Fédération des Industries Mécaniques

www.fim.net

NOTE DE POSITION

Enjeux en matière d'intelligence artificielle et de cyber-sécurité dans le cadre de la révision de la Directive Machines

Auteur : **Benjamin Frugier**
bfrugier@fimeca.org - + 33 (0)1 47 17 60 20

Date de publication : **08/07/2019**

La digitalisation de l'industrie est d'ores et déjà une réalité. De nombreuses entreprises, tous secteurs confondus (automobile, agroalimentaire, aéronautique, industries de process,…) déploient dans leurs usines existantes ou dans leurs nouveaux projets industriels un certain nombre de solutions nouvelles en matière de technologies de production, dans un contexte d'amélioration de la flexibilité et de l'optimisation des ressources.

Parmi ces technologies émergentes, l'intelligence artificielle va permettre aux fabricants de machines de proposer des fonctionnalités nouvelles, comme la maintenance prédictive ou l'automatisation de certains contrôles qualité, mais aussi de mettre en œuvre des machines autonomes et apprenantes telles que les Automated Guided Vehicles (AGV) ou les robots. Du fait de ces deux caractéristiques particulières - autonomie et capacité d'apprentissage -, il est nécessaire d'évaluer la robustesse de la Directive Machines vis-à-vis de l'intelligence artificielle.

Par ailleurs, la généralisation de la connectivité entre machines (« machine to machine ») accroît les risques de hacking et de cyberattaque des installations industrielles, avec deux risques potentiels, le premier en matière économique (par exemple : l'arrêt du process de production), le second en matière de sécurité (par exemple : la neutralisation des butées logicielles d'un bras articulé, conduisant à un accident). Dans ce contexte, il est nécessaire de déterminer comment prendre en compte la cybersécurité dans le processus de conception, en vue de la mise sur le marché d'une machine sûre. Cette question doit être posée tout au long du cycle de vie de la machine.

Cybersécurité

Usage normal et mauvais usage raisonnablement prévisible

La Directive Machines, qui a pour finalité de protéger la santé et la sécurité des utilisateurs, prend appui en termes de conception sur la notion de « limites de la machine » déclinée de la façon suivante (voir Principes généraux et article 1.1.2.c de l'annexe I) :

- L'usage normal, défini comme l'utilisation d'une machine selon les informations fournies dans la notice d'instructions
- Le mauvais usage raisonnablement prévisible, défini comme l'usage de la machine d'une manière non prévue dans la notice d'instructions, mais qui est susceptible de résulter d'un comportement humain aisément prévisible

En ce qui concerne l'usage normal, le guide Machines[1] indique que « la machine n'est pas forcément sûre pour toutes les utilisations possibles : par exemple, le fabricant d'une machine destinée à l'usinage des métaux n'a généralement pas conçu la machine pour le travail du bois et vice-versa ».

[1] Guide to the application of the Machinery Directive

En ce qui concerne le mauvais usage raisonnablement prévisible, ce même Guide précise qu' « on ne peut s'attendre à ce que le fabricant de machines tienne compte de toute les mauvaises utilisations possibles de la machine. Mais certains types de mauvais usages, intentionnels ou non, sont prévisibles sur la base de l'expérience de l'utilisation antérieure du même type de machine ou de machines similaires, des enquêtes menées à la suite d'accidents et de la connaissance du comportement humain ». Plusieurs exemples sont cités, comme la loi du moindre effort ou le comportement résultant d'un défaut de concentration.

Par exemple, dans le cas d'une scie circulaire, le fabricant doit par conception prendre en compte l'usage et le mauvais usage raisonnablement prévisible. En revanche, il n'est pas envisageable que le fabricant conçoive cette machine dans la perspective de prendre en compte le risque d'une utilisation malveillante voire criminelle, dans la mesure où la conception achopperait sur des difficultés techniques majeures. En effet, cette prise en compte conduirait le fabricant à cartériser les éléments mobiles. Dans le même temps, la fonctionnalité de base de la scie ne pourrait plus être remplie.

- La FIM considère qu'une cyberattaque – en tant qu'acte malveillant - ne peut pas être considérée comme un mauvais usage raisonnablement prévisible. Ainsi, la problématique de la cybersécurité ne relève pas juridiquement de la Directive Machines ou de tout autre texte législatif relatif à la santé et à la sécurité. C'est une problématique de sûreté.

