Comment intégrer les cyber-attaques dans l'évaluation globale des risques pour les installations classées ? Proposition d'un cadre général d'analyse des risques

François Masse, H Abdo, Jean-Marie Flaus

Comment intégrer les cyber-attaques dans l'évaluation globale des risques pour les installations classées ? Proposition d'un cadre général d'analyse des risques

A General risk analysis framework to integrate cyberattacks to the overall risk assessment of hazardous installations

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

Abdo H. et Flaus J.M.
G-SCOP
Université Grenoble Alpes
Grenoble, France
Houssein.abdo@grenoble-inp.fr
jean-marie.flaus@grenoble-inp.fr

Résumé

De nombreux guides, méthodes, normes, recommandations ou réglementations traitent des sujets de la maîtrise des risques industriels d'une part ou de la cybersécurité des installations industrielles d'autre part. Ces deux sujets interagissent 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 coordonnée et efficiente à un même système.
Cet article compare les approches et présente les implications possibles de la cyber malveillance sur la maîtrise des risques pour les installations classées. Une démarche méthodologique générale pour prendre en compte la cybersécurité dans la maîtrise des risques pour les personnes et l'environnement, en particulier dans l'industrie des procédés est ensuite proposée.

Summary

Many guides, methods, standards, recommendations or regulations deal with industrial risk control on the one hand or cybersecurity of industrial installations on the other. These two subjects interact but the normative and regulatory documents as well as the methodologies implemented have been developed separately. It can therefore be difficult to apply them in a coordinated and efficient way to the same system.
This paper compares the approaches and presents the possible implications of cyber threats on the risk assessment of hazardous installations. A general framework to consider cyber security in the risk assessment for people and environment in the process industry is then proposed.

Introduction

Les vulnérabilités des systèmes de contrôle-commande et des systèmes instrumentés de sécurité constituent une menace pour la sécurité des installations industrielles. Ces systèmes peuvent être vulnérables soit à des attaques malveillantes ciblées soit à différents types d'attaques non ciblées auxquels sont exposés les systèmes ouverts sur internet (virus, rançongiciels, etc.). La convergence entre les technologies des automatismes industriels et les technologies informatiques, l'utilisation de réseaux sans fils, l'interconnexion entre les systèmes de contrôle-commande, les systèmes de sécurité et les systèmes de gestion (y compris les systèmes bureautiques et les connexion internet) entraînent l'accroissement de la vulnérabilité des systèmes industriels et donc des attaques les touchant.
Différentes enquêtes montrent l'augmentation exponentielle des incidents touchant des systèmes industriels. Ces attaques menées par des employés mécontents, des organisations criminelles, etc. sont courantes mais visent principalement l'arrêt ou l'endommagement d'installations, la fraude ou l'extorsion. Cependant, les méthodes pour réaliser ces attaques peuvent être utilisées pour corrompre les systèmes de contrôle industriels de manière à provoquer des phénomènes dangereux pour la sécurité des opérateurs, des riverains ou de l'environnement. Ces attaques sont susceptibles, au même titre que des défaillances aléatoires, de provoquer des accidents majeurs. Il apparaît donc nécessaire d'évaluer et de limiter l'impact de la cybersécurité sur la maîtrise des risques accidentels.

Le traitement conjoint de ces deux sujets est complexe : les cultures de ces deux métiers sont différentes, les domaines d'application se recouvrent partiellement (procédé physique et contrôle commande d'un côté, système de contrôle commande et systèmes d'information de l'autre) mais des exigences antagonistes peuvent donc ressortir des deux analyses.
Différents cadres méthodologiques ont été proposés pour traiter de manière conjointe sûreté de fonctionnement et cybersécurité ou maîtrise des risques industriels et cybersécurité (projet SESAMO, méthode CORAS). Il s'agit principalement de méthodes s'attachant à l'analyse du système de contrôle commande et de ses dérives.

L'objet de cet article est de présenter une méthodologie permettant d'intégrer la cybersécurité dans l'analyse des risques physiques d'un procédé chimique. Cette méthodologie d'analyse doit permettre d'identifier les scénarios d'attaques ayant des effets physiques sur le procédé et générateurs de risques pour les personnes et pour l'environnement et de faire le lien entre les études de danger des installations classées et l'évaluation de la cybersécurité des systèmes de contrôle industriels.
Cet article présente donc :

- le contexte et les enjeux de la cybersécurité des systèmes de contrôle industriel dans une première partie ;
- les méthodes d'analyse des risques existantes applicables aux systèmes de contrôle industriels ;
- le cadre d'analyse proposé par l'INERIS ainsi que par le laboratoire G-SCOP de l'INPG pour identifier et

évaluer les scénarios de cyberattaques affectant la sécurité des personnes et l'environnement.

Contexte de la cybersécurité des installations industrielles

Le sujet de la cybersécurité des installations industrielles a émergé suite à l'attaque Stuxnet (2011) visant les sites d'enrichissement d'uranium iraniens. Cet exemple, l'un des premiers cas d'attaque publiquement documenté, s'il a eu le mérite de mettre en lumière les enjeux de la cybersécurité des installations industrielles, a le défaut d'être peu représentatif pour la plupart des exploitants : il s'agit d'une attaque très sophistiquée, menée par des entités bénéficiant de moyens importants (estimés à 10 000 jours de développement hors acquisition de données sur les installations iraniennes et la conception de certains équipements) et ciblant une infrastructure stratégique précise pour interrompre ou ralentir sa production. Les exploitants pour la plupart ne se considèrent pas, à juste raison, des cibles potentielles pour ce type d'attaques. Cependant, des attaques plus récentes et moins sophistiquées ont mis en lumière les menaces cyber pesant sur les installations industrielles. L'émergence de ce sujet a été accentuée en France par l'application de la loi de programmation militaire 2014-2019 fixant des exigences de maîtrise de la cybersécurité aux opérateurs d'importance vitale (OIV) précisées dans des arrêtés sectoriels publiés en 2016 et 2017 et au niveau Européen par l'adoption de la directive NIS (sécurité des réseaux et des systèmes d'information) en 2016 et sa transposition au niveau national en 2018.
Une importante activité de normalisation est en cours pour traiter de ce sujet mais les normes ne sont pas encore stabilisées et plusieurs référentiels concurrents existent. Les méthodes d'analyse à mettre en œuvre et les moyens de protection contre les attaques demeurent mal connus et paraissent couteux ou contraignants pour l'exploitation. En conséquence, la progression de la protection des systèmes industriels pour les industries non OIV progresse lentement.

