L'incertitude en matière de technologie

Du fait de la vitesse croissante du développement technologique, il devient de plus en plus évident que nous ne savons que fort peu de choses sur notre avenir en la matière. Nous ne savons pas quelles nouvelles technologies nous rencontrerons dans le futur proche, et nous ne savons pas davantage comment nos vies, nos sociétés et notre environnement naturel seront affectées par les changements technologiques.

Diverses tentatives ont été faites pour réduire cette incertitude ; en particulier, deux nouvelles disciplines ont vu le jour à cet effet dans les années 1960 : l'évaluation technologique et l'analyse des risques. Toutefois, toutes deux rencontrent des difficultés considérables. L'objectif de cet article est d'expliquer ces difficultés, et de discuter la façon dont on pourrait cependant traiter les incertitudes des technologies futures.

par Sven Ove HANSSON*

L'évaluation des technologies

L'évaluation des technologies (TA – *Technology Assessment*) est née des interrogations apparues dans les années 1960 sur les effets sociaux de l'émergence des nouvelles technologies. L'expression « évaluation des technologies » a été introduite en 1966 par Philip Yeager, qui travaillait pour le compte d'un membre du Congrès américain, Emilio Q. Daddario (Ropohl, 1966).

E.Q. Daddario proposa la création d'une agence du Congrès ayant pour objectif d'anticiper les conséquences du développement des nouvelles technologies, afin d'en limiter les effets négatifs et d'en promouvoir et d'en amplifier les effets positifs. Ces tentatives conduisirent à la création, en 1972, de l'*Office of Technology Assessment* (OTA), qui avait pour tâche d'analyser et de prévoir les conséquences des développements technologiques futurs. Lorsque les activités de l'OTA furent interrompues en 1995 pour des raisons politiques, cet organisme avait publié plus de 700 rapports sur un large éventail de sujets en relation avec la science et la technologie.

Après la fermeture de l'OTA, le centre de gravité de l'évaluation des technologies se déplaça vers l'Europe : plusieurs pays européens se dotèrent de leur propre service parlementaire d'évaluation des technologies.

Cette tradition est en particulier fortement établie en Allemagne mais on la retrouve aussi, par exemple, en Suisse, au Danemark, en Hollande et en Autriche. Le Parlement européen dispose également d'un service destiné à « l'évaluation des choix scientifiques et industriels » (STOA – *Science and Technology Options Assessment*).

Cependant, depuis les années 1960, les ambitions des évaluateurs des technologies sont devenues de plus en plus modestes. Au départ, il s'agissait de prévoir et de contrôler les effets négatifs potentiels résultant du développement technologique. On attendait des évaluateurs qu'ils anticipent les conséquences à venir des nouvelles technologies, avant qu'il ne soit trop tard.

Cependant, l'optimisme initial en matière de prédiction technologique ne s'est pas concrétisé. Si les évaluateurs ont été capables d'identifier d'importants aspects du développement technologique et de les porter au débat public – ce qui n'est pas un résultat négligeable ! –, ils n'ont pas été en mesure de prévoir les développements futurs des technologies. En pratique, ils ont revu à la baisse leurs ambitions en matière de prévision. En revanche, d'autres aspects – tels que les procédures participatives ou les débats publics sur les technologies émergentes – se sont trouvés placés au centre de leurs activités.

Quatre sources majeures d'incertitude se conjuguent pour rendre imprévisibles les technologies futures, rendant ainsi impossible de remplir les ambitions initiales de l'Evaluation des technologies :

