Vers une approche intégrant les exigences de cybersécurité à la maîtrise des risques d'accidents majeurs pour les ICPE

F. MASSÉ
INERIS
Verneuil-en-Halatte, France
Francois.masse@ineris.fr

H. ABDO & J-M. FLAUS
G-SCOP
Université Grenoble Alpes
Grenoble, France

I. *Abstract*— Objectifs

De nombreux guides, méthodes, normes, recommandations ou réglementations traitent des sujets de la maîtrise des risques industriels d'une part et de la cybersécurité des installations industrielles d'autre part. Ces deux sujets sont liés mais les documents normatifs et réglementaires ainsi que les méthodologies mises en œuvre, ont été développés séparément. Il peut donc être difficile de les appliquer de manière globale, efficiente et simultanée à un même système.

L'article présente les processus et les exigences relatifs à la maîtrise des risques industriels et à la cybersécurité des systèmes de contrôle commande industriel et une analyse des implications des cyberattaques sur la maîtrise des risques. L'objectif est de proposer un cadre méthodologique permettant de prendre en compte de façon simple la cybersécurité dans la prévention des accidents majeurs. Cette étude est réalisée dans le contexte spécifique des Installations Classées.

***Index Terms*—Cybersécurité, Maîtrise des risques industriels, Analyse des Risques, Installations Classées**

II. INTRODUCTION

La numérisation des systèmes de production, y compris dans l'industrie du procédé, est une évolution majeure des installations industrielles apportée par les concepts « d'industrie du futur » ou « d'industrie 4.0 ». Elle implique en particulier l'utilisation de technologies issues de l'informatique dans les systèmes de contrôle-commande industriels et la connexion de ces derniers avec les systèmes d'information de l'entreprise - et donc la connexion à internet du système de contrôle industriel au travers du système d'information de l'entreprise. Ces évolutions offrent de nouvelles vulnérabilités à des attaquants potentiellement plus nombreux, plus compétents sur les technologies utilisées et ayant accès plus facilement à des connaissances techniques sur le fonctionnement des systèmes de production.

Depuis l'attaque Stuxnet, en 2011, de nombreuses attaques plus ou moins perfectionnées et médiatisées ont mis en évidence l'émergence de ce risque. En France, la réglementation sur la cybersécurité s'applique exclusivement aux OIV (Opérateurs d'Importance Vitale), cependant, le sujet est devenu critique pour l'ensemble des industriels et en particulier pour les exploitants d'Installations Classées (IC), qu'ils soient ou non OIV.

Les processus de maîtrise des systèmes de contrôle-commande et des systèmes instrumentés de sécurité nécessaires à la maîtrise des risques industriels doivent donc prendre en compte la vulnérabilité de ces technologies à des actes malveillants.

De nombreuses études pointent les similitudes, renforcement mutuels[1] et antagonismes entre les exigences de sûreté de fonctionnement et les exigences de cybersécurité et proposent des processus pour fusionner les deux approches ou au minimum pour intégrer des exigences de cybersécurité dans le processus de maîtrise de la sûreté de fonctionnement [12][13].

En revanche, les référentiels normatifs et la littérature scientifique sur les implications de la cybersécurité dans la maîtrise des risques industriels sont beaucoup moins développés. Un processus global de maîtrise des risques devrait intégrer les cyberattaques comme sources potentielles de danger.

Cet article présente dans un premier temps les exigences relatives à la maîtrise des risques industriels pour les installations classées d'une part et à la maîtrise de la cybersécurité pour les OIV d'autre part dans le contexte réglementaire français. Une seconde partie traite de l'implication de la cybersécurité sur la maîtrise des risques industriels. Enfin la troisième partie propose une démarche d'intégration de la cybersécurité dans l'évaluation et la maîtrise globales des risques industriels.

III. CONTEXTE REGLEMENTAIRE

A. La maîtrise des risques pour les installations classées

Toute exploitation industrielle susceptible de créer des risques ou de provoquer des pollutions ou nuisances, notamment pour la sécurité et la santé des riverains est une

[1] Le respect d'exigences de sécurité améliore la cybersécurité ou inversement

Installation Classée (IC). Différents régimes sont définis pour les installations classées, en fonction de l'importance des risques. Les installations présentant les risques les plus importants - identifiés sur la base de la nomenclature des installations classées qui fixe des seuils en fonction des substances employées ou stockées sur le site et du type d'activité – sont soumises au régime de l'autorisation. Pour ces installations, l'exploitant doit faire une demande d'autorisation démontrant la maîtrise des risques ; la demande doit être acceptée par le préfet avant mise en service de l'installation.

Pour démontrer l'acceptabilité des risques, l'exploitant d'une IC réalise une Etude de Danger (EDD) qui recense l'ensemble des phénomènes dangereux et accidents majeurs liés à l'installation et pouvant avoir des effets à l'extérieur du site, évalue leur intensité et gravité (distance d'effet et nombre de personnes potentiellement exposées) et leur probabilité d'occurrence. L'évaluation de la probabilité dans les EDD a été instaurée dans le code de l'environnement par la loi du 30 juillet 2003. Probabilités et gravités sont estimées selon des échelles définies dans l'Annexe 1 de l'arrêté ministériel du 29 septembre 2005 [1]. Le couple gravité / probabilité permet de situer les différents accidents identifiés dans une matrice d'acceptabilité et ainsi d'apprécier la maîtrise des risques d'accident majeur pour l'établissement considéré.

