# Transitions et analyses de risques : défis et perspectives

Jean-Christophe Le Coze, Agnès Vallee, Emmanuel Plot, Marine Boutillon, François Masse, Chabane Mazri, Thomas Marcon

# Transitions et analyses de risques : défis et perspectives

Jean-Christophe Le Coze
*Direction des Risques Accidentels*

*Ineris*
Verneuil en Halatte, France
jean-christophe.lecoze@ineris.fr

Marine Boutillon

*Direction des Risques Accidentels*

*Ineris*
Verneuil en Halatte, France

Marine.boutillon@ineris.fr

Thomas Macron
*Direction des Risques Accidentels*

*Ineris*
Verneuil en Halatte, France
thomas.macron@ineris.fr

Agnès Vallée
*Direction des Risques Accidentels*

*Ineris*
Verneuil en Halatte, France
agnes.vallee @ineris.fr

François Masse
*Direction des Risques Accidentels*

*Ineris*
Verneuil en Halatte, France
francois.masse@ineris.fr

Emmanuel Plot
*Direction des Risques Accidentels*

*Ineris*
Verneuil en Halatte, France
emmanuel.plot@ineris.fr

Chabane Mazri
*Direction des Risques Accidentels*

*Ineris*
Verneuil en Halatte, France
chabane.mazri@ineris.fr

***Résumé*—**Cet article explore les implications des mutations actuelles sur la pratique et l'usage des analyses de risques (AR). Il introduit les dernières évolutions des AR dans le domaine des ICPE et introduit la question des limites des AR. Ensuite, plusieurs thèmes et travaux associés menés à l'Ineris depuis quelques années sont présentés. Ils concernent la cybersécurité, les natech (catastrophes naturelles ayant des effets sur les installations à risques), le management numérique de la sécurité, les conséquences environnementales et les effets domino. Considérés ensemble, ces thèmes constituent des évolutions notables dont les implications pour la pratique et l'usage des AR sont discutées.

***Mots clés—analyse de risques, transition, cybersécurité, natech, management numérique, conséquences environnementales, effets dominos***

## I. Introduction

L'analyse de risque est au cœur du processus de gestion des risques et fait l'objet de questionnements méthodologiques, réflexifs ou critiques depuis de nombreuses années. Ces questionnements interrogent les fondements, la pratique et les usages des analyses de risques [1]. Du côté des sciences pour l'ingénieur, les fondements de l'analyse de risques reposent sur une connaissance des phénomènes, des installations et des activités qui s'y déroulent pour évaluer, quantifier, anticiper et prévenir des événements catastrophiques. La pratique correspond à l'animation d'un groupe de travail qui procède à l'identification des scénarios à prévenir, qui font ensuite l'objet de modélisation pour déterminer des effets. Les usages se définissent comme le passage des résultats de ces analyses en matière de conception, de procédures et d'activités vers leur mise en œuvre concrète dans la réalité. Cette vision méthodologique ingénieure est complétée par des questionnements réflexifs et parfois plus critiques sur les fondements, pratiques et usages de l'analyse de risque par les sciences humaines et sociales. Puisant dans des travaux sur les sciences et technologies, de nombreux auteurs soulignent le caractère subjectif, construit et historiquement situé de l'analyse de risque par opposition à une vision qui serait objective et purement rationnelle, détaché des contingences situationnelles. Ces connaissances méthodologiques, réflexives et critiques sont particulièrement importantes dans un contexte de transitions.

En ce qui concerne les installations classées pour la protection de l'environnement (ICPE), l'exercice d'analyse de risque est cadré par une réglementation qui requiert des exploitants la production d'une étude de danger. L'accident d'AZF (2001) a contribué à faire évoluer la réglementation (loi Bachelot de 2003 intégrant la probabilité et la prise en compte plus forte des territoires et de leurs enjeux au travers de dispositifs de concertation) et a donné lieu à de nombreux travaux sur les fondements, les usages et les pratiques des analyses de risques dans les années qui ont suivi [2]. Un certain nombre d'éléments ont notamment été synthétisés dans la circulaire du 10 mai 2010. Depuis une dizaine d'année, il y a eu peu d'évolutions ou de remises en question de ces évolutions post-AZF. Or, les analyses de risques sont confrontées à un nouveau contexte de mutations profondes de l'industrie et de son environnement, non plus cette fois réglementaire, mais, comme indiqué dans le thème de la conférence, digitales et environnementales mais aussi sociétales (comme l'événement de Lubrizol l'a montré, sur les effets domino et conséquences sanitaires d'événements accidentels). Ces mutations tendent à faire évoluer les menaces, les vulnérabilités, les attentes et les objectifs de la gestion des risques. L'objectif de cette communication est de

présenter comment faire évoluer les fondements, pratiques et usages de l'analyse de risques dans ce nouveau contexte.