- ✔ La première de ces sources d'incertitude est due à l'impossibilité de prévoir ce que seront des outils ou des systèmes technologiques qui n'existent pas encore. A titre d'exemple, examinons une proposition visant à développer un nano-mécanisme destiné à être injecté dans le corps d'un malade atteint du cancer, tel que les cellules cancéreuses actionnent elles-mêmes ce mécanisme pour qu'il libère une substance destinée à les tuer. Il s'agit bien d'une des multiples applications potentielles des nanotechnologies qui ont été proposées. Mais tant que les détails de cette technologie (hypothétique) sont inconnus, on ne peut en évaluer ni l'efficacité thérapeutique, ni les effets secondaires. Nous pouvons établir une liste de caractéristiques possibles (positives ou négatives), mais nous ne pouvons espérer l'établir de façon complète.
- ✔ La seconde source d'incertitude est liée au comportement individuel des utilisateurs d'une technologie. Les

inventeurs d'Internet n'ont, semble-t-il, pas prévu les abus liés à son utilisation, que nous connaissons si bien aujourd'hui. Voici un autre exemple : les réactions des utilisateurs de technologies de sécurité sont difficiles à prévoir. Parfois, les effets de mesures de sûreté se trouvent réduits par une forme de « comportement de compensation » : les utilisateurs compensent l'amélioration technologique de la sécurité par une prise de risque accrue dans leur comportement (Rothengatter 2002). En pratique, un tel comportement est souvent impossible à prévoir.

- ✔ La troisième source d'incertitude correspond à l'émergence de nouveaux modes sociaux et culturels adoptés en réaction à une nouvelle technologie. L'expérience montre que la nature même des innovations sociales et culturelles est quasiment impossible à prévoir. Un exemple célèbre est constitué par la réponse apportée par un responsable du British Post Office, en 1879, devant la Chambre des Communes, sur l'avenir possible du téléphone. Il prévoyait que l'usage du téléphone resterait peu répandu en Grande-Bretagne, car l'on n'y manquait pas de jeunes gens susceptibles de porter des messages (de Sola Pool, 1983, p. 65). Aujourd'hui, une certaine réflexion est nécessaire pour comprendre pourquoi une telle réponse a pu être donnée par une personne intelligente et bien informée. L'explication tient simplement au fait que, contrairement au téléphone proprement dit (une invention technologique), la conversation téléphonique (une invention sociale) était alors inconnue.

  Le téléphone fut donc d'abord considéré comme un moyen de transmettre des messages, comme une version améliorée du télégraphe. De même aux débuts de la télévision, son utilisation à des fins de surveillance avait été envisagée, mais pas son utilisation comme instrument de loisir domestique.

  Le programme de télévision fut une invention sociale qui émergea des années après l'invention technologique de la télévision (de Sola Pool, 1983, p. 99) ;
- ✔ La quatrième source d'incertitude tient à l'interaction des technologies avec des systèmes naturels complexes, en particulier avec les écosystèmes, qui sont, eux aussi, imprévisibles dans la pratique. De nombreux problèmes environnementaux sont la conséquence de ces interactions imprévues avec des mécanismes naturels. Deux des exemples les plus connus sont les effets des composés organo-halogénés sur la couche d'ozone et ceux des gaz à effet de serre sur le climat.

La leçon générale de tout ceci est que le développement technologique est un processus si complexe qu'il est en pratique impossible à prévoir. L'évaluation des technologies a apporté maintes réflexions utiles, mais elle a dû renoncer à son ambition initiale qui était la prévision.

L'analyse du risque

L'autre tentative significative pour réduire l'incertitude sur les effets des technologies est l'analyse du risque (RA – *Risk Assessment*). A l'instar de l'évaluation des technologies, elle trouve ses origines dans le mécontentement public face au développement technologique dans les années 1960. L'analyse du risque a souvent été associée aux contre-réactions vis à vis des craintes, réputées irrationnelles, relatives aux dangers potentiels des technologies. La plupart des premières études se focalisèrent sur des technologies chimiques ou nucléaires, précisément les facteurs de risques qui étaient pris pour cible par l'opposition publique.

Un thème courant de l'analyse de risques était (et est encore aujourd'hui) le fait que l'opposition publique aux risques a souvent pour fondement des incompréhensions et des sur-réactions irrationnelles.

