entre l'utilisation de ces normes et la rédaction du document pour la certification, restent néanmoins peu explicites.

6 Conclusion

Les technologies ont aujourd'hui atteint un tel niveau de développement, qu'il est désormais possible de transférer au robot un ensemble de responsabilités et de fonctions jusqu'alors réservées exclusivement aux humains. Le domaine de la robotique de service, et plus particulièrement de la robotique médicale, est un exemple représentatif de cette évolution. Dans ce cadre, se pose la problématique de la confiance accordée à ces systèmes technologiques, et notamment celle de la sécurité.

La complexité de tels systèmes est telle qu'il est impossible de garantir aujourd'hui une sécurité absolue. Ainsi, il n'existe pas d'outils ou de techniques permettant de s'affranchir de tout risque pour les utilisateurs de robots médicaux. Par conséquent, pour gérer au mieux cette problématique, une première approche se base sur la notion de risque, qui intègre le caractère relatif de la sécurité. Pour cela, cet article a repris les notions de base, comme le dommage, le risque et le danger pour faire le lien entre les normes internationales et la recherche en robotique médicale sur ces sujets.

Nous avons choisi de décomposer la gestion du risque en trois étapes comme cela est proposé par certaines normes : l'analyse du risque, l'évaluation du risque et la maîtrise du risque. Au sein du processus de gestion du risque subsistent deux points essentiels en cours de développement. Tout d'abord l'inclusion des facteurs humains dans les différentes activités n'est pas explicite, et nous avons montré comment il était possible de prendre en compte ce concept à plusieurs niveaux du processus de gestion des risques. Le second point concerne l'estimation du risque pour le logiciel qui constitue un élément de plus en plus important des robots médicaux. Il est en effet difficile d'estimer la probabilité d'occurrence de défaillance d'un logiciel. Cette problématique est en partie traitée par l'introduction des SIL (*Software Integrity Level*) au sein de différentes normes. Cette démarche est actuellement absente des normes dédiées aux dispositifs médicaux ou aux robots de service. Mais au vu de l'évolution de ces systèmes, ce travail devrait être bientôt réalisé.

Afin de mettre en application les activités de la gestion du risque, des techniques sont utilisées mais ne couvrent que certains aspects du processus. Ainsi, l'analyse

du risque est en partie traitée par l'utilisation de techniques comme l'AMDEC ou les arbres de fautes. Ces techniques largement utilisées dans d'autres domaines sont aujourd'hui applicables à des dispositifs comme les robots de service. Les principales techniques pour la réduction du risque ont ensuite été présentées, en se concentrant sur deux aspects : la prévention et la protection des risques. Beaucoup de techniques utilisées dans la robotique industrielle, mais aussi dans l'avionique ou le nucléaire, sont utilisables pour la robotique médicale. Les particularités des applications médicales nécessitent cependant des investigations qui n'existaient pas jusqu'ici, en particulier sur de nouvelles architectures, de nouveaux actionneurs, et sur l'intégration des facteurs humains du fait du couplage fort existant entre le système, le patient et le praticien. Ces thèmes de recherche ont une incidence directe sur la sécurité, qui est la contrainte principale pour le développement de nouvelles applications de robots médicaux.

Afin de valider qu'une conception a bien intégré les différents concepts relatifs à la sécurité, la société propose un système d'assurance par le biais de la certification. Dans le cas des dispositifs médicaux, c'est un ensemble de directives qui définit le cadre légal de la certification. Nous avons montré comment cette réglementation intègre les aspects liés au risque, présentés dans les sections précédentes. Comme pour des démarches qualité de type ISO 9000, nous avons montré comment la certification des dispositifs médicaux dont font partie les robots médicaux, se base plus sur la manière dont le système est conçu que sur l'évaluation du système lui-même. L'observation des informations de conception ne peut se faire que si la documentation a été correctement réalisée, et permet notamment la *traçabilité* des choix de conception.

Cet article pose les bases de l'activité de gestion du risque, permettant de prendre en compte l'ensemble des composantes d'un système aussi complexe qu'un robot médical. Cette approche montre bien que sur la base de concepts communs à de nombreux domaines, il est possible de les utiliser en intégrant les spécificités du domaine médical. Il reste malgré tout à développer un véritable cadre d'étude (et normatif) pour ces systèmes, en développant de nouvelles techniques, mais également en continuant à intégrer celles des autres systèmes à sécurité critique.