Dynamique contractuelle

Un certain nombre de machines ont vocation à être intégrées physiquement et digitalement sur le site industriel des utilisateurs, qui dispose de sa propre protection contre les cyberattaques. Dans ces conditions, il est nécessaire qu'un dialogue s'instaure entre d'un côté le fabricant de la machine (le cas échéant l'intégrateur) et de l'autre l'utilisateur, afin de prendre en compte la question de la cybersécurité, au moment de la mise en service mais aussi tout au long du cycle de vie de la machine, ce risque étant en effet évolutif.

D'autres situations peuvent se présenter et il est à noter qu'il n'est pas envisageable de traiter de la même façon une machine destinée à un consommateur et une machine destinée à une installation industrielle. Dans le premier cas, c'est au fabricant de concevoir une machine résiliente en termes de sûreté, en prenant en compte la demande du marché, par exemple en matière de certification.

Du côté de la réglementation, la Directive 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (Directive NIS) prévoit notamment des dispositions en matière de sécurité pour les opérateurs de services essentiels (secteurs de l'énergie, des transports,…). En particulier, l'article 14 indique que « Les États membres veillent à ce que les opérateurs de services essentiels prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités ». Le législateur a souhaité ainsi protéger la continuité du fonctionnement de ces installations, considérant que le bon niveau d'intervention en matière de cybersécurité était le site industriel et non pas les machines et les équipements pris individuellement.

Du plus, un texte sur la cybersécurité (Règlement 2019/881 du Parlement européen et Conseil relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications) a été publié le 17 avril dernier. Celui-ci crée notamment un mécanisme pour l'établissement de systèmes européens de certification de cybersécurité pour des produits, incluant de fait les machines. Ces systèmes de certification sont des référentiels techniques visant à obtenir vers un niveau de cybersécurité harmonisé et pouvant faire l'objet d'une certification volontaire. Les utilisateurs pourront ainsi requérir – ou non - auprès des fabricants, une certification en matière de cybersécurité.

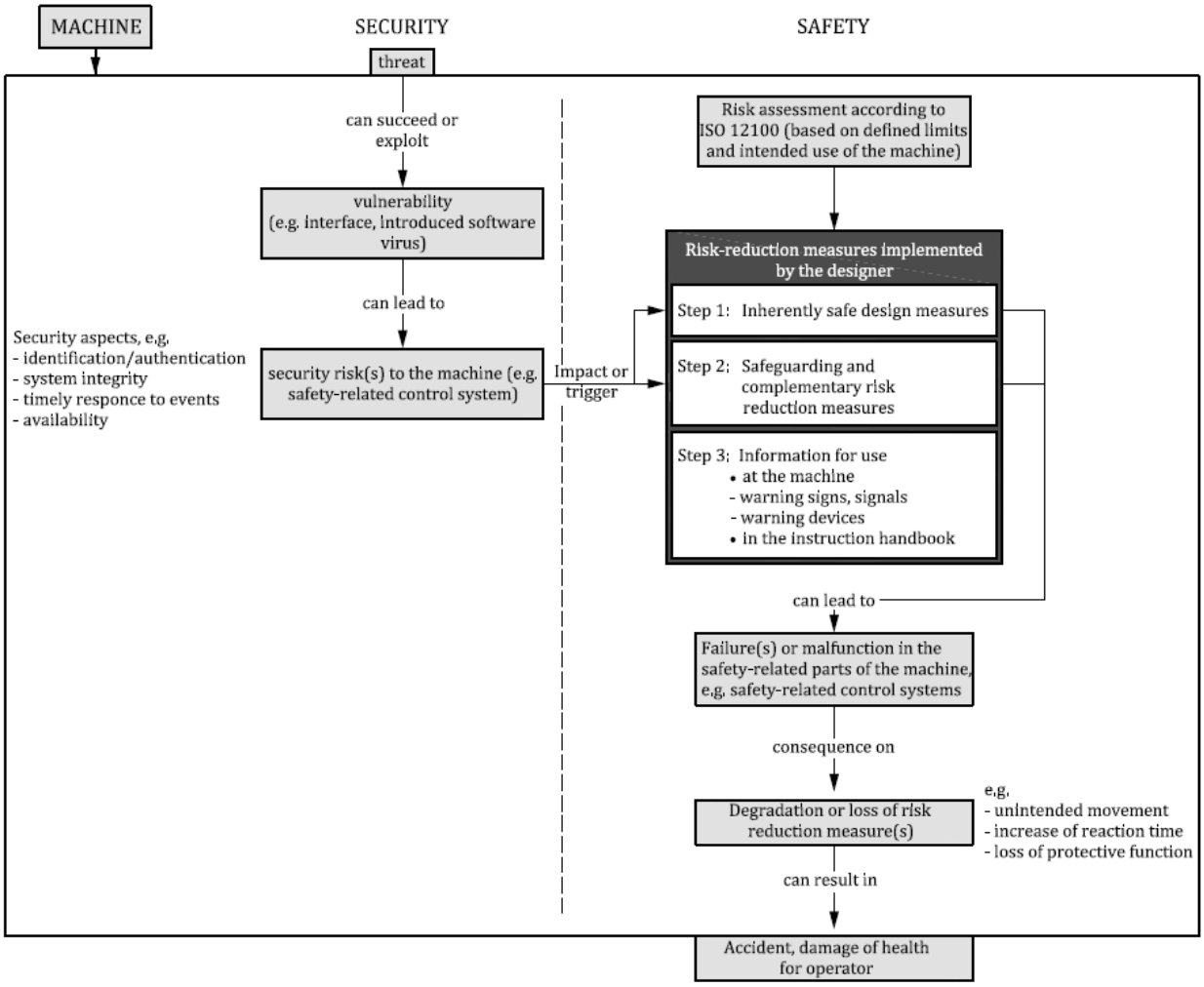
- La FIM considère que le niveau de protection optimal en matière de cybersécurité relève d'une dynamique contractuelle entre l'utilisateur et le fabricant de machines. Il n'est pas nécessaire à ce stade d'envisager un cadre horizontal contraignant.