L'analyse du risque diffère de l'évaluation technologique en ce qu'elle ne s'intéresse qu'aux effets négatifs des technologies. Une autre de ses caractéristiques est le fait qu'elle met l'accent sur la quantification et l'analyse probabiliste. En fait, le terme même de « risque » est habituellement entendu par les analystes comme référant à une quantité. Cette approche a été empruntée à la théorie de la décision : en effet, les théoriciens de la décision font la distinction entre une « incertitude » (qu'il n'est pas nécessaire de quantifier) et un risque (qui est supposé être associé à des probabilités de survenue précisément définies).

En termes de théorie de la décision, on agit « sous risque » si toutes les probabilités dont relève la décision sont connues, sinon on parle d'« incertitude ». De la même manière, en analyse du risque, le terme « risque » désigne généralement une quantité. Dans les premiers temps de l'analyse du risque, le terme « risque » signifiait habituellement « probabilité ». Aujourd'hui, ce terme réfère plus souvent à une autre quantité, l'espérance mathématique d'un événement mesurable non désiré, comme, par exemple, le nombre de décès ou de cas de maladie statistiquement prévus (Hansson, 2002).

Cet accent mis sur la quantification a eu des avantages importants. Quand les risques sont quantifiés, ils peuvent être comparés avec exactitude et l'analyse de risques peut être utilisée comme un moyen permettant de définir des priorités dans des choix politiques.

La quantification permet aussi de combiner analyse de risques et analyse économique. En analyse risques/bénéfices, les coûts marginaux des différents projets de réduction du risque peuvent être comparés, afin de déterminer la meilleure utilisation possible de l'argent disponible pour réduire le risque.

Mais en dépit d'une large utilisation de la quantification dans l'évaluation des risques, ceux-ci sont, dans de nombreux cas, beaucoup plus incertains qu'on ne veut bien le reconnaître. Il y a au moins quatre raisons importantes pour lesquelles l'analyse probabiliste du risque des technologies ne fournit pas les évaluations fiables qui en étaient attendues :

— La première de ces raisons tient au fait que l'on ne dispose bien souvent que d'une connaissance limitée des événements indésirables (comme, par exemple, les accidents) dont on cherche à déterminer la probabilité. Lorsqu'on dispose d'une expérience approfondie d'un événement (la

défaillance d'un appareil, par exemple), on peut en déterminer la probabilité en rassemblant des statistiques, puis en les analysant. Ainsi, si l'on veut connaître la probabilité du risque qu'un *airbag* (coussin gonflable de sécurité) d'une marque donnée d'automobile ne soit pas libéré au cours d'une collision, il faut réunir les statistiques concernant les accidents qui impliquent ce modèle de voiture. Si la voiture concernée se trouve être sur le marché depuis un certain temps, il devrait être possible de disposer de données statistiques suffisantes pour pouvoir répondre à cette question. Mais pour des technologies nouvelles et non testées, cette méthode n'est pas pertinente. Par nature, les statistiques d'accidents permettant de déterminer la probabilité d'une défaillance d'*airbag* pour un nouveau modèle de voiture ne sont pas encore disponibles.

Si la construction du véhicule est, pour l'essentiel, inchangée par rapport aux modèles précédents, on peut alors se référer aux données statistiques relatives à ces anciens modèles ; mais ce n'est plus le cas si des changements significatifs ont été introduits.

Dans de tels cas, un avis d'expert est utilisé pour remplacer les statistiques. Souvent, ces avis d'experts sont traités de la même manière que des probabilités fondées sur des fréquences connues, mais ils sont, bien sûr, beaucoup moins fiables.

Pour des événements inhabituels, comme les accidents à grande échelle mais très rares, les fréquences ne peuvent être déterminées, même après de nombreuses années d'expérience pratique. A titre d'illustration, il y a eu – heureusement – trop peu d'accidents graves sur des réacteurs nucléaires pour que l'estimation de la probabilité de leur survenue soit possible. En particulier, la plupart des types de réacteurs en fonctionnement n'ont jamais été impliqués dans un accident sérieux. Il n'est donc pas possible de déterminer la probabilité d'un accident grave sur un type de réacteurs donné.