1 Quelles sont les limites d'un système de contrôle industriel ?

La notion de Système de Contrôle Industriel est large et peut inclure différents types d'éléments plus ou moins ouverts allant du contrôle physique d'un équipement local jusqu'au système d'information de l'entreprise. De manière générale, un Système de Contrôle Industriel peut être défini comme tout système « numérique » permettant d'avoir une action directe dans le monde « physique ». Les acronymes ICS (Industrial Control System) ou IACS (Industrial Automation and Control System) sont parfois utilisés pour les identifier.

La pyramide CIM est une représentation conceptuelle représentant ces systèmes selon une hiérarchie logique organisée en 5 niveaux (figure 1) :
- Le niveau 0 correspond aux interactions entre le système de contrôle industriel et le procédé physique. Il s'agit des capteurs et des actionneurs.
- Le niveau 1 correspond aux différents systèmes de contrôle commande permettant de faire l'acquisition des mesures physiques du niveau 0 et de commander les actionneurs. On trouve à ce niveau des automates programmables industriels, des PC industriels ou encore des automates de sécurité. Ils communiquent avec le Niveau 0 par des liaisons analogiques ou numériques filaires, plus rarement sans fil.
- Le niveau 2 correspond aux systèmes de supervision de l'installation (écrans de contrôle, interfaces opérateurs, acquisition et enregistrement de données) de type SCADA (System Control and Data Acquisition) qui permettent d'envoyer des ordres aux automates par des protocoles de communication spécifiques tels que OPC.
- Le niveau 3 correspond à la gestion de la production avec des fonctions de gestion des ressources, ordonnancement de production, planification de la maintenance, etc. Il s'agit de systèmes de type MES (Manufacturing Execution System) il communique avec le niveau 2 par des réseaux ethernet
- Le niveau 4 correspond au système de gestion de l'entreprise ERP qui est très intégré aux systèmes d'information de l'entreprise (I.E. au réseau bureautique). Il communique avec le niveau 3 via des liaisons ethernet.
Les niveaux 3 et 4 peuvent être physiquement distants des sites de production et donc impliquer des communications du site de production vers l'extérieur.

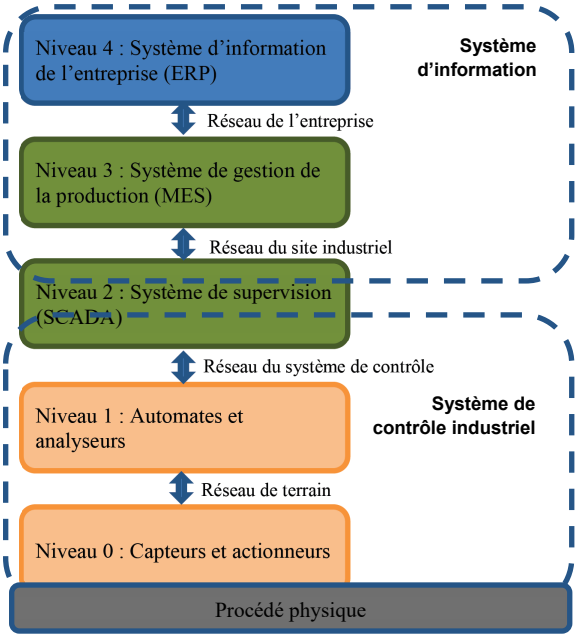


Figure 1. Représentation simplifiée de la pyramide CIM

Chaque niveau du système utilise des briques technologiques - matérielles, logicielles ou réseau - spécifiques. De manière générale, plus on s'élève dans cette pyramide, plus on s'éloigne du procédé physique et des technologies des automatismes industriels agissant sur ce procédé et plus on se rapproche des technologies des systèmes d'information (bureautique) : le niveau 4 est intégré au système d'information de l'entreprise ; les niveaux 2 et 3 sont propres aux systèmes de production mais très intégrés au systèmes d'information ou au minimum utilisant des technologies similaires ; les niveaux 0 et 1 utilisent des technologies de l'automatisme et du contrôle commande industriel.

Cette représentation simplificatrice peut être trompeuse dans la mesure où elle représente mal l'intégration entre les différents niveaux, laisse supposer que chaque niveau du modèle ne communique qu'avec les niveaux directement inférieurs et supérieurs et que seuls les niveaux les plus élevés sont connectés vers l'extérieur de l'entreprise. Dans de nombreux cas, les systèmes de gestion opérationnelle et d'information de l'entreprise peuvent être situés sur des sites distants des systèmes de production, ce qui induit l'utilisation du réseau internet pour communiquer entre ces différents niveaux. Par ailleurs, les systèmes d'information, même situés sur le site de production, disposent le plus souvent d'accès au réseau internet (mails, télémaintenance, etc.).

Afin de différencier le contrôle-commande, qui appartient aux technologies de l'automatisme, des systèmes de gestion qui appartiennent au monde des systèmes d'information, on désignera les premiers comme OT (Operational Technology) et le second comme IT (Information Technology). Les systèmes de supervision, de type SCADA, assurent une interface entre les systèmes OT et les systèmes IT de l'entreprise.

Dans le cadre des analyses et de la maîtrise des risques accidentels, qui fait appel aux méthodes de maîtrise des risques industriels et de sûreté de fonctionnement, on étudie particulièrement les systèmes de niveaux 0 ou 1 qui sont en interaction directe avec le procédé. En effet, une défaillance de ces systèmes peut mener à des scénarios accidentels et ils peuvent également être valorisés comme barrières de sécurité sur ces scénarios. On évalue donc leur fiabilité et disponibilité. Dans ce cadre-là, les systèmes de niveau 2 peuvent également être partiellement étudiés pour leur fonction d'alarmes et d'interfaces opérateurs.