Dans une première partie, les travaux critiques portant sur l'analyse de risques sont introduits afin de penser les limites de l'analyse de risques avec l'éclairage des sciences humaines et sociales. Cet éclairage permet ensuite d'introduire dans une deuxième partie un ensemble de travaux qui cherchent à faire évoluer l'analyse de risque face aux transitions en cours. Dans une troisième partie, une discussion est proposée.

## II. REGARD SUR L'ANALYSE DE RISQUE

### *A. Les limites des analyses de risques*

Depuis quelques années, les sciences sociales et la philosophie nous expliquent que l'analyse de risque (AR) n'est pas une pratique objective, mais bien plutôt une construction dont les limites sont intrinsèques [3]. L'AR dépend en effet des connaissances disponibles, des modèles utilisés, des choix sur les paramètres, des expertises mobilisées lors de l'identification des scénarios, etc. Nous sommes familiers de cette réalité car nous savons par expérience ou avons entendu que deux experts qui travailleraient sur une même étude arriveraient à des résultats différents, par exemple en matière de scénarios et de probabilités d'événements.

Dans le domaine nucléaire, les premiers calculs probabilistes dans les années 1970 ont ainsi été contestés sur de nombreux points, comme la pertinence et fiabilité des données utilisées pour les calculs mais également la possibilité de pouvoir identifier puis combiner tous les événements potentiels pour arriver à une estimation globale valide [4]. Pourtant, cette affirmation que l'AR est construite et non purement objective, parfaitement admise d'un point de vue des recherches, est régulièrement source de crispations. Après Fukushima par exemple, un ensemble de rhétoriques ont été déployées pour tenter de préserver la part de rationalité de l'AR [5].

Tout d'abord si l'accident a eu lieu, c'est dit-on, parce que l'événement était en dehors du dimensionnement prévu par les AR. Si on avait retenu 10 m pour la hauteur d'un mur et que la vague en faisait 20, on est bien en dehors de ce qui était admis comme pertinent, et on ajoute que les dégâts auraient par ailleurs être beaucoup plus importants sans l'AR. Ensuite, si l'accident est survenu, c'est parce que les ingénieurs qui ont fait les calculs se sont trompés, et que leurs erreurs ne sont pas représentatives de l'industrie, dont les standards sont plus exigeants que ceux constatés dans le cas de cet accident.

Une autre rhétorique porte sur le manque de conformité de l'entreprise en question (ici Tepco pour la centrale de Fukushima), c'est-à-dire la remise en cause de la validité des calculs non pas intrinsèquement mais parce que les exploitants n'ont pas fait ce qui était attendu d'eux, faussant ainsi les calculs, qui eux restent bien valides. Enfin, dernière rhétorique, si l'accident est bien arrivé, il est en effet important d'en tirer les leçons pour que celui-ci ne se reproduise plus. La conception et les calculs doivent donc intégrer ce retour d'expérience pour être plus à même de se conformer avec la réalité des risques. En d'autres termes, l'AR s'améliore.

Ces quatre rhétoriques contribuent à atténuer la critique qui consiste à dire que les AR ne sont pas objectives. Or, pour chacune d'entre elles, c'est bien d'une remise en cause dont il s'agit et dont la portée mérite d'être pesée. Reprenons-les, une par une. Un scénario hors dimensionnement de ce qui était prévu est bien une preuve des limites puisque cela revient à admettre que l'AR n'a pas tenu compte, pour diverses raisons, de cette possibilité. La démarche n'est donc pas objective, et contient une part de subjectivité.

Des erreurs de calcul par les ingénieurs qui seraient dans leur pratique non représentatifs de la profession est une possibilité, mais le Japon était jusqu'alors considéré comme à la pointe (avec des centrales basées sur des conceptions américaines). L'absence de conformité de l'exploitant par rapport à ce qui était prévu tend à protéger l'exercice d'AR mais expose également ses limites. Si l'AR ne prend en compte qu'un idéal qui est irréaliste étant donné les réalités opérationnelles concrètes des systèmes à risque, de telles limites sont donc intrinsèques.

Enfin, si les AR doivent apprendre de leurs échecs, la question reste ouverte de savoir si ce cycle d'apprentissage demeure un cycle sans fin, car l'erreur du passé ne sera probablement pas celle du futur. Mieux protéger la centrale contre un tsunami ne sera d'aucun secours contre la chute d'une météorite ou contre une cyber-attaque.