— La deuxième raison tient au fait que la dépendance statistique entre différents événements est le plus souvent très difficile à déterminer. Or, cette dépendance peut avoir une influence décisive sur l'analyse du risque. Dans les structures technologiques complexes, la plupart des accidents résultent d'un enchaînement d'événements, plutôt que d'événements isolés. En combinant les probabilités des événements de ces chaînes, il devrait être possible (du moins en principe) de calculer la probabilité d'un accident grave. Mais les interdépendances entre les probabilités de ces événements peuvent avoir un impact majeur sur la probabilité globale de l'accident. Supposons, par exemple, qu'un accident surviendra dans le cas où deux vannes de sécurité enregistreraient simultanément une défaillance, et supposons en outre que l'on sait, par expérience, que la probabilité de défaillance d'une vanne du modèle considéré est de 1/500, sur une période d'un an. On ne peut pas pour autant en conclure que la défaillance simultanée de deux vannes sur cette période serait de 1/500 x 1/500, soit 1/250 000. La raison tient au fait que ces deux défaillances ne sont pas des événements indépendants. Il est possible que ces deux vannes connaissent une défaillance simultanée dans le cas d'un incendie, ou si l'équipe de maintenance répète la même erreur sur les deux vannes.

— La troisième raison est que des accidents peuvent se produire de plus de façons que celles que l'on a pu imaginer. Dans la pratique, il est impossible de faire une liste complète de tous les types d'accidents susceptibles de se produire, par exemple, dans une mine ou dans une grande usine chimique (Il est souvent utile d'essayer d'établir une liste aussi complète que possible, mais l'on n'est jamais certain d'y être parvenu). Même si l'on peut disposer de probabilités raisonnables pour tous les types d'accidents que l'on peut prévoir, la catégorie résiduelle des « autres types d'accidents imprévus » ne peut être éliminée et, bien entendu, aucune probabilité significative ne peut lui être attribuée. Cette remarque est particulièrement pertinente pour les technologies nouvelles.

Dans les premiers temps des biotechnologies, la possibilité de graves accidents imprévus liés à la manipulation des matériaux génétiques était une préoccupation majeure. Aujourd'hui, une situation analogue peut exister pour certaines applications des nanotechnologies (Hansson, 1996, 2004).

— La quatrième raison est que les risques dépendent largement du comportement humain. Certains risques technologiques parmi les plus redoutés sont liés à des comportements humains volontaires, comme le terrorisme ou le sabotage. Des attaques terroristes sur des sites nucléaires peuvent, dans certains cas, constituer un risque plus important que des incidents non intentionnels. Pour un système informatique, l'attaque de *hackers* peut constituer une menace plus grave que des défaillances techniques.

L'analyse probabiliste des menaces intentionnelles est en pratique quasi impossible. (Des modèles de théorie des jeux sont, dans ce domaine, des outils plus utiles que les modèles probabilistes).

En bref, l'analyse probabiliste des défaillances technologiques est fertile en incertitude. Néanmoins, le recours à des approximations et à des estimations de probabilités, comme si celles-ci correspondaient à des fréquences parfaitement connues et exactes, est une tendance très répandue. En d'autres termes, les décisions sur les risques (le terme de « risques » étant pris dans son acception la plus courante, comme un synonyme de « danger ») sont souvent traitées comme des décisions « sous risque » (dans le sens de la théorie de la décision, c'est-à-dire avec des probabilités connues). De fait, les décisions « sous risque » sont le plus souvent des décisions « sous incertitude ».