Dans le cadre de la cybersécurité d'une installation industrielle, on étudie les différentes actions délibérées illégitimes visant à dérober ou corrompre des données (paramètres, programmes, informations) à des fins malveillantes. Tous les niveaux de la pyramide CIM sont susceptibles d'être attaqués, éventuellement en tant que voie d'accès aux autres niveaux. Les études de cybersécurité des installations industrielles visent toutefois principalement les niveaux 2 et 3 de la pyramide et de manière moins détaillée le niveau 1. Le niveau 4 est vu comme extérieur au système de contrôle industriel. Il s'agit d'une partie du système auquel on considère que l'attaquant aura toujours accès.

2 L'évolution des vulnérabilités des systèmes industriels

2.1 Les évolutions technologiques

De plus en plus d'équipements intelligents (I.e. Programmables) et communicants sont utilisés dans les installations industrielles, y compris au niveau 0 de la pyramide CIM telle que présentée ci-avant. L'utilisation de ces technologies vise à optimiser le diagnostic, la maintenance et la disponibilité, à améliorer la flexibilité en permettant la programmation ou les mises à jour logicielles à distance, et donc à réduire les coûts. Ces technologies permettent par exemple de décentraliser les traitements afin de rendre les systèmes plus résilients et adaptables ou encore de centraliser la collecte de données sur un équipement ou une installation afin d'améliorer la connaissance, d'optimiser la production.
Par ailleurs, ces technologies pour les capteurs et actionneurs sont souvent liées au remplacement des communications analogiques point à point par des réseaux de communication numérique (également moins coûteux et plus simples à mettre en œuvre). Pour certaines applications, des protocoles de communication sans fils industriels sont également utilisés.
Enfin, les briques technologiques utilisées dans les niveaux 0 et 1 de la pyramide CIM sont de plus en plus issus du domaine de l'IT. 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.

2.2 L'évolution des architectures

De nouvelles fonctions de collecte et traitement des informations sont de plus en plus intégrées aux systèmes de contrôle industriels. L'objectif est d'améliorer la productivité par exemple en :

- obtenant un accès en temps réel aux données depuis des sites distants ;
- sous-traitant des fonctions de maintenance ou d'ingénierie nécessitant de donner des accès (physique ou à distance) à des prestataires extérieurs ou à des fournisseurs de matériels disposants d'outils de maintenance informatisés ou de consoles de programmation, etc ;
- utilisant des équipements mobiles (maintenance, TMD, outils de maintenance) disposant de connexions sans-fils ;

Par ailleurs, certaines technologies émergentes (dans la production d'énergie notamment) tendent à décentraliser la production en implantant de petites unités de production communicantes et éventuellement physiquement accessibles.

Ces évolutions de fonctionnalités supposent des modifications des architectures des systèmes d'information industriels. Les systèmes de contrôle commande étaient dans le passé des systèmes fermés utilisant des technologies électromécaniques et des automates programmables industriels. Ces systèmes OT étaient techniquement différents ainsi que physiquement et fonctionnellement indépendants des systèmes d'information de l'entreprise. 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.
Ces évolutions offrent de nouvelles vulnérabilités exploitables par des attaquants potentiels d'une part dues à l'ouverture des systèmes et d'autre part dues à l'utilisation de technologies connues d'un plus grand nombre d'attaquants.

3 L'évolution des menaces pesant sur les systèmes industriels

Depuis l'attaque Stuxnet (2011) qui nécessitait des connaissances très précises sur les technologies utilisées et des ressources très importantes pour ses concepteurs, la population d'attaquants potentiels est plus nombreuse et a une meilleure connaissance des technologies industrielles. En effet :
- les états ont renforcé leurs capacités offensives ;
- les attaquants hors des organismes étatiques ont une meilleure connaissance des technologies utilisées dans l'industrie (qui se rapprochent de l'informatique classique) ;
- des failles de sécurité sur les équipements industriels sont régulièrement publiées ;
- les attaques à motivations lucratives se sont popularisées (rançongiciels).

L'ANSSI propose la classification des attaquants suivante :

Niveau	Qualificatif	Description /exemples
1	Non ciblé	Virus, Robot…
2	Hobbyiste	Personne avec des moyens très limités, pas nécessairement de volonté de nuire.
3	Attaquant isolé	Personne ou organisme avec des moyens limités mais avec une certaine détermination (employé licencié par exemple).
4	Organisation privée	Organisme aux moyens conséquents (terrorisme, concurrence déloyale, par exemple).
5	Organisation étatique	Organisme aux moyens illimités et à la détermination très forte

Table 1. Classification des attaquants selon l'ANSSI

Les attaquants peuvent poursuivre différents types d'objectifs (lucratifs, militaires, activistes, terroristes, ludique, vengeance…).
Les profils et motivations des attaquants sont donc variés. L'analyse des attaquants potentiels permet de définir le niveau de protection souhaitable pour un système ou une installation.
Malgré la création de nombreux groupes de travail plus ou moins ouverts sur le sujet, il est pour l'instant difficile d'obtenir des informations sur des incidents ayant concrètement touché des installations voire exposé les personnes ou l'environnement à des risques physiques. S'il existe des sources fiables sur les vulnérabilités des différents équipements, il n'en est pas de même pour les bases de victimologie. Les industriels sont réticents à communiquer sur les attaques dont ils sont victimes, néanmoins, un certain nombre d'attaques ont été médiatisées ou analysées par des experts en cybersécurité. On peut citer en particulier :
- La désactivation du système de détection de fuite sur un réseau de canalisation de transport de pétrole brut par un employé mécontent (Etats-Unis, 2009) ;
- La prise de contrôle de la commande d'aiguillages d'un tramway en Pologne au moyen d'une télécommande modifiée ;
- L'endommagement de centrifugeuses d'enrichissement en uranium iraniennes, vraisemblablement par une organisation étatique (Stuxnet, 2011) ;
- L'intrusion depuis l'étranger sur le système de commande des vannes d'un barrage écrêteur de crue dans l'état de New-York (Bowman Dam, 2013) ;
- L'endommagement d'une aciérie en Allemagne après dérive non détectée de la température des hauts-fourneaux (2014) ;
- Le piratage de TV5 monde (2014) ;
- La coupure de la distribution électrique dans une partie de l'Ukraine (black energy, 2015) ;
- Le cryptage de données d'hôpitaux aux Etats-Unis et au Royaume-Uni (2016) ;
- Les attaques WannaCrypt et NotPetya qui ont interrompu entre autres le fonctionnement d'hôpitaux, de sites de production, de la télémesure de radioactivité du site de Tchernobyl (mai et juin 2017) ;
- Malware Trisis : découverte d'un malware destiné à la prise de contrôle des automates de sécurité de la gamme Triconex de Schneider Electric (décembre 2017).