Des éclairages de Downer à partir de ces 4 rhétoriques, nous pouvons retenir quatre limites des AR : le dimensionnement des scénarios, les limites des calculs de probabilité, la question de la conformité des pratiques aux attendus de l'AR et enfin les scénarios non pris en compte ou retenus (tableau 1).

Tableau 1 : limites AR (à partir de Downer, 2014)

| Limite | Description | Exemple Fuskushima (2011) |
|---|---|---|
| Dimensionnement des scénarios | Evénement identifié mais intensité sous-estimée | La vague est plus haute que prévue en conception |
| Calculs de probabilité | Problème dans les données, dans les formules de calcul | Fréquence du tsunami plus élevée que prévue |
| Conformité des pratiques aux attendus de l'AR | Mesures de prévention et protection mises en œuvre ne correspondent pas dans la réalité à ce qui était prévu par l'AR | Non connaissance par les opérateurs du fonctionnement des mesures de refroidissement du réacteur en cas de coupure d'alimentation électrique |
| Scénario non pris en compte | Evénement inconnu ou dont la probabilité est jugée négligeable | Météorite ou cyber-attaque au-delà du tsunami ? |

Cette mise en perspective de Downer des rhétoriques de défense de l'analyse de risque de l'après Fukushima indique ce que beaucoup d'ingénieurs admettent néanmoins volontiers, et Downer le premier : malgré ces limites, les AR sont incontournables, et permettent de prévenir de nombreux

événements. Travailler sur leurs limites n'est donc pas un exercice seulement critique, mais aussi constructif. Ce travail pointe là où des améliorations pourraient être attendues, en ce qui concerne par exemple la visibilité de ces limites pour la société civile, ou encore la dynamique d'évolution des AR.

### *B. Les limites dans le contexte actuel*

Un exemple de cette confrontation de l'AR aux limites est l'incendie de l'usine Lubrizol et des dépôts de Logistique Normandie en septembre 2019 à Rouen. Où se situent, dans ce cas, les limites de l'AR ? Il est difficile de le dire sans un retour d'expérience approfondi, mais sont-elles dans l'absence ou la superficialité de prise en compte des effets domino ? Dans l'absence de considération pour l'exposition aux menaces d'intrusions et de malveillance ? Dans les limites de fonctionnement des sprinklers par rapport à des feux d'une cinétique inattendue ? Dans le fait que l'exploitant n'a pas suivi les règles qui étaient prévues ?

Au-delà de Lubrizol, les mutations actuelles, au cœur du colloque, telles que le changement climatique ou encore la digitalisation des entreprises ne révèlent-elles pas de nouveaux espaces de problèmes qui redéfinissent les contours de l'exercice ? Les « natech » (conséquences des catastrophes naturelles sur les installations à risques), la cybersécurité ? Quelles sont les conséquences d'une interrogation comme celle-ci sur l'AR pour les ingénieurs? Comment mieux intégrer cette critique, qui revient, finalement, à traiter des AR comme des exercices dont les limites sont en effet plus que jamais questionnées dans un contexte en mutation? L'expérience de l'Ineris dans ce domaine est présentée.

## III. NOUVEAUX DÉFIS

Plusieurs axes de travail sont en effet actuellement développés, et une réflexion à l'intersection de ces différents axes est devenue nécessaire du fait du caractère systémique de leur combinaison. Une présentation succincte des champs est dans un premier temps proposé. Le premier concerne la digitalisation et est envisagé sous au moins deux angles. Le premier concerne la thématique de la cybersécurité, et le deuxième le thème du management numérique de la sécurité. Le second champ est celui des changements climatiques et leur impact sur l'exposition aux risques des sites industriels. Le troisième porte sur les effets dominos et conséquences environnementales.

### *A. Digitalisation et AR*

#### *A.1. Cybersécurité*

Ces dernières années, les systèmes de contrôle commande industriels, qui sont des systèmes informatiques ou électromécaniques ayant une action dans le monde physique ont connu de profondes mutations : ils sont plus numérisés - reposant sur des technologies issues de l'informatique - et plus connectés - entre eux, vers l'extérieur ou vers les systèmes d'information de l'entreprise. De ce fait, la surface d'attaque des systèmes de contrôle industriel tend à augmenter. En parallèle les attaquants aux motivations et moyens variables sont de plus en plus nombreux et compétents. Ceci induit une recrudescence des cyberattaques visant les installations industrielles qui est confirmée par l'étude de l'accidentologie récente (WannaCry, NotPetya, Stuxnet, TRISIS…). Certaines attaques visent à causer des dommages humains ou matériels.

Ce contexte pousse à considérer les menaces cyber dans l'analyse globale des risques que font peser les installations industrielles sur les personnes et l'environnement.