L'approche retenue pour évaluer les risques dans les études de dangers se déroule en plusieurs étapes :

- une analyse qualitative des risques permet d'identifier tous les scénarios et de sélectionner les phénomènes avec des effets potentiels à l'extérieur du site ;
- une étude détaillée des risques permet de quantifier ces risques en probabilité et gravité ;
- les mesures de maîtrise des risques permettant de maintenir le risque à un niveau acceptable sont identifiées.

Pour l'analyse qualitative, on utilise généralement une démarche telle que l'Analyse Préliminaire des Risques (APR) qui permet d'identifier les risques de manière exhaustive sans entrer dans le détail du fonctionnement de l'installation. On identifie ainsi des situations dangereuses sans étudier de manière détaillée leur probabilité ou gravité.

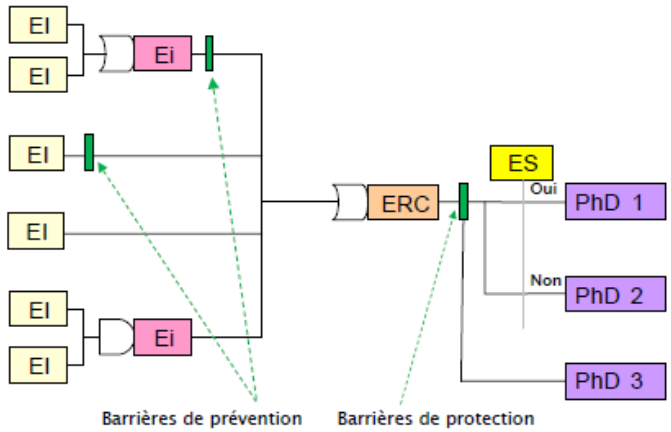
La phase d'étude détaillée des risques (EDR) a pour objectif de déterminer la probabilité, la gravité et la cinétique des phénomènes dangereux susceptibles de générer des effets à l'extérieur des limites du site retenus lors de la phase d'analyse qualitative.

Le modèle du nœud papillon, qui combine pour un système arbre de défaillances et arbre d'événements, est le modèle le plus utilisé pour l'étude détaillée des risques. En effet, il donne un aperçu global des scénarios menant aux accidents majeurs, en mettant en évidence les différentes causes possibles, qui sont des évènements aléatoires et accidentels tels que des fuites ou ruptures d'équipements mécaniques, des défaillances de systèmes de contrôle commande ou des erreurs opératoires, avec les liens logiques existant entre elles et en mettant en valeur les barrières de sécurité permettant de réduire leur probabilité d'occurrence. De plus, la représentation permet de visualiser les chemins critiques, c'est à dire d'identifier les branches causales les plus contributives à l'occurrence du scénario d'accident en vue d'améliorer la maîtrise des risques. La figure 1 donne un exemple de représentation d'un scénario sous forme de nœud papillon.

Les barrières de sécurité peuvent être des dispositifs passifs (cuvettes de rétention), mécaniques (soupapes) électromécaniques ou instrumentés (SIS : Systèmes Instrumentés de Sécurité).

L'évaluation des performances des barrières de sécurité et de leur probabilité de défaillance repose généralement sur une approche semi-quantitative. Des règles de maîtrise du vieillissement s'appliquent ; elles supposent l'application d'exigences de conception, test et maintenance définies notamment par les arrêtés du 29 septembre 2005 et du 4 octobre 2010. Ces exigences sont inspirées des normes de sécurité fonctionnelle IEC 61508 et IEC 61511 [9] qui fixent des règles sur les architectures des systèmes, le développement des logiciels et les processus de validation, tests périodiques et gestion des modifications. Les barrières de sécurité reposant sur des capteurs actionneurs et automates sont classifiées comme MMRI (Mesures de Maîtrise des Risques Instrumentées).

La maîtrise des risques industriels, telle qu'elle est appliquée dans les EDD, vise donc à évaluer et réduire à un niveau acceptable les risques que des installations, principalement de l'industrie du procédé, font peser sur les personnes et l'environnement. Il s'agit d'une démarche globale – prenant en compte une installation dans son ensemble - de maîtrise d'un risque spécifique (impacts sur les personnes et l'environnement).



Légende :
EI : Evènement initiateur
Ei : Evènement intermédiaire
ERC : Evènement Redouté Central. Il s'agit généralement d'une perte de confinement.
ES : Evènement secondaire. Il peut s'agir de 'inflammation d'un nuage de gaz par exemple.
PhD : Phénomènes Dangereux (explosions, incendies, dispersions toxiques pouvant porter atteinte à des enjeux à protéger.