Les attaques les plus médiatisées sont en général les attaques ayant nécessité les moyens les plus importants tels que Stuxnet et Blackenergy (de nombreuses ressources humaines et des mois voire années de préparation). Dans ces conditions la menace peut paraitre théorique à un certain nombre d'industriels surtout au regard des investissement nécessaires pour s'en prémunir. Néanmoins, les enjeux commencent à être bien perçus, les moyens à mettre en œuvre selon le type d'installation demeurent difficiles à appréhender.
L'historique des attaques montre une évolution des attaquants et des modes opératoires : Les premières attaques étaient réalisées depuis l'extérieur par des organisations disposant de moyens importants ou depuis l'intérieur par des personnes ayant une bonne connaissance du système. Les plus récentes sont dues à des attaques non ciblées (virus) destinées aux technologies IT et affectant des systèmes de production voire des logiciels malveillants ciblant des technologies industrielles précises et mis à disposition des attaquants.
Des impacts majeurs sur la santé et la sécurité des personnes, à la suite d'attaques à motivations terroristes par exemple, n'ont pour l'heure pas été communiqués. Cependant, les attaques réalisées démontrent la possibilité d'aboutir à de tels effets. Le Malware TRISIS, ciblant des systèmes instrumentés de sécurité, démontre la volonté de causer des dommages humains.

Face aux évolutions des menaces et des vulnérabilités, il semble important, notamment dans l'industrie des procédés chimiques, qui présente des potentiels de dangers importants, d'intégrer les causes cyber-malveillantes à l'étude et à la maîtrise des risques pour les personnes et l'environnement. Des cadres méthodologiques et réglementaires existent pour les risques accidentels d'une part et pour la sécurité des systèmes d'information d'autre part. L'objectif de l'INERIS est de faire un lien entre ces approches afin d'avoir une vision complète des scénarios et de fournir les données nécessaires et cohérentes aux différents acteurs pour maîtriser de manière efficace les deux types de risques.

Démarches de maîtrise des risques existantes

4 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 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 d'exploiter 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. 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.

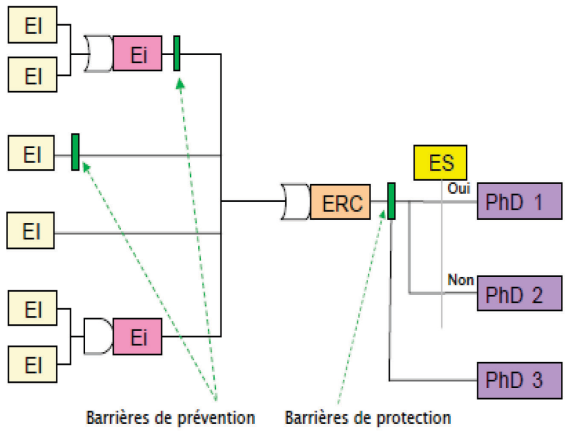
4.1 L'analyse qualitative des risques

Pour l'analyse qualitative, on utilise généralement une démarche telle que l'Analyse Préliminaire des Risques (APR) ou l'HAZOP qui permettent d'identifier les risques de manière exhaustive.
Ainsi l'HAZOP est une démarche d'analyse systématique visant à identifier les risques liés à un procédé. L'HAZOP est conduite par un groupe de travail pluridisciplinaire qui identifie les dérives potentielles des paramètres physiques du procédé et identifie leurs causes éventuelles et conséquences possibles pour la sécurité des personnes, de l'environnement ou des biens.
Pour faciliter l'examen, un système est divisé en plusieurs parties (ou nœuds) de telle sorte que la fonction puisse être définie de manière adéquate pour chacune d'elles.
Pour chacune des parties, l'équipe de l'étude HAZOP vérifie si chaque propriété (PRESSION, DEBIT…) présente un écart qui peut avoir des conséquences non souhaitables. Pour identifier ces écarts elle emploie un système de questions dans lequel interviennent des mots-

guides prédéfinis (NE PAS FAIRE, PLUS, MOINS, INVERSE…).
Le groupe de travail examine par exemple la dérive PLUS DE PRESSION dans le nœud « système de remplissage d'un réacteur chimique », ce nœud comprenant des tuyauteries, pomperies, vannes et instrumentation. On cherchera à déterminer les causes de cette dérive (fermeture d'une vanne en aval d'un compresseur), les conséquences (éclatement de la tuyauterie et perte de confinement d'une substance inflammable) et les mesures de maîtrise des risques éventuelles (fonction de sécurité sur pression haute, fin de course sur les vannes, soupape…).
L'intérêt de l'HAZOP est qu'il s'agit d'un processus créatif qui passe en revue de manière systématique les dérives d'un procédé.
Dans le cadre d'une analyse de cybersécurité, le groupe de travail pourrait envisager les causes malveillantes menant à la dérive (commande illégitime de la vanne en aval du compresseur via l'automate de contrôle commande, désactivation des fonctions instrumentées de sécurité pression haute et fin de course de la vanne). Le format de l'HAZOP telle qu'elle est pratiquée n'est toutefois pas prévu pour cet usage. De plus, l'HAZOP ne permet pas d'étudier des variations de plusieurs paramètres simultanément.