Prise en compte de la cybersécurité dans la conception des machines

En fonction des différentes situations envisagées ci-dessus, le fabricant de machines doit prendre en compte la question de la cybersécurité dans la conception.

A ce sujet, l'ISO/TC 199 "Sécurité des machines" a publié en 2018 un rapport technique (*ISO/TR 22100-4:2018 Safety of machinery - Relationship with ISO 12100 - Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*).

Ce document donne aux concepteurs des éléments méthodologiques utiles, en partant de l'analyse de risque obligatoire au titre de la Directive Machines (voir aussi la norme harmonisée ISO 12100 Sécurité des machines - Principes généraux de conception - Appréciation du risque et réduction du risque) :



Par ailleurs, l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) a publié un guide intitulé « Good Practices for Security of Internet of Things in the context of Smart Manufacturing ». Ce guide identifie les enjeux et les risques du déploiement de l'internet des objets (IoT) et classe les mesures méthodologiques, organisationnelles et techniques à mettre en œuvre pour assurer la sûreté de l'usine connectée. Enfin, à chaque mesure de sûreté est associée une liste de normes et référentiels pertinents.

Enfin, il faut noter la publication de la série des IEC 62443 Industrial communication networks - Network and system security / Security for industrial automation and control systems et ISO/IEC 27001/2 Technologies de l'information - Techniques de sécurité.

- La FIM recommande la mise en œuvre des normes ISO/TR 22100-4, IEC 62443 et ISO/IEC 27001/2 ainsi que l'utilisation du guide de l'ENISA « Good Practices for Security of Internet of Things in the context of Smart Manufacturing »

Intelligence artificielle

La FIM s'appuie à ce stade sur la définition donnée dans le document de la Commission européenne intitulé « A definition of AI : Main capabilities and discipliines »[2] de mars 2019 :

> *Artificial intelligence (AI) refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to predefined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions.*

Cette définition signifie qu'en dernière instance, il y a toujours un concepteur qui délimite les différentes fonctionnalités de la machine, en particulier la capacité d'apprentissage. Elle reste néanmoins imparfaite dans la mesure où elle renvoie à une certaine forme d'anthropomorphisme, l'IA étant le sujet de verbes d'action (agir, interpréter, percevoir, raisonner, décider et apprendre).