Fig. 1. Modèle de représentation de scenario d'accident sous forme de nœud papillon

B. La cybersécurité des installations industrielles

La cybersécurité des installations industrielles fait l'objet d'une importante activité de réglementation, de publication de guides méthodologiques et de normalisation. Elle touche les systèmes industriels au sens large, qu'il s'agisse de transports, hôpitaux, production d'énergie, distribution d'eau, industrie manufacturière ou industrie du procédé. En France, des exigences réglementaires sont applicables aux Opérateurs d'Importance Vitale (OIV) depuis le dernier trimestre 2016 au travers d'arrêtés spécifiques qui s'appuient sur des guides élaborés par des Groupes de Travail sur la cybersécurité des installations industrielles dirigés par l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) [6][7].

Les OIV, Opérateurs d'Importance Vitale, sont des opérateurs, publics ou privés, qui exercent des activités comprises dans l'un des 12 Secteurs d'Activité D'Importance Vitale (SAIV) définis sous l'autorité du premier ministre, et gèrent ou utilisent au titre de ces activités un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement :

- d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation ;
- ou de mettre gravement en cause la santé ou la vie de la population.

L'article 22 de la loi de programmation militaire 2014-2019[4], intègre des dispositions spécifiques à la cybersécurité des OIV. Selon cet article, le premier ministre - par le biais de l'ANSSI - sera en mesure :

- de fixer des obligations de protection contre la cyber-menace ;
- d'imposer la mise en place d'un système de détection des attaques ;
- de faire vérifier le niveau de sécurité des systèmes informatiques par l'intermédiaire de contrôles (par l'ANSSI ou par des prestataires qualifiés) ;
- d'exiger que les opérateurs l'informent de tout incident affectant la sécurité de leurs systèmes.

Le décret d'application de l'article 22 a été publié au JO le 29 mars 2015 [5]. Il précise que :

- l'ANSSI est chargée de la rédaction des arrêtés sectoriels après avis des ministres coordonnateurs des secteurs d'activités d'importance vitale concernés;
- chaque OIV établit et tient à jour sa liste des « systèmes d'information d'importance vitale » (SIIV) ;
- la mise en œuvre de moyens de détection des atteintes à la sécurité des SIIV sera imposée ;
- les OIV doivent informer l'ANSSI des incidents affectant leurs SIIV ;
- des contrôles de sécurité peuvent être imposés aux OIV ;
- l'ANSSI propose au premier ministre les mesures appropriées en cas de crise majeure.

Des arrêtés sectoriels ont été rédigés sous responsabilité de l'ANSSI en impliquant les différents ministères coordinateurs ainsi que les OIV concernés et publiés en 2016 et 2017.

L'application de cette réglementation nécessite l'identification des SIIV - systèmes d'informations d'importance vitale - qui sont les systèmes informatiques (technologies de l'information ou technologies industrielles), impliqués dans la gestion ou le contrôle des OIV et « pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ».

Les exigences d'identification des SIIV et de définition de mesures de sécurité applicables ont été définies en s'inspirant notamment des guides « Méthode de classification et mesures principales »[6] et « mesures détaillées » [7] du GT Cybersécurité des installations industrielles de l'ANSSI.

Ces guides permettent d'appliquer une démarche en trois étapes, similaire à celle de l'étude de dangers :

- identification des systèmes d'information critiques à partir d'une démarche qualitative ;
- analyse détaillée des risques pour ces systèmes d'information ;
- définition des mesures de sécurité applicables à ces systèmes.

Le premier guide présente une méthode de classification des Systèmes automatisés de contrôle industriels – qui comprennent les systèmes de contrôle commande et leurs interactions avec les systèmes de gestion.

Pour réaliser cette classification on doit disposer dans un premier temps d'une cartographie du réseau du site ou de l'entreprise permettant d'identifier un ou plusieurs systèmes de contrôle industriels qui peuvent être cloisonnés. Une analyse de risques succincte est ensuite réalisée pour chaque système de contrôle identifié. Pour cela, deux paramètres sont évalués : la vraisemblance de l'attaque du système et sa gravité en termes d'impacts sur des biens essentiels. Cette méthode de classification est une approche simplifiée des différentes méthodes d'analyse des risques cyber telles que la méthode EBIOS par exemple.

La figure 2 ci-dessous, tirée du guide ANSSI, présente les critères de classification.

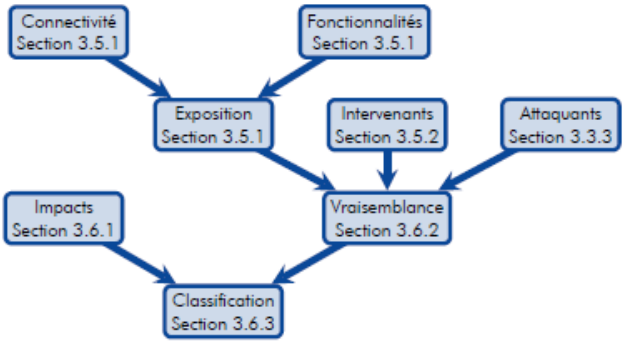


Fig. 2. Schéma représentant la méthode de classification

Le guide de l'ANSSI traite principalement de l'évaluation de la vraisemblance des risques. Celle-ci est l'estimation de la possibilité qu'un scénario de menace ou un risque, se produise. Elle est estimée en fonction des technologies et des fonctionnalités des systèmes, de leur connectivité, de la gestion des intervenants et du niveau des attaquants potentiels.