4.2 L'étude détaillée des risques

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 2 donne un exemple de représentation d'un scénario sous forme de nœud papillon.
Le nœud papillon sert de support à l'évaluation probabiliste des risques. Les principales données d'entrée de cette évaluation sont les fréquences et durée des évènements initiateurs, tirées de bases de données d'accidentologie ou d'hypothèses d'exploitation, les probabilités moyennes de défaillance à la demande (PFD_{avg}), des de sécurité, évaluées à partir d'une étude de sûreté de fonctionnement ou d'approches semi-quantitatives, et les probabilités conditionnelles des évènements secondaires (par exemple, probabilités d'inflammation). Les modèles de calculs appliqués aux arbres des causes et arbre d'évènements composant le nœud papillon permettent de calculer des Probabilités d'Occurrence Annuelles moyennes (POA) des évènements redoutés centraux et des phénomènes dangereux. Le calcul de la probabilité d'occurrence d'un scénario (intégrant éventuellement plusieurs causes aléatoires concomitantes et les défaillances de plusieurs barrières) repose sur des hypothèses d'indépendance entre les différents évènements. Cette hypothèse ne serait pas valable dans l'analyse d'un scénario d'origine malveillante car l'objectif de l'attaquant serait justement de provoquer des évènements concomitants et de contourner ou désactiver les barrières.
Par ailleurs la cinétique, l'intensité et la gravité des phénomènes dangereux sont évaluées selon des scénarios supposés majorants (conditions initiales de pression, température, quantité de substance dangereuse… au moment de la perte de confinement). Un attaquant pourrait cependant sortir de ces scénarios enveloppes en provoquant plusieurs scénarios simultanément ou en activant plusieurs causes du scénario par exemple.



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.

Figure 2. Modèle de représentation de scénarios d'accident sous forme de Nœud papillon

4.3 L'évaluation des mesures de maîtrise des risques

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 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).
Les différentes barrières de sécurité sont valorisées dans les nœuds papillon au travers de réduction qu'elles apportent à la probabilité des scénarios d'accidents majeurs en considérant que leur fonctionnement est indépendant du scénario, c'est-à-dire que la défaillance d'une barrière n'est pas provoquée par le scénario en lui-même.

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 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 d'origine accidentelle sur les personnes et l'environnement).

5 La cybersécurité des installations industrielles

5.1 Maîtrise de la cybersécurité pour les OIV

La cybersécurité des installations industrielles fait l'objet d'une importante activité de réglementation, de

publications 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).
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 » et « mesures détaillées » 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.

Ces étapes sont couvertes par la majorité des méthodes de maîtrise des risques sur la sécurité des systèmes d'information.
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 risque 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 présentée plus loin par exemple.
La figure 3 ci-dessous, tirée du guide ANSSI, présente les critères de classification.

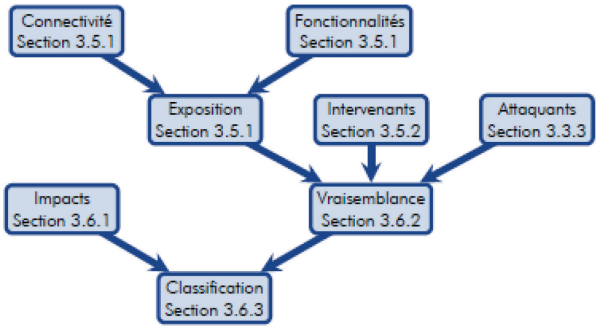


Figure 3. Schéma représentant la méthode de classification

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, 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-dessous (fig. 3) tirée du guide ANSSI permet de classer les systèmes en fonction des Impacts et de la Vraisemblance de leur attaque.

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+

Figure 4. Matrice Impact/Vraisemblance

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 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.

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).

5.2 La méthode EBIOS

La méthode EBIOS® (Expression des Besoins et Identification des Objectifs de Sécurité) est un cadre global d'analyse des risques cyber appliqués principalement en France et permettant de couvrir globalement la maitrise de la cybersécurité. Cette méthode est applicable à tout type de système d'information, qu'il s'agisse d'un système de contrôle industriel ou d'un site internet. Cette méthode n'est pas spécifiquement destinée aux OIV. Le cadre général de la méthode est présenté par la figure 5 ci-après.

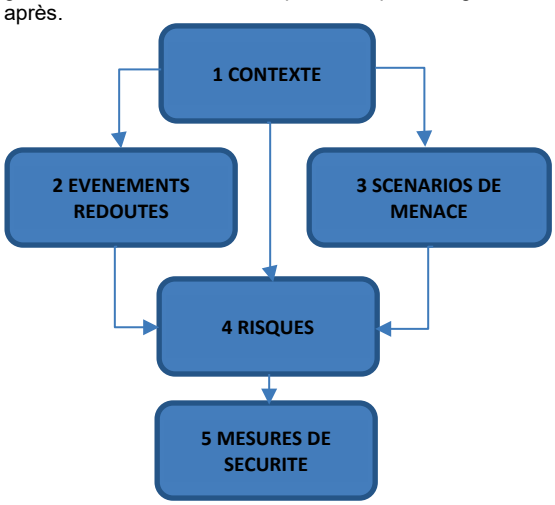


Figure 3. Schéma synthétique de la méthode EBIOS

C'est une méthode qui s'applique à tout type de système d'information, qu'il s'agisse d'un système industriel ou non. C'est une méthode itérative, chaque étape pouvant être reprise plusieurs fois afin d'en affiner et préciser le contenu en fonction des sorties des autres étapes. Chacune des étapes est découpée en plusieurs activités.
La première étape consiste en l'identification du périmètre de gestion des risques. On cherchera à cartographier les systèmes d'information ou de contrôle industriel, à identifier les fonctions essentielles qu'ils assurent et les biens supports de ces fonctions, c'est-à-dire les systèmes et équipements nécessaires pour réaliser ces fonctions. Les activités de cette étape sont :

- Activité 1.1 – Définir le cadre de la gestion des risques
- Activité 1.2 – Préparer les métriques
- Activité 1.3 – Identifier les biens

La deuxième étape consiste en l'appréciation des risques. On cherche à évaluer les besoins en sécurité des fonctions essentielles (disponibilité, intégrité, confidentialité, traçabilité…) ainsi que les l'impacts en cas de non-respect de ces besoins (financiers, juridiques, concurrentiels, humains…). L'expression des besoins repose sur l'élaboration et l'utilisation d'une échelle de besoins et la mise en évidence des impacts inacceptables pour l'organisme. Cette étape comprend une activité :

- Activité 2.1 – Apprécier les événements redoutés

Lors de la 3ème étape, les scénarios pouvant porter atteinte aux éléments du SI sont étudiés. Pour se faire on étudie les origines des menaces et les vulnérabilités afin de formaliser les menaces. Cette étape comprend une activité :