Références

[1] 90/385/CEE. Directive du conseil du 20 juin 1990 relative aux dispositifs médicaux implantables actifs. Journal Officiel des Communautés Européennes (JOCE) N°L189, 1990.

[2] 93/42/CEE. Directive du conseil du 14 juin 1993 concernant les dispositifs médicaux. Journal Officiel des Communautés Européennes (JOCE) N°L169, 1993.

[3] 98/79/CE. Directive du parlement européen et du conseil du 27 octobre 1998 relative aux dispositifs médicaux de diagnostic in vitro. Journal Officiel des Communautés Européennes (JOCE) N°L220, 1998.

[4] A. Avižienis, J. C. Laprie, B. Randell, and C. Landwehr. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1) :11–33, 2004.

[5] A.J. Baerveldt. A safety system for close interaction between man and robot. In *Safety of Computer Control Systems SAFECOMP'92*, pages 25–29. Elsevier, 1992.

[6] W.L. Bargar, A. Bauer, and M. Borner. Primary and revision total hip replacement using the ROBODOC system. Joint Surgeons of Sacramento, 1998. http ://www.jointsurgeons.com/clinical.htm.

[7] P. Cain, P. Kazanzides, J. Zuhars, B. Mittelstadt, and H. Paul. Safety considerations in a surgical robot. In *Proc. of the 30th Annual Rocky Mountain Bioengineering Symposium*, pages 291–194, San Antonio, 1993. Biomedical Sciences Instrumentation.

[8] A. Casals, R. Villà, and X. Cufi. Tou, an assistant arm : Design, control and performance. In *Proc. 6th International Conference on Advanced Robotics ?ICAR93, Tokyo, Japan*, pages 355–360, 1993.

[9] P.S. Cosgriff. Quality assurance of medical software. *Journal of medical engineering and technology*, 8(1) :1–10, 1994.

[10] M. Daouk and N. Leveson. An approach to human-centered design. In *Workshop on Human Error and System Development, Linkoping, Suède*, 2001. http ://sunnyday.mit.edu/safety.

[11] P. Dario, E. Guglielmelli, B. Allotta, and M.C. Carrozza. Robotics for medical applications. *IEEE Robotics and Automation Magazine*, 3(3) :44–56, 1996.

[12] B. Davies. Safety of medical robots. In *Proceedings of International Conference on Advanced Robotics ICAR'93, Tokyo, Japan*, pages 311–313. IEEE Publisher, 1993.

[13] B.L. Davies, S.J. Harris, W.J. Lin, R.D. Hibberd, R. Middleton, and J.C. Cobb. Active compliance in robotic surgery - the use of control as a dynamic constraint. *Journal of Engineering in Medicine - Part H*, 211(4) :285–292, 1997.

[14] E. Degoulange, L. Urbain, P. Caron, S. Boudet, J. Gariepy, F. Pierrot, and E. Dombre. Hippocrate : an intrinsically safe robot for medical applications. In *IEEE/RSJ International Conference on Intelligent Robots and Systems IROS98*, volume 2, pages 959–964, 1998.

[15] Y. Delnondedieu. *Un robot à sécurité passive en réponse aux problèmes d'ergonomie et de sécurité en Robotique médicale*. PhD thesis, Institut National Polytechnique de Grenoble, France, 1997.

[16] B.S. Dhillon. *Robot reliability and safety*. Springer-Verlag, 1991.

[17] B.S. Dhillon and A.R.M. Fashandi. Safety and reliability assessment techniques in robotics. *Robotica*, 15 :701–708, 1997.

[18] DO178B/ED-12 Revision B. Software considerations in airbone systems and equipment certification. Requirement and Technical Concepts for Aviation (RTCA) Inc., 1992.

[19] I. Edmond and M. William. Human factors risk management as a way to improve medical device safety : A case study of the Therac 25 radiation therapy system. *Joint Commission Journal on Quality and Patient Safety*, 30(12) :689–695(7), 2004.

[20] Food and Drug Administration. Medical device use-safety : incorporating human factors engineering into risk management. Technical report, U.S. Departement of Health and Human Service, 2000.

[21] J. Fox and S. Das. *Safe and sound - Artificial intelligence in hazardous applications*. AAAI Press - The MIT Press, 2000.

[22] J.C. Geffroy and G. Motet. *Sûreté de fonctionnement des systèmes informatiques*. InterEditions, Paris, 1998.

[23] D. Glauser, P. Flury, CW. Burckhardt, and M. Kassler. Mechanical concept of the neurosurgical robot Minerva. *Robotica*, 11(6) :567–575, 1993.