Pour l'évaluation de la gravité des risques, le guide présente simplement des échelles de gravité pour les impacts humains et environnementaux et pour les impacts consécutifs à l'arrêt du service rendu (impacts économiques). Les moyens d'évaluer précisément les impacts d'une attaque et de les situer sur ces échelles ne sont pas présentés dans le guide.

La cotation des systèmes de contrôle industriels dans une matrice vraisemblance-gravité permet de les classer en fonction de leurs besoins de sécurité. Trois classes sont proposées par cette méthode. La matrice ci-contre (fig. 3) tirée du guide ANSSI permet de classer les systèmes en fonction des Impacts et de la Vraisemblance de leur attaque.

Les guides donnent peu d'éléments sur l'analyse détaillée des risques. Ils précisent uniquement que pour les systèmes de classe 3, l'analyse des risques devrait être faite par un prestataire homologué. Il est également recommandé que « la cybersécurité du système industriel soit intégrée à l'analyse de risque globale du système pouvant traiter par exemple des aspects de sûreté de fonctionnement ». Les références pour cette partie citent la norme ISO/CEI 27005 [8] qui définit un processus général de gestion de risques liés aux systèmes d'information mais ne propose pas de méthode détaillée d'analyse. Le processus traite en particulier de l'appréciation des risques liés à un système en termes d'impacts sur des biens essentiels, propose différentes stratégies de traitement de ces risques et définit une phase d'acceptation des risques résiduels.

En fonction de la classe d'un système industriel et des résultats de l'analyse des risques, des mesures de sécurité plus ou moins contraignantes sont applicables. Ces mesures sont de différentes natures :

- mesures organisationnelles : responsabilités, gestion, contrôle et formation des intervenants, processus de veille sur les menaces et vulnérabilités ;
- mesures techniques : outre les règles sur l'architecture et les fonctionnalités autorisées (télémaintenance, etc.) deux types de dispositifs de sécurité peuvent être mis en œuvre :
    - les dispositifs prévenant les intrusions au niveau des interconnexions réseaux tels que les diodes ou les pare-feu ;
    - les moyens de surveillance ou de détection permettant de détecter les attaques tels que les sondes ;
- processus de gestion de crise.

Les arrêtés sectoriels définissent des règles d'identification et de classification des SIIV et les mesures de sécurité requises spécifiques pour chaque SAIV.

5+	Classe 2	Classe 2	Classe 3	Classe 3
4	Classe 2	Classe 2	Classe 2	Classe 3
3	Classe 1	Classe 2	Classe 2	Classe 2
2	Classe 1	Classe 1	Classe 2	Classe 2
1	Classe 1	Classe 1	Classe 1	Classe 1
Impact/Vraisemblance	1	2	3	4+

Fig. 3. Matrice Impact/Vraisemblance

La maîtrise de la cybersécurité des systèmes industriels vise donc à évaluer et réduire à un niveau acceptable les risques que des installations critiques de tous types font peser sur les personnes, l'environnement ou les risques liés à l'arrêt du service rendu par ces installations. Il s'agit d'une démarche de maîtrise des risques de tous types liés à des technologies spécifiques (numériques).

IV. Interactions entre la maîtrise globale des risques et la cybersécurité

A. Impacts de la cybersécurité sur la maîtrise des risques industriels

Les systèmes de contrôle commande étaient dans le passé des systèmes fermés utilisant des technologies électromécaniques et des automates programmables industriels. Ces systèmes, que l'on peut désigner comme OT (Operational Technology) étaient techniquement différents ainsi que physiquement et fonctionnellement indépendants des systèmes d'information de l'entreprise. Ces systèmes d'information, regroupant des systèmes de gestion et de bureautique, communiquant le plus souvent avec l'extérieur sont souvent désignés comme IT (Information technology). Les systèmes OT étaient (et sont toujours) conçus et mis en œuvre par des automaticiens, les systèmes IT par des informaticiens.

La ségrégation entre ces systèmes tend à disparaître dans les installations industrielles actuelles, y compris dans l'industrie des procédés. Les systèmes OT, sont de plus en plus interconnectés avec l'IT et utilisent des technologies issues de ce domaine. Par exemple, certains automates sont émulés sur des PC industriels tournant sur des OS (Operating System) grand public, ou encore, les communications industrielles, analogiques sont remplacées par des bus de terrain industriels (profibus, modbus) voire par des protocoles de communication issus de l'IT (ethernet). Au minimum, même lorsque la diversité technologique est maintenue, les systèmes OT sont connectés avec les systèmes IT pour assurer des fonctions de supervision, de gestion de production ou de télémaintenance par exemple.

Conséquence de cette convergence, les virus et les attaques informatiques qui ont longtemps ciblé principalement les systèmes IT touchent désormais également les systèmes OT. Par exemple, les attaques WannaCry et NotPetya en 2017 visaient des failles de sécurité de Windows et ont affecté le fonctionnement de systèmes industriels [9][10]. Ces systèmes

sont également plus vulnérables à des attaques ciblées telles que Stuxnet (attaque bénéficiant de moyens techniques et humains très importants) ou telles que l'attaque (sans conséquences graves) du barrage de bowman dam dans l'état de New-York par exemple [11].