Cette introduction est d'importance car le sujet de l'intelligence artificielle a fait récemment l'objet de nombreuses publications, en premier lieu scientifiques mais aussi dans la presse généraliste, avec souvent une tonalité très critique. On peut penser par exemple à la polémique à propos des robots tueurs.

Le Parlement Européen a lui aussi pris la parole en prenant une résolution le 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique[3]. Au-delà du titre, les députés européens s'intéressent en pratique aux systèmes autonomes utilisant l'IA.

Cette résolution précise à son considérant Z : « considérant que, grâce aux impressionnants progrès technologiques au cours des dix dernières années, non seulement les robots contemporains sont capables de mener à bien des tâches qui relevaient autrefois exclusivement de la compétence humaine, mais encore que la mise au point de certaines fonctionnalités autonomes et cognitives (comme la capacité de tirer des leçons de l'expérience ou de prendre des décisions quasi-indépendantes) rapprochent davantage ces robots du statut d'agents interagissant avec leur environnement et pouvant le modifier de manière significative; que, dans un tel contexte, la question de la responsabilité juridique en cas d'action dommageable d'un robot devient une question cruciale ». Là aussi, l'anthropomorphisme empêche d'orienter correctement le débat et laisse entendre que la créature pourrait échapper à son créateur.

Dans ce contexte, la Commission Européenne a initié des travaux relatifs à l'Intelligence Artificielle, avec pour objectif d'établir des recommandations sur la mise en œuvre de la stratégie communautaire en la matière. Les premiers livrables ont été publié en mars 2019, le premier traitant des définitions (voir ci-dessus), le second de l'éthique[4]. Du fait de son caractère généraliste, ce dernier document n'a pas vocation à être utilisé dans toutes ses composantes par les concepteurs de machines mais il donne des éléments de cadrage importants. Pus récemment (juin 2019), la Commission Européenne a publié un document relatif à sa stratégie en la matière (R&D, aspects réglementaires, formation…) et aux investissements[5].

Après ces propos liminaires, il est nécessaire d'évaluer la robustesse de la Directive Machines vis-à-vis de l'intelligence artificielle.

Neutralité technologique des exigences essentielles

L'intelligence artificielle est un moyen technique permettant d'améliorer le fonctionnement d'une machine et de mettre à disposition de l'utilisateur de nouvelles fonctionnalités. Cette technologie ne crée pas intrinsèquement un nouveau phénomène dangereux dans la mesure où il s'agit d'une strate logicielle.

Par ailleurs, le concepteur d'une machine doit effectuer, au titre des principes généraux et des principes d'intégration de la sécurité (paragraphe 1.1.2) de l'annexe I de la Directive Machines, une appréciation du risque et déterminer

---

[2] « A definition of AI: Main capabilities and disciplines »
[3] Résolution du 16 février 2017 du Parlement européen
[4] « Ethics guidelines for trustworthy AI »
[5] « Policy and investment recommendations for trustworthy Artificial Intelligence »

quelles exigences essentielles sont applicables. Il peut ensuite utiliser des référentiels techniques, en particulier les normes harmonisées, afin de mettre en œuvre des solutions conformes à l'état de l'art.

Le législateur a fait le choix de ne définir au niveau de la Directive que des exigences générales et technologiquement neutres afin de ne pas brider l'innovation et d'éviter que la législation ne devienne un catalogue de solutions techniques.

Appréciation du risque et état de l'art

Comme indiqué ci-dessus, le fabricant doit déterminer les exigences essentielles applicables puis mettre en œuvre des solutions techniques permettant de respecter ces exigences.

A titre d'exemple, il est indiqué au paragraphe 1.2.1. Sécurité et fiabilité des systèmes de commande de l'annexe I de la directive Machines que « la machine ne doit pas se mettre en marche inopinément ». Cela s'applique si la mise en marche automatique, ie sans ordre de l'opérateur, génère un risque pour celui-ci. Dans le cas d'une machine autonome, le concepteur ne pourra envisager un démarrage que s'il n'y a pas d'opérateurs (ou de personnes) dans l'environnement de la machine. La machine devra donc être en capacité d'identifier de façon sûre les personnes à proximité.