[24] J. Guiochet. *Maîtrise de la sécurité des systèmes de la robotique de service - Approche UML basée sur une analyse du risque système*. PhD thesis, Institut National des Sciences Appliquées de Toulouse, 2003.

[25] J. Guiochet, G. Motet, C. Baron, and G. Boy. Toward a human-centered UML for risk analysis - application to a medical robot. In *WCC 18th IFIP World Computer Congress, Human Error Safety and System Development*, August 2004.

[26] J. Guiochet and D. Powell. Étude et analyse de différents dispositifs externes de sécurité-innocuité de type safety bag. Technical Report 0555, LAAS-CNRS, Toulouse, France, November 2005.

[27] J. Guiochet, B. Tondu, and C. Baron. Safety analysis and integration for robotic systems - application to a medical robot for tele-echography. In M.H. Hamza, editor, *Proc. of the IASTED International Conference on Robotics and Applications (RA'01), Tampa, USA*, pages 158–162. ACTA press, November 2001.

[28] J. Guiochet and A. Vilchis. Safety analysis of a medical robot for tele-echography. In *Proc. of the 2nd IARP IEEE/RAS joint workshop on Technical Challenge for Dependable Robots in Human Environments, Toulouse, France*, pages 217–227, October 2002.

[29] HSE. Reducing risk, protecting people. Technical report, Health and Safety Executive, UK, 1999. http ://www.hse.gov.uk.

[30] HSE. Proposed framework for addressing human factors in IEC 61508. Technical Report 373/2001, Health and Safety Executive, UK, 2001. http ://www.hse.gov.uk.

[31] IEC 60300-3-9. Dependability management - Part 3 : Application guide - Section 9 : Risk analysis of technological systems. International Electrotechnical Commission, 1995.

[32] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission, 2001.

[33] IARP / IEEE-RAS. Dependability in human-friendly robots - special issue. *IEEE Robotics and Automation Magazine*, 11, June 2004.

[34] K. Ikuta and H. Ishii. Safety evaluation method of design and control for human-care robot. *The International Journal of Robotics Research*, 22(5) :281–297, 2003.

[35] F. Ingrand and F. Py. An execution control system for autonomous robots. In *Proceedings IEEE International Conference on Robotics and Automation*, Washington D.C., USA, May 2004.

[36] INRS. Sites robotisés - Guide technique de sécurité. Technical Report ND 1728-135-89, Institut National de Recherche et de Sécurité, Paris, Mai 1998.

[37] ISO 14971. Dispositifs médicaux - Application de la gestion des risques aux dispositifs médicaux. International Organization for Standardization, 2000.

[38] ISO/CEI Guide 51. Aspects liés à la sécurité - Principes directeurs pour les inclure dans les normes. International Organization for Standardization, 1999.

[39] ISO/IEC 15026. Information technology - system and software integrity levels. International Organization for Standardization, 1998.

[40] ISO/IEC Guide 73. Risk management - Vocabulary - Guidelines for use in standards. International Organization for Standardization, 2002.

[41] W. Johnson. *MORT safety assurance systems*. Deker, Marcel Incorporated, 1980.

[42] K. Khodabandehloo. Analyses of robot systems using fault and event trees : case studies. *Reliability Engineering and System Safety*, 53 :247–264, 1996.

[43] W. Korb, M. Kornfeld, W. Birkfellner, R. Boesecke, M. Figl, M. Fuerst, J. Kettenbach, A. Vogler, S. Hassfeld, and G. Kornreif. Risk analysis and safety assessment in surgical robotics : A case study on a biopsy robot. *Minimally Invasive Therapy and Allied Technologies*, 14(1) :23–39, 2005.

[44] B. M. Kraft, C. Jäger, B. J. Leibl K. Kraft, and R. Bittner. The AESOP robot system in laparoscopic surgery : Increased risk or advantage for surgeon and patient ? *Surgical Endoscopy*, 18, August 2004.

[45] U. Laible, T. Bürger, and G. Pritschow. A fail-safe dual channel robot control for surgery applications. *Safety Science*, 42 :423–436, 2004.

[46] J-C. Laprie, J. Arlat, J-P. Blanquart, A. Costes, Y. Crouzet, Y. Deswarte, J-C. Fabre, H. Guillermain, M. Kaâniche, K. Kanoun, C. Mazet, D. Powell, C. Rabéjac, and P. Thévenod. *Guide de la sûreté de fonctionnement*. Cépaduès - Éditions, Toulouse, France, 1995.