Les objectifs et conséquences des cyber-attaques sont variés : les motivations des attaquants peuvent être lucratives, idéologiques, techniques ou pathologiques par exemple. De plus les attaques peuvent être non ciblées et à grande échelle (virus touchant une technologie IT) ou cibler une installation spécifique (attaque préparée et coordonnée visant un site industriel ou une infrastructure critique spécifique).

Pour les attaques ciblées, les profils des attaquants sont également divers : on peut considérer des attaquants externes disposant de compétences en informatique et de moyens techniques importants ou des attaquants internes (employés mécontents) disposant de connaissances importantes sur le site et d'un accès facilité à l'intérieur du réseau.

Suivant les motivations, les profils et les moyens des attaquants, les équipements visés et les conséquences seront différents. Dans le domaine de la cybersécurité, les principaux référentiels tels que la norme ISO 27001[9] visent à protéger différentes propriétés de l'information :

- la disponibilité : le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu ;
- l'intégrité : les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante ;
- la confidentialité : seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

La corruption de ces propriétés sur un système de contrôle industriel peut avoir des impacts variables. De manière générale, les actes de sabotage ayant pour objectif d'atteindre les personnes ou l'environnement nécessiteront de corrompre l'intégrité des données : l'attaquant cherchera à exécuter des commandes non légitimes pouvant provoquer des phénomènes dangereux. L'atteinte à la disponibilité de certains systèmes, qui ne seront alors plus aptes à exécuter les fonctions attendues, peut également avoir des impacts sur la sécurité.

On peut considérer qu'il faut au minimum évaluer la résistance d'un système de contrôle industriel à une attaque non ciblée de type rançongiciel provoquant l'indisponibilité de certains systèmes. Ce type d'attaques étant relativement fréquent, elles pourraient être prises en compte comme des agressions externes dans les EDD au même titre que les agressions environnementales. La prise en compte d'attaques ciblées, d'origines internes ou externes, doit être envisagée en fonction de l'importance des enjeux et de leur difficulté de réalisation.

De nombreux guides et normes traitant de la cybersécurité des installations industrielles ont été publiés ou sont en cours de rédaction, ils sont pour beaucoup difficilement applicables au contexte des IC car ils sont soit trop complexes, soit trop généraux et souvent issus d'approches utilisées pour les technologies de l'information et donc peu adaptés au contrôle-commande industriel. Par ailleurs, ils ne traitent pas du sujet spécifique de la maîtrise des risques pour les personnes et l'environnement.

Les technologies utilisées pour certaines barrières de sécurité sont vulnérables du point de vue de la cybersécurité. En particulier, la note de doctrine du 2 octobre 2013 comme les évolutions récentes des normes internationales autorisent la valorisation de mesures de maîtrise des risques réalisées par les automates de conduite de l'installation. Ceci tend à augmenter la vulnérabilité de l'installation aux attaques car ces systèmes sont souvent moins bien isolés du réseau que les systèmes instrumentés de sécurité. D'autres évolutions technologiques, potentiellement utilisées par les MMRI peuvent être sources de vulnérabilités en mettant en cause leur indépendance ou leur isolement : on peut citer en particulier les réseaux sans-fils, la télémaintenance, les capteurs intelligents, les systèmes de health monitoring.

Les exigences requises par les référentiels d'évaluation de la performance des barrières instrumentées, les normes de sécurité fonctionnelle et les textes relatifs à la cybersécurité sont souvent de nature similaire et s'appuient sur le cycle de vie complet du système. Différents documents visent donc à intégrer des exigences de cybersécurité à des référentiels de sûreté de fonctionnement tels que les normes de sécurité fonctionnelle IEC 61508 et IEC 61511 par exemple. L'application de ces normes n'est toutefois qu'un des éléments de l'approche globale de la maîtrise des risques industriels.

Dans ce contexte, toujours en évolution, il apparaît nécessaire d'intégrer l'exigence de maîtrise de la cybersécurité à la maîtrise globale des risques des Installations Classées. Pour ce faire, des modèles combinant ces deux problématiques ont été développés [8]. Ils devront être intégrés à une approche globale de maîtrise des accidents majeurs (impacts sur les personnes et l'environnement) intégrant les évènements accidentels aléatoires et les problématiques de cybersécurité.

Différents aspects de la cybersécurité devront être pris en compte dans cette approche :

- l'intégration de la cybersécurité dans les analyses des risques pour intégrer les scénarios malveillants dans le cadre de la maîtrise des risques pour les personnes et l'environnement de manière globale ;
- l'intégration de critères de cybersécurité dans la conception des Systèmes Instrumentés de Sécurité ayant des exigences de sûreté de fonctionnement définies par les normes de sécurité fonctionnelle (IEC 61508 et IEC 61511) ;
- le développement de processus de gestion de crise permettant de maintenir le niveau de risque de l'installation à un seuil acceptable lorsqu'une attaque, ciblée ou non, provoque l'indisponibilité de certains systèmes.