- Activité 3.1 – Apprécier les scénarios de menaces

La quatrième étape consiste en l'identification des risques pesant sur l'organisme en confrontant les événements redoutés aux scénarios de menaces. Il s'agit également d'estimer et évaluer ces risques, et enfin d'identifier les objectifs de sécurité à atteindre pour les traiter. Les activités de cette étape sont :

- Activité 4.1 – Apprécier les risques
- Activité 4.2 – Identifier les objectifs de sécurité

La cinquième étape porte sur le traitement des risques. Elle consiste à spécifier les mesures de sécurité à mettre en œuvre, planifier la mise en œuvre de ces mesures et valider le traitement des risques et les risques résiduels. Les activités de cette étape sont :

- Activité 5.1 – Formaliser les mesures de sécurité à mettre en œuvre
- Activité 5.2 – Mettre en œuvre les mesures de sécurité

D'autres démarches d'analyse et maîtrise de la sécurité des systèmes d'information existent (Mehari, Octave, cyber Kill Chain…). De manière générale concernant les risques d'origine malveillante, les méthodes d'analyse doivent identifier les éléments suivants :

- La cible : Quels objectifs peuvent être visés par des attaquants ?
- Les attaquants : Quels types d'attaquants peuvent viser ces objectifs ? Quels sont leur niveaux et ressources ?
- Les vulnérabilités : Quels seront les moyens d'action des attaquants ?

En fonction de ces informations, des mesures visant à anticiper les risques, protéger les systèmes et réagir en cas d'attaque pourront être définis.

Démarche d'analyse des risques intégrant les causes accidentelles et malveillantes

6 Objectifs et contraintes

On cherche à définir une méthodologie d'analyse des risques majeurs pour les personnes et l'environnement intégrant les cyberattaques comme évènements initiateurs et permettant de :

1. Identifier les risques : lister de manière la plus exhaustive possible les risques pour les personnes et l'environnement et les coter en gravité
2. Analyser les risques : identifier les scénarios d'attaques menant aux risques identifiés et les coter en probabilité ou vraisemblance
3. Evaluer les risques : statuer sur l'acceptabilité du risque

Cette méthodologie doit s'appliquer aux procédés industriels et à leurs systèmes de contrôle et être, autant que possible, cohérente avec le cadre général d'analyse des risques utilisé pour les installations classées.Plusieurs difficultés peuvent mettre en cause l'application de la méthode :

- le type d'attaquants et leurs motivations sont variables ;
- les moyens d'attaques ne sont pas connus : on ne sait pas par avance quels systèmes sont le plus susceptibles d'être attaqués et les procédés d'attaques sont variables ;
- les attaquants chercheront – dans la mesure de leur compétence – à contourner les sécurités existantes ;
- évaluer la probabilité d'une attaque n'a pas vraiment de sens ;
- la complexité du système rend difficile l'analyse exhaustive des scénarios d'attaques.

On définit donc une méthodologie d'analyse centrée sur les cibles : connaissant l'effet potentiel atteignable pour les attaquants, on identifiera les systèmes mis en jeu et les comportements de ces systèmes que l'attaquant cherchera à obtenir pour atteindre ces objectifs, sans évaluer à ce niveau les moyens d'attaque utilisés.
Une telle analyse nécessite des compétences sur les procédés physiques et les risques associés et également des compétences précises sur la maîtrise de la cybersécurité qui ne sont généralement pas intégrées aux groupes de travail réalisant les HAZOP ou les APR. Le cadre méthodologique fera donc intervenir différents groupes de travail dans les différentes phases d'analyse :

- le groupe de travail chargé de l'évaluation des risques physiques du procédé, chargé par ailleurs des analyses de types HAZOP ou APR ;
- le groupe de travail chargé de l'analyse de la cyber sécurité du système de contrôle industriel.

7 Mise en œuvre de la méthode

La figure 4 ci-dessous montre les interactions entre les processus d'analyse des risques physiques et cyber.

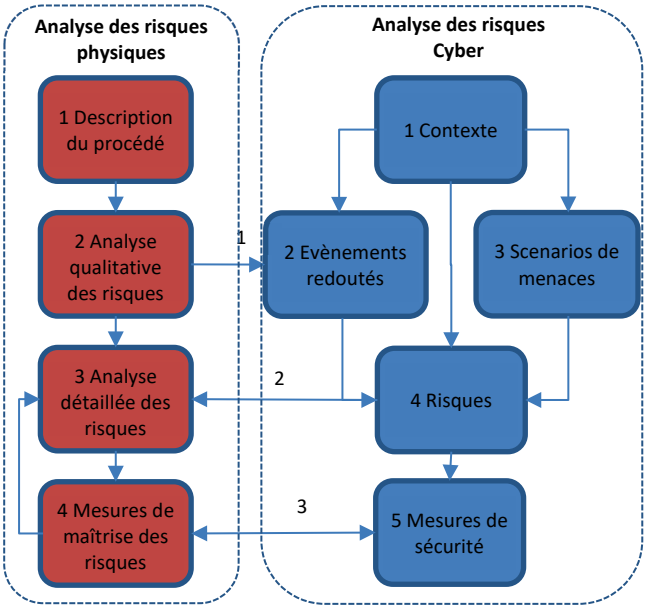


Figure 4. Interactions entre analyse des risques physiques et cyber

Différentes informations doivent être échangées entre les deux groupes de travail :
(1) Le groupe de travail sur les risques physiques identifiera les scénarios et éléments de bas niveau de la pyramide CIM permettant de provoquer des dommages aux personnes ou à l'environnement. Ces données de sorties seront fournies au groupe de travail chargé d'évaluer la cybersécurité du système industriel et seront intégrées à leurs analyses comme évènements redoutés. Ce groupe de travail identifiera ensuite les scénarios d'attaques, les différents biens supports de la pyramide CIM mis en œuvre, les mesures de sécurité existantes ou à mettre en œuvre et le niveau de risque résiduel (vraisemblance de l'attaque). Ce groupe de travail appliquera donc la méthode d'analyse des risques cyber utilisée de manière générale par l'organisation aux scénarios de risques majeurs pour les personnes et l'environnement (méthode EBIOS par exemple).
(2) La vraisemblance de l'attaque sera ensuite intégrée à un modèle de nœud papillon intégrant les causes aléatoires et malveillantes.
(3) Enfin les exigences sur les mesures de maîtrise des risques et mesures de sécurité permettant d'atteindre un niveau de risque acceptable seront spécifiées et mise en œuvre.