Pour éclairer cette différence, on peut recourir à l'analogie suivante : les décisions d'un joueur à la table de roulette sont un exemple caractéristique de décisions « sous risque » au sens de la théorie de la décision. Il s'agit en effet de décisions avec des probabilités connues. Si l'on admet que la roulette est sans défaut, la probabilité des divers événements – gain ou perte – est facilement calculable et peut, dès lors, être connue, bien que le joueur puisse ne pas en tenir compte. Un exemple, tout aussi caractéristique, d'une

décision « sous incertitude » est celui d'un explorateur pénétrant dans une partie éloignée de la jungle, jusqu'ici non foulée par le pied de l'homme. Dans la jungle, les dangers sont nombreux, mais aucune estimation de leur probabilité, autres que des suppositions, ne peut être avancée. Il peut, en outre, exister des dangers dont on ignore tout. L'analyse de risques pour des technologies nouvelles et émergentes ressemble davantage au risque couru dans la jungle qu'au risque à la table de roulette – on dispose seulement d'une liste incomplète des risques et, pour ceux qui figurent sur cette liste, les probabilités significatives ne sont le plus souvent pas disponibles. Ce que nous offrent les futures technologies est plus proche d'une expédition dans la jungle que d'une visite au casino (Hansson, 2009).

En résumé, l'évaluation technologique et l'évaluation des risques se heurtent, toutes deux, à de sévères limitations. L'analyse de risques, dans sa forme traditionnelle, est fondée sur des mesures quantitatives du risque, sous la forme d'espérance mathématique. Pour obtenir ces mesures, il faut avoir des valeurs de probabilités qui, le plus souvent, ne sont pas disponibles, y compris pour des technologies existantes, et à plus forte raison, pour des technologies futures qui diffèrent, par leurs structures de base, des technologies déjà en usage.

L'évaluation des technologies a été initialement conçue comme un moyen de prévoir le développement de nouvelles technologies et leurs conséquences sociales. Elle n'a pas été en mesure de fournir de telles prévisions, mais elle a contribué utilement au débat public sur la technologie de diverses autres manières.

Il existe, toutefois, une autre discipline, beaucoup plus ancienne que les deux précédentes, qui s'avère extrêmement utile pour faire face à de nombreux problèmes difficiles soulevés par le développement technologique : l'ingénierie de sécurité.

L'ingénierie de sécurité

Depuis le XIX^{e} siècle, des ingénieurs se sont spécialisés sur la sécurité des travailleurs et sur d'autres problèmes de sécurité. Bien que l'ingénierie de sécurité soit enseignée dans les collèges technologiques et dans les universités, sa présence est beaucoup plus discrète que celle de l'analyse des risques. Une des raisons à cela est que l'ingénierie de sécurité est éclatée entre différents domaines technologiques, alors que l'analyse des risques présente une grande unité, s'intéressant à toutes sortes de risques au moyen d'une même méthodologie.

L'ingénierie de sécurité s'est largement développée en parallèle dans différents secteurs techniques, et sa terminologie diffère souvent selon ses domaines d'application (Hansson, 2009 b). Mais une étude plus approfondie montre que ses différentes formes sont fondées sur des approches similaires en matière de risque et de sécurité.

Portons un regard plus aiguisé sur trois des principes de sécurité les plus importants utilisés par les ingénieurs de sécurité : la sécurité intrinsèque, les barrières de sécurité multiples et les facteurs de sécurité.

La sécurité intrinsèque (également appelée « prévention primaire ») consiste en l'élimination d'un danger. Elle s'oppose à la « prévention secondaire », qui ne vise pas à supprimer le danger mais à réduire le risque qui lui est associé. Pour prendre un exemple simple, considérons un procédé qui utilise des matériaux inflammables : la sécurité intrinsèque consiste pour ce procédé à recourir à des matériaux non inflammables, et la sécurité secondaire consiste à supprimer (ou à isoler) les sources d'inflammation et/ou à installer un équipement anti-incendie. Comme cet exemple le montre, la prévention secondaire utilise en général des équipements de sécurité additionnels. Les ingénieurs de sécurité (en particulier dans l'industrie chimique) ont développé des méthodes assurant un niveau de sécurité intrinsèque aussi élevé que possible au sein des usines. L'idée de base, en matière de sécurité intrinsèque, est que, toutes choses égales par ailleurs, si l'on peut choisir entre l'élimination et la gestion du danger, l'élimination est préférable. La raison principale en est que tant que le danger existe, il peut survenir à la suite d'un événement déclenchant non prévu. Même avec les meilleures mesures de contrôle possibles, une chaîne imprévue d'événements peut, par exemple, provoquer un incendie.