B. Comparaison des concepts et approches en Maîtrise des Risques Industriels et Cybersécurité

Le tableau ci-dessous donne des éléments de comparaison entre la maîtrise des risques industriels et la maîtrise de la cybersécurité pour les installations industrielles :

TABLE I. COMPARAISON ENTRE MAITRISE DES RISQUES INDUSTRIELS ET CYBERSECURITE

Maîtrise des risques industriels	**Cybersécurité des installations**
Réglementaire pour les IC	Réglementaire pour les OIV
Principalement industrie du procédé	Types d'activités très variables
Prévention des risques affectant la santé et la sécurité des riverains ou l'environnement	Protection du service rendu, des infrastructures, du potentiel économique, de la sécurité des personnes et de l'environnement
Evaluation des conséquences de situations accidentelles aléatoires	Evaluation des conséquences d'attaques malveillantes délibérées
Analyse des risques orientée par les phénomènes dangereux	Analyse des risques orientée par la conception des systèmes de contrôle-commande
Analyse des risques découpée par installations	Analyse des risques découpée par systèmes de contrôle commande
Prise en compte d'un éventail large d'évènements initiateurs	Attaques vues comme l'intrusion sur le système OT depuis le système IT
Evènements initiateurs et couches de protection indépendante	Attaques coordonnées de différents systèmes possibles
Evaluation de la probabilité	Evaluation de la vraisemblance
Maîtrise des risques basée sur des couches de protection et de prévention indépendantes	Les différents systèmes de contrôle commande ne peuvent pas être considérés comme indépendants dans le cas d'une attaque ciblée
Evolutions récentes permettent de valoriser des fonctions indépendantes sur un système unique suffisamment fiable	L'utilisation d'un système unique rend l'attaque plus simple et augmente sa vraisemblance
Mesures de maîtrise des risques basées sur les scénarios d'accident (déviation des situations normales de procédé)	Mesures de sécurité basées sur la sécurisation des vulnérabilités du système informatique
Maintenance préventive pour maintenir la performance dans le temps	Application de correctifs lorsque des vulnérabilités sont découvertes

V. VERS UNE DÉMARCHE D'ANALYSE DE RISQUES INTÉGRANT LA CYBERSÉCURITÉ

L'intégration de causes malveillantes et en particulier de cyberattaques aux analyses des risques n'est pas évidente : en effet, des attaques complexes peuvent mettre en œuvre la corruption simultanée de plusieurs systèmes et la réalisation de commandes multiples conçues pour provoquer un phénomène dangereux. Les méthodes habituellement utilisées, telles que les APR et les HAZOP, ne permettent pas de prendre en compte les actes malveillants délibérés et les combinaisons de différentes attaques.

L'application de solutions issues de l'IT à l'ensemble des systèmes de contrôle industriels n'est pas satisfaisante non plus : ces solutions peuvent être très contraignantes d'un point de vue opérationnel (forte limitation des communications par exemple) et les dispositifs de sécurité développés pour l'industrie s'avèrent très couteux lors de l'acquisition initiale et pour leur maintien dans le temps. De plus les solutions techniques sont toujours susceptibles de contenir des failles de sécurité et d'être contournées, ce qui peut être plus critique dans le cadre de la prévention d'accidents majeurs que dans le cadre général de la sécurité des systèmes IT.

Abdo, et al.[15], propose une méthode, dite ATBT (Attack Tree Bow Tie), combinant les nœuds-papillons et des arbres d'attaques permettant d'identifier des causes malveillantes aux scénarios décrits dans les analyses de risques classiques.

Cette approche s'applique toutefois à la phase d'analyse détaillée des risques uniquement et ne permet pas d'identifier de façon exhaustive les phénomènes dangereux ayant des causes uniquement malveillantes et qui ne seraient donc pas identifiés lors des analyses préliminaires des risques.

Cet article propose donc une démarche en trois étapes :

- une analyse qualitative des risques intégrant les cyberattaques basées sur les APR ;
- une évaluation détaillée des risques basée sur le modèle ATBT ;
- une identification des barrières à mettre en œuvre vis-à-vis des évènements accidentels et des évènements malveillants.

A. Analyse qualitative des risques

L'intégration de causes malveillantes et en particulier de cyberattaques à ces analyses de risques n'est pas évidente : en effet, des attaques complexes peuvent mettre en œuvre la corruption de plusieurs systèmes et la réalisation de commandes multiples.

La réalisation d'une analyse inductive, de type AMDEC ou HAZOP, partant des différents types de corruption possibles de de chaque équipement du système de contrôle industriel et identifiant leurs conséquences possibles ainsi que les conséquences de la combinaison de corruptions concomitantes de plusieurs équipements s'avère complexe. Les équipements peuvent être nombreux, les modes de corruptions variés (indisponibilité (suite à une anomalie détectée, la corruption ou destruction de données), modification de seuils, corruption de

commandes, modification de variables ou des valeurs mesurées).

Une approche déductive, partant des évènements redoutés pour en identifier les causes malveillantes possibles est donc privilégiée.