Le processus d'analyse des risques cyber est similaire à la méthode EBIOS présentée précédemment avec un intérêt particulier porté aux évènements redoutés issus de l'analyse des risques physiques. Elle n'est donc pas présentée de manière plus détaillée dans cet article.
La prise en compte des évènements relatifs à la cybersécurité dans les différentes étapes de l'analyse des risques physiques est présentée ci-après.

8 Analyse des risques physiques intégrant la cybersécurité

8.1 Analyse qualitative des risques

L'intégration de cyberattaques comme évènements initiateurs des accidents majeurs dans les analyses de risques n'est pas évidente : en effet, de multiples chemins d'attaques sur des systèmes très variés peuvent être à l'origine des scénarios redoutés. De plus, un scénario d'attaque reposera la plupart du remps sur la corruption de plusieurs systèmes simultanément.
La réalisation d'une analyse inductive, de type AMDEC partant des différents types de corruption possibles de chaque équipement du système de contrôle industriel et identifiant leurs conséquences ainsi que les conséquences de la combinaison de corruptions concomitantes de plusieurs équipements s'avère irréaliste. 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. On cherche donc à enrichir le processus créatif, tel qu'il est organisé par les méthodes APR et HAZOP en ajoutant la recherche de causes malveillantes. Pour ce faire, le groupe de travail réalisant l'analyse accidentelle devra disposer d'une description des différents systèmes de contrôle commande de niveau 0 et 1 de la pyramide CIM en interaction avec le procédé étudié. Lors de la recherche des causes des différentes dérives (pour l'HAZOP) ou des différents évènements redoutés (pour l'APR) on cherchera à identifier les corruptions de données, les modifications de consignes ou de logique de commande ou les actions intempestives d'actionneurs pouvant amener à ces évènements.

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, compresseurs, systèmes de chauffe et de refroidissement ;
- B : dispersion de substance dangereuse par débordement d'une capacité ou ouverture d'organes de vidange ;
- 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 la dispersion l'épandage, pour chaque produit :
  - B1- Identification des risques liés à un épandage malveillant ;
  - B2- identification des moyens (actionneurs) permettant de réaliser cet épandage ;
  - 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 (actionneurs) 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 (régulation de pression, inertage, régulation de température) ;
  - D2- identification des moyens de les corrompre ou de les arrêter ;
  - D3- Identification des moyens de détection et des barrières de sécurité intervenant sur les scénarios dont les barrières instrumentées.

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.

8.2 Etude détaillée des risques

L'analyse détaillée des risques se base sur le formalisme des diagrammes de nœuds papillon présenté précédemment. L'analyse détaillée des risques pourrait servir de point d'entrée à l'intégration de la cybersécurité au processus d'analyse des risques : à partir des évènements redoutés centraux et des nœuds papillon développés lors de l'analyse des risques accidentels, on pourrait identifier les évènements initiateurs, les évènements secondaires et les défaillances de barrières susceptibles d'être provoqués par une cyber-attaque. Dans la méthodologie présentée ici, il a été choisi de compléter ces scénarios par des scénarios supplémentaires issus de l'analyse qualitative des risques intégrant la cybersécurité.
Pour intégrer les cyberattaques aux nœuds papillon, Abdo, et al., propose une méthode, dite ATBT (Attack Tree Bow Tie), combinant les nœuds-papillon et des arbres d'attaques permettant d'identifier des causes malveillantes aux scénarios décrits dans les analyses de risques classiques. Cette représentation permet de lier les risques liés à la sécurité (malveillance) et les risques liés à la sûreté (accidentels).

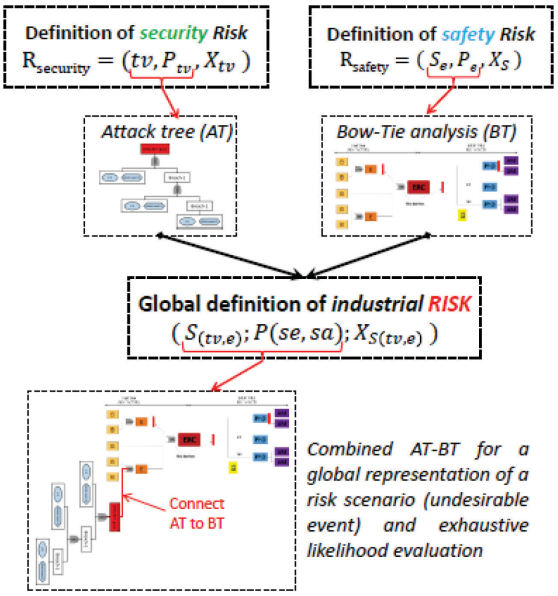


Figure 5. Présentation générale du modèle ATBT selon Abdo et al.

Les risques liés à la sécurité sont décrits par :
tv représentant une menace ou attaque *t* (threat) exploitant une vulnérabilité *v (description du scénario d'attaque) ;*
P_{tv} la vraisemblance que la menace *t* exploite la vulnérabilité *v ;*
X_{tv}, la gravité des conséquences si *t* exploite la vulnérabilité *v.*
Les scénarios d'attaque peuvent être représentés par des arbres d'attaques représentant les différentes vulnérabilités exploitées par un attaquant pour produire l'effet recherché sur le système physique (c'est-à-dire les différents systèmes informatiques à corrompre pour manœuvrer une vanne par exemple). Ces modèles sont issus de l'analyse des risques cyber qui a développé les scénarios d'attaques des éléments du système de contrôle industriel identifiés lors de la phase d'analyse qualitative des risques.
Les risques liés à la sûreté sont décrits par :

- S_e, le scénario représentant l'évènement indésirable *e*, ses causes et ses conséquences
- P_e la probabilité d'occurrence de S_e ;
- X_e, la gravité des conséquences si *t* exploite la vulnérabilité S_e.