Même la meilleure des technologies de sécurité additionnelle peut être défaillante ou être détruite, du fait d'un accident. La sécurité intrinsèque est un moyen qui permet de prendre en considération ces incertitudes.

Les barrières de sécurité multiples reposent sur des principes qui sont au moins aussi anciens que les forteresses de l'antiquité. Si l'ennemi parvient à passer la première enceinte, il se heurte à des couches additionnelles, qui protègent les assiégés.

L'ingénierie de certaines barrières de sécurité suit ce même principe de barrières concentriques. Un exemple en est la série de barrières physiques contre les fuites radioactives des réacteurs nucléaires modernes. Dans d'autres cas, les barrières de sécurité sont consécutives sur un plan temporel, plutôt que spatial. Considérons, par exemple, la protection des travailleurs contre un gaz dangereux, tel que l'hydrogène sulfuré (ou sulfure d'hydrogène, H_2S), qui présente un risque de fuite dans une usine chimique. La première barrière consiste à construire toute l'usine de manière à exclure le plus possible une fuite incontrôlée. La seconde barrière correspond à une maintenance de qualité incluant la vérification régulière de points vulnérables (comme les vannes). La troisième barrière est un système d'alerte, combiné à des instructions définies au préalable et relatives aux modalités d'une évacuation en cas de fuite. La quatrième barrière est constituée de services de secours efficaces et bien entraînés.

L'idée de base présidant au système à barrières multiples est que même une barrière bien conçue peut se révéler défaillante pour une raison imprévue et que la barrière suivante peut alors fournir une protection efficace.

Enfin, **les facteurs de sécurité** sont des facteurs numériques que l'on utilise pour dimensionner une réserve de sécurité. L'utilisation de facteurs de sécurité a été introdui-

te dans la deuxième moitié du XIX[e] siècle. Ils jouent maintenant un rôle central dans les structures mécaniques et leurs multiples applications dans les différentes disciplines de l'ingénierie.

L'élaboration de systèmes de facteurs de sécurité a été spécifiée par des normes et des standards. Le plus couramment, un facteur de sécurité est exprimé par le rapport entre la mesure de la charge maximale n'entraînant pas le type de défaillance considéré et la mesure correspondante de la charge appliquée.

Par conséquent, nous pouvons choisir de construire un pont assez solide pour résister à deux fois la charge la plus élevée à laquelle il pourrait être soumis. On a alors utilisé un facteur de sécurité de 2.

Selon les standards des structures mécaniques, les facteurs de sécurité sont prévus pour compenser cinq catégories principales de sources de défaillance : des charges plus élevées que prévues, de moins bonnes propriétés des matériaux que celles attendues, une théorie imparfaite du mécanisme de défaillance considéré, éventuellement des mécanismes de défaillance inconnus et, enfin, l'erreur humaine (par exemple, au niveau de la conception) (Knoll, 1976 ; Moses, 1997).

Les trois derniers types de défaillance correspondent à des erreurs au plan de la théorie ou de son application. Les facteurs de sécurité prennent donc en compte non seulement les risques calculables, mais aussi les incertitudes non numériques (Clausen et al., 2006).