Dans le cadre des Etudes de dangers, et dans le contexte de procédés industriels, les Evènements Redoutés sont définis comme la perte de confinement non maîtrisée d'un produit (généralement liquide ou gaz). La perte de confinement en elle-même peut être la source de phénomènes dangereux dans certains cas, dans d'autres cas des évènements secondaires (e.g. inflammation d'un nuage de gaz explosible) peuvent être nécessaires.

On cherche donc à identifier pour chaque produit présent sur le site les conditions possibles d'une perte de confinement pouvant provoquer un phénomène dangereux susceptible d'atteindre des personnes ou l'environnement. Les conditions de réalisation des pertes de confinement sont de différentes natures :

- A : modification de paramètres physiques (pression, température, débit…) par commande de vannes, compresseur ou systèmes de chauffe par exemple ;
- B : rejet dangereux par débordement d'une capacité ou manœuvres illégitimes d'organes (vannes, clapets) ;
- C : mise en contact de produits réagissant de manière dangereuse ;
- D : arrêt de système fonctionnant en continu pour maintenir le procédé dans un état de sécurité (ventilation, aspiration, inertage).

Le modèle de cyber-APR suit une démarche systématique cherchant à déterminer quels phénomènes sont critiques, s'il existe des moyens de provoquer ces phénomènes et s'il existe des moyens de les détecter ou des barrières de sécurité qui éviteront les conséquences. La démarche proposée est la suivante :

- Phase préparatoire
  - O1- Identification des produits de l'installation ;
  - O2- Identification des équipements de contrôle commande de bas niveau (capteurs, automates et actionneurs).
- A : Analyse des risques liés à la variation des paramètres physiques, pour chaque produit :
  - A1- identification des paramètres physiques critiques ;
  - A2- identification de l'existence de moyens de commande permettant de dépasser ces paramètres ;
  - A3- Identification des moyens de détection et des barrières de sécurité et de la possibilité pour l'attaquant de les rendre inopérants.
- B : Analyse des risques liés aux rejets, pour chaque produit :
  - B1- Identification des risques liés à un rejet malveillant ;
  - B2- identification des moyens (vannes, pompes, compresseurs, corruption de capteurs) permettant de réaliser ces rejets ;
  - B3- Identification des moyens de détection et des barrières de sécurité et de la possibilité pour l'attaquant de les rendre inopérants ;
- C : Analyse des risques liés aux mélanges incompatibles :
  - C1- Réalisation d'une matrice d'incompatibilité permettant d'identifier les mélanges potentiellement dangereux ;
  - C2- identification des moyens permettant de réaliser ces mélanges ;
  - C3- Identification des moyens de détection et des barrières de sécurité et de la possibilité pour l'attaquant de les rendre inopérants.
- D : Analyse des risques liés à la corruption de systèmes maintenant l'installation dans un état sûr :
  - D1- Identification de ces systèmes ;
  - D2- identification des moyens de les corrompre ou de les arrêter ;
  - D3- Identification des moyens de détection et des barrières de sécurité et de la possibilité pour l'attaquant de les rendre inopérants.

Pour chacune des 4 étapes A, B, C et D, on retiendra les évènements critiques, pouvant être provoqués par des actions illégitimes sur le contrôle commande et pour lesquels il n'existe pas de barrières ou moyens de détection ne pouvant être corrompus. Ces évènements seront étudiés en détail dans l'étude détaillée des risques.

L'évaluation présentée ci-dessus vient en complément de l'analyse des risques classique réalisée au travers d'une APR par exemple.

B. Evaluation détaillée des risques

L'analyse détaillée des risques repose sur le modèle ATBT combinant nœuds papillons et arbres de défaillance. Les évènements modélisés par ces nœuds papillon sont issus de l'APR classique et de la cyber-APR. Il convient de fusionner les différents évènements lorsque c'est possible.

Pour les évènements issus de l'APR classique, à partir des nœuds papillon réalisés, les évènements pouvant être provoqués par une attaque malveillante (e. g. fermeture d'une vanne, commande erronée d'un automate) sont identifiés. Les arbres d'attaques menant à ces évènements sont ensuite construits et reliés au nœud papillon. Les modèles ainsi construits permettent d'identifier des séquences purement accidentelles, des séquences purement malveillantes et des séquences mixtes. La possibilité d'occurrence des différentes séquences est ensuite cotée selon un vecteur à 2 dimensions : la probabilité (accidentelle) et la vraisemblance (malveillante).

On considère qu'une attaque nécessitant l'occurrence simultanée d'un évènement aléatoire pour aboutir au phénomène dangereux souhaité a peu de risque d'être réalisée

avec succès et n'a pas besoin d'être retenue comme scénario critique.

Cette approche met en évidence les séquences malveillantes et permet donc d'identifier soit les systèmes de contrôle à sécuriser pour diminuer leur vraisemblance soit les barrières de sécurité d'autres technologies, non vulnérables aux cyberattaques, permettant de réduire la probabilité de réussite de l'attaque.

Pour les évènements identifiés dans les cyber APR et non pris en compte dans les nœuds papillon issus de l'APR classique, on réalise des nœuds papillon spécifiques qui contiendront uniquement des séquences purement malveillantes.