[47] J. Leplat. *Erreur humaine, fiabilité humaine dans le travail*. Armand Colin, 1985.

[48] N.G. Leveson. *Safeware - System safety and computers*. Addison-Wesley, 1995.

[49] MIL-STD-882C. System safety program requirements. Military Standard, Departement of Defense, U.S.A., 1993.

[50] T. Morita, H. Iwata, and S. Sugano. Development of human symbiotic robot : WENDY. In *Proceedings 1999 IEEE International Conference on Robotics and Automation*, volume 4, pages 3183–3184, 1999.

[51] T. Morita and S. Sugano. Development of an anthropomorphic force controlled manipulator WAM 10. In *8th International Conference on Advanced Robotics*, pages 701–706, 1997.

[52] T. Morita and S. Sugano. Double safety measure for human symbiotic manipulator. In *IEEE/ASME International Conference on Advanced Intelligent Mechatronics'97*, page 130, 1997.

[53] M. Nagel, G. Schmidt, G. Schnuetgen, and W.A. Kalender. Risk management for a robot-assisted needle positioning system for interventional radiology. In *CARS*, pages 549–554, 2004.

[54] NF EN 46003. Systèmes qualité - Dispositifs médicaux - Exigences particulières relatives à l'application de l'EN ISO 9003. International Organization for Standardization, 1999.

[55] W.S. Ng and C.K. Tan. On safety enhancements for medical robots. *Reliability Engineering and System Safety*, 54(1) :34–45, 1996.

[56] Y. Papadopoulos and J.A. McDermid. The potential for a generic approach to certification of safety critical systems in the transportation sector. *Reliability Engineering and Systems Safety*, 63 :47–66, 1998.

[57] J. Pransky. Robodoc - surgical robot success story. *Industrial Robot*, 24(3) :231–233, 1997.

[58] J. Reason. *Human Error*. Cambridge University Press, 1990.

[59] H. Reichenspurner, D.H. Boehm, H. Gulbins, C. Schulze, S. Wildhirt, C. Detter, and B. Reichart. Three-dimensional video and robot-assisted port-access mitral valve operation. *The Annals of Thoracic Surgery*, 69 :1176–82, 2000.

[60] B. Saintot, D. Pagliero, and J. Brémont. Performances d'arrêt d'urgence des robots manipulateurs industriels. Technical Report CDU 658-564, Institut National de Recherche et de Sécurité, 1991.

[61] R.H. Taylor and D. Stoianovici. Medical robotics in computer-integrated surgery. *IEEE Transactions on Robotic and Automation*, 19(5) :765–781, 2003.

[62] B. Tondu, S. Ippolito, J. Guiochet, and A. Daidié. A seven-degrees-of-freedom robot-arm driven by pneumatic artificial muscles for humanoid robots. *International Journal of Robotics Research*, 24(4), 2005.

[63] J. Troccaz and Y. Delnondedieu. Semi-active guiding systems in surgery. A two-DOF prototype of the passive arm with dynamic constraints (PADyC). *Mechatronics*, 6(4), 1996.

[64] A. Vilchis, P. Cinquin, J. Troccaz, A. Guerraz, B. Hennion, F. Pellissier, P. Thorel, F. Courreges, A. Gourdon, G. Poisson, P. Vieyres, P. Caron, O. Mérigeaux, L. Urbain, C. Daimo, S. Lavallée, P. Arbeille, M. Althuser,

J-M. Ayoubi, B. Tondu, and S. Ippolito. TER : a system for Robotic Tele-Echography. In *4th Int. Conf. on Medical Image Computing and Computer-Assisted Intervention (MICCAI'01)*, volume 2280 of *Lecture Notes in Computer Science*, pages 326–334. Springer, 2001.

[65] A.P. Wadegaonkar, V.K. Sunnapwar, and J.P. Modak. Development of a knowledge-based system for robot work-station safety. In *Proceedings of International Manufacturing Engineering*, pages 359–361. ICPR, 1996.

[66] I. Walker and J. Cavallero. Failure mode analysis for a hazardous waste clean-up manipulator. *Reliability Engineering and System Safety*, 53 :277–290, 1996.

[67] Y. Yamada, Y. Hirasawa, S.Y. Huang, and Y. Umetani. Fail-safe human/robot contact in the safety space. *5th IEEE International Workshop on Robot and Human Communication*, 1 :59–64, 1996.