En résumé, l'application de cette exigence essentielle à une machine non dotée d'intelligence artificielle conduit le concepteur à subordonner le démarrage de la machine à un ordre de l'opérateur alors que dans le cas d'une machine autonome, le concepteur doit s'assurer que la mise en marche ne puisse se faire qu'en l'absence d'opérateurs à proximité. Une même exigence essentielle applicable mais un traitement technique différentié du fait des fonctionnalités nouvelles rendues possibles par l'intelligence artificielle.

Cet exemple montre que l'émergence de l'intelligence artificielle nécessite de revoir en profondeur le processus d'appréciation du risque et de formaliser l'état de l'art pour chaque catégorie de machines, afin de permettre aux fabricants de mettre en œuvre des solutions techniques sûres. Cela passe par l'élaboration de documents professionnels, de spécifications techniques ou de documents normatifs, comprenant une méthodologie de validation. A l'inverse, elle ne nécessite pas de revoir les différentes exigences essentielles, du fait de leur caractère général et technologiquement neutre.

Apprentissage et autonomie

Une des principales techniques d'Intelligence artificielle est basée sur l'apprentissage profond (« deep learning »). A ce stade, il s'agit essentiellement d'apprentissage supervisé, effectué en amont de la mise sur le marché des machines. Il est néanmoins envisageable que les machines puissent continuer d'apprendre (apprentissage non supervisé ou non), après la mise en service. Il est à noter que cette fonctionnalité ne peut résulter que d'une intention délibérée du fabricant, par exemple pour améliorer la performance de la machine.

Dans ce contexte, le fabricant doit, par conception, encadrer cette faculté d'apprentissage, afin de garantir tout au long du cycle de vie de la machine un niveau de sécurité adéquat.

Le déploiement de l'intelligence artificielle permet de mettre sur le marché des machines autonomes comme des AGV ou des robots agricoles. Cette faculté d'autonomie se traduit notamment par l'absence d'un conducteur mais aussi par le fait que la machine puisse se mouvoir à proximité d'opérateurs, dans un mode de coexistence. A l'instar de l'exemple détaillé ci-dessus (paragraphe Appréciation du risque et état de l'art), le fabricant doit ainsi procéder à une analyse de risque lui permettant de prendre en compte cette nouvelle fonctionnalité.

Ethique

Le guide de la Commission européenne déjà cité (cf. note 4) définit sept axes (ou lignes directrices) méthodologiques que les concepteurs de systèmes utilisant l'Intelligence Artificielle sont invités à mettre en œuvre :

- Facteur humain et contrôle
- Robustesse technique et sécurité
- Respect de la vie privée et gouvernance des données
- Transparence
- Diversité, non-discrimination et équité
- Bien-être sociétal et environnemental
- Responsabilisation

Par exemple, l'axe Transparence s'intéresse à la traçabilité des systèmes d'IA, qui doit être assurée, en particulier en enregistrant et en documentant les décisions prises par les systèmes, ainsi que l'ensemble du processus qui a abouti aux décisions.

Par ailleurs, l'Organisation de Coopération et de Développement Economiques (OCDE) vient de publier une Recommandation sur l'Intelligence Artificielle[6]. Ce document donne des lignes directrices pour les concepteurs de systèmes utilisant la technique d'Intelligence Artificielle :

- Croissance inclusive, développement durable et bien-être
- Valeurs centrées sur l'humain et équité
- Transparence et explicabilité
- Robustesse, sûreté et sécurité
- Responsabilité

Il serait utile que ces différents principes soient adaptés au secteur des machines.

Recommandations de la FIM

- La FIM considère que la mise à l'épreuve de la Directive Machines révèle que ses exigences essentielles restent robustes (« fit for purpose ») car elles sont complètes (pas de nouveau phénomène dangereux), rédigées de manière suffisamment large pour accueillir des technologies émergentes comme l'intelligence artificielle et technologiquement neutres.
- La FIM recommande d'enrichir le processus d'appréciation du risque sur l'ensemble du cycle de vie de la machine et de formaliser l'état de l'art pour chaque catégorie de produits, afin de permettre aux fabricants de mettre en œuvre des solutions techniques sûres.
- La FIM recommande la mise en œuvre des lignes directrices de la Commission Européenne relatives à l'éthique et la Recommandation de l'OCDE, de façon adaptée à l'usage des machines.

Contact FIM
Benjamin Frugier
+ 33 (0)1 47 17 60 20
bfrugier@fimeca.org

6 Recommandation du Conseil sur l'Intelligence Artificielle