Ces séquences seront cotées en vraisemblance dans un premier temps. Suivant les mesures de sécurité mises en œuvre, une probabilité pourra également être affectée à ces séquences.

C. Définition des mesures de sécurité

Les mesures de sécurité adaptées aux risques accidentels et aux risques malveillants peuvent se renforcer mutuellement.

En effet, la mise en œuvre de barrières passives (type cuvette de rétention) ou de dispositifs actifs (type soupape) sur une séquence purement malveillante obère la capacité de l'attaquant à atteindre ses objectifs. Cette approche permet d'éliminer des scénarios malveillants et de limiter les besoins de sécurité informatique. Il faut néanmoins prendre en compte les scénarios résiduels résultant de l'activation de ces barrières.

Dans certains cas, les mesures de sécurité informatique seront nécessaires, l'analyse des risques aidera dans ce cas à identifier les parties du système de contrôle commande devant être protégées et les types d'attaques à considérer (interne/ externe, ciblée/ non ciblée). On appliquera au minimum pour les systèmes identifiés les bonnes pratiques de cybersécurité des systèmes industriels et si besoin des normes de cybersécurité et des mesures techniques devront être mises en œuvre. Des critères de performance de ces mesures de sécurité, permettant d'évaluer leur impact sur la vraisemblance doivent encore être définis.

Ce processus d'analyse des risques permettra également d'améliorer l'utilisation et le paramétrage des sondes de détection des cyberattaques. En effet, de nombreuses sondes industrielles sont en cours de qualification pour être mises sur le marché. Ces sondes peuvent en général intégrer des règles métier qui leur permettent de détecter des évènements (trames, paramètres) anormaux et de remonter des alarmes. Le plus souvent, les fournisseurs ne disposent pas de règles métiers complètes et formalisées. Ils réalisent donc un paramétrage lié à l'architecture informatique du système et non aux évènements redoutés. Les résultats de la méthode proposée permettront de paramétrer les sondes en fonction des risques.

VI. CONCLUSION

Les exploitants étant responsables des risques que leurs installations font peser sur les populations et l'environnement, ils doivent prendre en compte les phénomènes émergents que sont les attaques des systèmes de contrôle industriel. L'intégration de cette problématique dans l'analyse globale des risques permet de valoriser des mesures de maîtrise des risques liées aux scénarios accidentels dans la maîtrise des risques cyber, et inversement de valoriser des mesures de sécurisation des systèmes de contrôle commande dans la maîtrise des risques accidentels. Cette approche permet également de mieux cibler les systèmes à protéger. Cette approche est centrée sur la maîtrise globale des risques accidentels mais ne prend pas en compte la protection d'autres enjeux comme les informations ou la production.

Les développements ultérieurs permettront d'affiner les critères d'acceptabilité d'un risque ayant des dimensions de vraisemblance et probabilité. On cherchera également à proposer une démarche plus globale intégrant les exigences relatives à la cybersécurité au processus global de gestion des risques industriels en prenant en compte par exemple le maintien du niveau de sécurité dans le temps, la gestion des personnes et des compétences, la préparation des plans d'urgence.

REFERENCES

[1] Arrêté ministériel du 29/09/05 relatif à l'évaluation des risques dans les études de dangers des installations classées soumises à autorisation

[2] Guide méthodologique pour la gestion et la maîtrise du vieillissement des mesures de maîtrise instrumentées (MMRI) DT 93, (BRIEC (ex BRTICP), 2011)

[3] Note de doctrine sur les mesures de maîtrise des risques instrumentées (MMRI) (BRIEC (ex BRTICP), 2013)

[4] Loi de programmation militaire du 19 décembre 2013 – Article 22

[5] Décret d'application n°2015-351 du 27 mars 2015

[6] Méthode de classification et mesures principales – GT Cybersécurité des installations industrielles (ANSSI 2014)

[7] Mesures détaillées – GT Cybersécurité des installations industrielles (ANSSI 2014)

[8] ISO/IEC 27005 :2011 Technologies de l'information -- Techniques de sécurité -- Gestion des risques liés à la sécurité de l'information

[9] WannaCry Campaign: Potential State Involvement Could Have Serious Consequences, Centre de Cyber-défense de l'OTAN, 2017

[10] NotPetya and WannaCry Call for a Joint Response from International Community, Centre de Cyber-défense de l'OTAN, 2017

[11] Analysis of the recent reports of attacks on US infrastructure, SANS ICS, 2016

[12] A suvrey of approaches combining safety and security for industrial control systems, Siwar Kriaa, Ludovic Pietre-Cambacedes, Marc Bouissou, Yoran Halgand, 2015

[13] Recommendations to align safety and security for industrial automation control systems, ISA 99 WG7, 2015

[14] ISA-TR84.00.09-2013: Security Countermeasures Related to Safety Instrumented Systems (SIS), ISA, 2013

[15] H. Abdo, M. Kaouk, J-M. Flaus, F. Massé, "Towards a better industrial risk analysis: a new approach that combines cyber security within safety", ESREL, 2017

Norme IEC 61511 ed.2, (Commission Electrotechnique Internationale, 2015).