L'ensemble de ces scénarios sont intégrés dans des nœuds papillon dans le cadre de l'analyse des risques physiques.
Les arbres d'attaques sont ensuite connectés aux nœuds papillon pour les évènements initiateurs, intermédiaires ou barrières pouvant être causés par une action malveillante.
L'exploitation du modèle ATBT consiste à identifier tous les scénarios menant à des évènements indésirables, c'est-à-dire les coupes minimales composés d'évènements incidentels et d'actions malveillantes menant à un évènement indésirable, et à évaluer le risque global selon les paramètres suivants :

- $S_{(tv,e)}$, la description du scénario pouvant résulter d'une combinaison incidents et d'actes malveillants ;
- $P_{(se, sa)}$ qui est la vraisemblance de l'occurrence du scénario $S_{(tv,e)}$ avec *se* la vraisemblance liée à la réalisation des actes malveillants et *sa* la probabilité d'occurrence des évènements incidentels ;
- $X_{(tv, e)}$, la gravité des conséquences de $S_{(tv,e)}$.

La possibilité d'occurrence des différents scénarios est donc cotée selon un vecteur à 2 dimensions : la probabilité (évènements aléatoires) et la vraisemblance (de la réalisation d'une attaque). Chaque scénario est évalué indépendamment, trois types de scénarios sont possibles :

- des scénarios purement incidentels caractérisés uniquement par une probabilité ;
- des scénarios purement malveillants caractérisés par une vraisemblance ;
- des scénarios dus à l'occurrence simultanés d'attaques et d'évènements incidentels caractérisés par une probabilité et une vraisemblance : cela représente la probabilité que les phénomènes dangereux atteignent leur cible sachant que l'attaque du système de contrôle commande a été réalisée avec succès.

On pourrait considérer 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. Cependant, le propre d'une cyberattaque étant de pouvoir être réalisée simultanément sur un grand nombre de systèmes similaires, on pourrait considérer qu'un attaquant maximiserait ses probabilités de succès en réalisant plusieurs attaques simultanément. (Exemple : si la montée en pression dans une capacité équipée d'une soupape a 1 chance sur 100 d'aboutir à l'éclatement de la capacité (probabilité de défaillance de la soupape), la montée en pression dans 10 réservoirs a une chance sur 10 d'aboutir à l'éclatement d'au moins un réservoir). Une échelle d'acceptabilité des risques combinant les deux dimensions doit donc être définie.

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.

8.3 Exploitation des résultats

Définition des exigences de conception et mesures de sécurité

Les exigences issues des analyses de risques accidentels et des études de cybersécurité peuvent être fonctionnellement dépendantes, antagonistes, se renforcer mutuellement ou être indépendantes. L'un des objectifs de la méthodologie est d'avoir un cadre général permettant de traiter ces exigences de manière cohérente.

Par exemple, 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. On peut valoriser ces dispositifs pour évaluer la probabilité de réussite de scénarios d'attaques et dimensionner les besoins de sécurité informatique. Il faut néanmoins prendre en compte les scénarios résiduels résultant de l'activation de ces barrières.

Les bonnes pratiques relatives à la cybersécurité des systèmes de contrôle-commande resteront nécessaires mais l'analyse des risques aidera à identifier les parties du système de contrôle commande devant être plus spécifiquement protégées, les types d'attaques à considérer (interne/ externe, ciblée/ non ciblée) et éventuellement la conduite à tenir lorsqu'une nouvelle vulnérabilité sera identifiée. Des critères de performance des mesures de sécurité, permettant d'évaluer leur impact sur la vraisemblance de l'occurrence d'attaques réussies 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.

Modélisation des phénomènes dangereux

Les modélisations de l'intensité des phénomènes dangereux et l'évaluation de leur gravité devraient être réalisées en prenant en compte les hypothèses de réalisation des cyberattaques. Les conditions initiales du phénomène et l'hypothèse de fonctionnement de certaines barrières, notamment d'atténuation peuvent être remises en causes pour un scénario malveillant.

Conclusion

La méthodologie proposée permet d'intégrer la cybersécurité aux analyses de risques physiques et de compléter les scénarios menant à des effets dangereux pour les personnes ou l'environnement. Suite à l'identification des scénarios une étude détaillée de la vraisemblance (malveillance), probabilité (accidentelle) et gravité peut être réalisée pour chacun d'entre eux. Cette approche détaillée permet de mettre en évidence les systèmes critiques pour lesquels une protection, une surveillance et des procédures de maintien dans le temps sont nécessaires, de paramétrer des systèmes de détection d'attaque, ou de mettre en œuvre des barrières de sécurité non informatiques et qui agissent tant sur les effets physiques des attaques que sur les phénomènes accidentels.

À l'avenir, ce travail sera complété en précisant certaines parties de l'analyse dont en particulier :

- La manière dont est définie la vraisemblance des scénarios malveillants et les critères pris en compte dans l'évaluation de la vraisemblance. Une échelle de vraisemblance et des grilles d'acceptabilité pourront être définies.
- L'évolution dans le temps de la menace et des vulnérabilités devra également être prise en compte afin d'obtenir des évaluations du risque stables dans le temps et de mettre en œuvre des moyens (techniques, organisationnels…) pour maintenir le risque à un niveau acceptable.

Une réflexion devra être menée sur la conduite des analyses de risques : ces analyses qui sont menées par des équipes pluridisciplinaires (services HSE, production, maintenance…) devront intégrer de nouvelles compétences sur les parties informatiques.

Références

H. Abdo, J-M. Flaus et F. Masse. Towards a better industrial risk analysis: A new approach that combines cyber security within safety. In Safety and Reliability Theory and Applications: Proceedings of ESREL (Portoroz, Slovenia), pages 179–187, 2017.

H. Abdo, M. Kaouk, J.-M. Flaus, F. Masse. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie - combining new version of attack tree with bowtie analysis, In Computers & Security, Volume 72, 2018, Pages 175-195, ISSN 0167-4048.

S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, Y. Halgand, A survey of approaches combining safety and security for industrial control systems, In Reliability Engineering & System Safety, Volume 139, 2015

F. Masse, H. Abdo, J-M. Flaus. Vers une approche intégrant les exigences de cybersécurité à la maîtrise des risques d'accidents majeurs pour les ICPE). In 12ème Congrès International Pluridisciplinaire en Qualité, Sûreté de fonctionnement et Développement durable, Bourges, France 2017