Ainsi que nous venons de le voir, les principes directeurs majeurs de l'ingénierie de sécurité visent à gérer non seulement des risques, mais aussi des incertitudes. Pour donner un autre exemple, supposons qu'un constructeur de bateaux produise un plan convaincant de navire insubmersible (bien meilleur que le Titanic). L'analyse probabiliste des risques montre que la probabilité qu'a un navire de couler est infime. Sur la base d'une analyse de risques, une analyse risques/bénéfices est réalisée. Elle montre que le coût d'équipement en canots de sauvetage serait économiquement indéfendable. Cette analyse nous conduit à conclure que ce bateau ne devrait pas être équipé de canots. Un ingénieur de sécurité accepterait-il cette analyse et exclurait-il les canots de sauvetage dans sa conception ? La réponse est non, si sa conception suit les règles de l'art et cela pour une raison très simple : les calculs peuvent être faux et, s'ils le sont, les conséquences peuvent être dramatiques. La barrière de sécurité additionnelle constituée par les canots de sauvetage (ainsi que par les consignes d'évacuation et toutes les autres mesures de sécurité prises) ne doit pas être écartée, bien que les estimations de probabilités montrent qu'elle n'est pas nécessaire.

L'ingénierie de sécurité suit une forte tradition, selon laquelle on reconnaît que l'on peut se tromper, et cela, de diverses manières :

- ✔ nos constructions et nos dispositifs technologiques peuvent être défaillants ;
- ✔ notre évaluation des risques et des dangers peut être inexacte ;
- ✔ nos prévisions des futures technologies peuvent être fausses.

Les ingénieurs de sécurité cherchent à mettre au point des systèmes technologiques suffisamment robustes pour que l'on puisse les utiliser en dépit d'erreurs potentielles. Que les erreurs et les défaillances soient possibles (et même attendues) est un facteur indispensable dans toute tentative pour traiter les dangers possibles des futures technologies. Même quand les prédictions sont impossibles (c'est souvent le cas), des constructions robustes et évolutives doivent être développées.

Ainsi, l'incertitude technologique peut être en partie traitée par des moyens *technologiques*, plutôt que par le méta-niveau de l'évaluation technologique et de l'analyse de risques…

Note

* Professeur de philosophie et Président du département de philosophie et d'histoire des technologies à l'Institut royal de technologie (KTH) de Stockholm.

Bibliographie

[1] (Jonas) CLAUSEN, (Sven Ove) HANSSON and (Fred) NILSSON, « Generalizing the Safety Factor Approach », *Reliability Engineering and System Safety* 91:964-973, 2006.

[2] (F.) KNOLL, « Commentary on the basic philosophy and recent development of safety margins », *Canadian Journal of Civil Engineering* 3:409-416, 1976.

[3] (F.) MOSES, « Problems and prospects of reliability-based optimisation », *Engineering Structures* 19:293-301, 1997.

[4] (Sven Ove) HANSSON, « Decision-Making Under Great Uncertainty », *Philosophy of the Social Sciences* 26:369-386, 1996.

[5] (Sven Ove) HANSSON, « Les incertitudes de la société de savoir », *Revue internationale des sciences sociales* 171:43-51, 2002.

[6] (Sven Ove) HANSSON, « Great Uncertainty about Small Things », *Techne* 8(2):26-35, 2004.

[7] (Sven Ove) HANSSON, « From the Casino to the Jungle. Dealing with uncertainty in technological risk management », *Synthese* 168:423-432, 2009a.

[8] (Sven Ove) HANSSON, Risk and Safety in Technology, pp. 1069-1102 in Anthonie Meijers (ed.), Handbook of the Philosophy of Science, Volume 9: Philosophy of Technology and Engineering Sciences, Elsevier 2009b.

[9] (G.) ROPOHL, *Ethik und Technikbewertung*, Frankfurt am Main : Suhrkamp Verlag, 1996.

[10] (Talib) ROTHENGATTER, « Drivers' illusions – no more risk », *Transportation Research, part F*, 5:249-258, 2002.

[11] (Ithiel) de SOLA POOL, *Forecasting the Telephone : A Retrospective Technology Assessment*, Ablex Publishing, 1983.