Des cadres réglementaires et des méthodes bien définies existent pour l'analyse et la maîtrise des risques accidentels mais ils ne sont pas adaptés à la prise en compte de la cybersécurité. En effet, l'évaluation et la maîtrise dans le temps de risques liés à des phénomènes accidentels connus, ou du moins pour lesquels on suppose que la connaissance progresse, et de risques liés à une menace consciente et évolutive sont fondamentalement différents.

Lorsqu'on s'intéresse à un scénario accidentel, on recherche des dérives, défaillances ou agressions accidentelles dont on va déterminer les différentes conséquences possibles en fonction, par exemple, du fonctionnement ou de l'échec de barrières de sécurité. On étudie donc la probabilité d'occurrence et la gravité de séquence d'événements avec une cause unique.

Pour les scénarios d'attaque, les analyses et les caractérisations sont différentes : un attaquant cherchera à accomplir différentes actions coordonnées pour atteindre un objectif défini. On cherche donc à identifier les attaquant et les cibles potentiels pour déterminer les chemins d'attaque possible et les vulnérabilités qui pourront être exploitées par l'attaquant. Celui-ci étant doué d'intelligence, et éventuellement de temps et de moyens techniques, il mettra en œuvre des stratégies d'infiltration du réseau, exploration puis contournement des moyens de sécurité existants.

La prise en compte des risques liés à la cybersécurité dans l'analyse de risques d'une Installation Classée demande donc d'élargir le champs d'analyse et les compétences des analystes : il faut d'une part identifier des scénarios reposant sur des événements coordonnés visant à maximiser les conséquences et contourner les barrières en place et d'autre part inclure l'ensemble du système informatique industriel dans le champs de l'analyse sous l'angle de la sécurité informatique alors qu'on étudiait jusqu'à présent uniquement les couches basses de ce système (c'est-à-dire celles les plus proches du procédé contrôlé – capteurs, actionneurs et automates) sous l'angle de la sûreté de fonctionnement.

De la même manière, en exploitation, il faudra maintenir le niveau de cybersécurité par l'application de dispositions organisationnelles, humaines et techniques adaptées, comme pour les risques accidentels, mais il faudra également être en mesure de prendre en compte l'évolutivité de la menace par le biais par exemple de veille sur la publication de vulnérabilités sur les équipements ou logiciels intégrés au système de contrôle industriel. Pour cela, les scénarios et systèmes critiques doivent être correctement identifiés en phase d'analyse des risques.

Pour prendre en compte ces nouveaux enjeux, l'INERIS a développé une méthodologie générale d'analyse combinée des risques liés à la cybersécurité et des risques d'accidents majeurs. L'objectif de la démarche est d'identifier des scénarios d'attaques ayant potentiellement des conséquences graves pour les personnes et l'environnement. Cette démarche repose sur la coordination de méthodes existantes pour l'analyse de risques accidentels d'une part et l'analyse des risques liés à la cybersécurité d'autre part. Elle permet de

prendre en compte le procédé physique et le risque métier de manière étendue dans une démarche de cybersécurité.

On cherche à articuler deux démarches d'analyse basées sur des méthodes existantes : une démarche d'analyse des risques physiques pour les personnes et l'environnement, issues des méthodes de type APR (analyse préliminaire des risques) dont on élargit le champ d'analyse pour prendre en compte la spécificité des scénarios liés à des attaques du système de contrôle industriel [1] et une démarche issue de la sécurité informatique centrée sur l'identification de scénarios pouvant avoir des conséquences physiques. L'articulation de ces deux démarches permet d'aboutir à un modèle de représentation unique dit AT/BT (Attack Tree / Bow Tie) [7].

Cette nécessaire articulation nécessite de faire appel à de nouvelles compétences, liées à la sécurité informatique, dans l'analyse des risques d'une installation industrielle et d'élargir e périmètre de l'analyse. Cela peut poser des difficultés pratiques, les principes, vocabulaires, métriques et objectifs pouvant parfois diverger. Le cadre d'analyse commun entre sûreté et sécurité permet de traiter ces antagonismes, valoriser les renforcements mutuels et d'aboutir à une vision plus complète des risques qu'une installation industrielle fait peser sur les personnes et l'environnement [8].

Ce nouveau cadre d'analyse introduit de nouvelles complexités et nécessite une vision systémique de l'installation De plus, la maîtrise de la cybersécurité repose sur une veille permanente sur les menaces et les vulnérabilités liées aux équipements et logiciels utilisés. Pour cela des outils numériques de description de système, analyse des risques et suivi en exploitation sont nécessaires. Les développements de l'Ineris sur le management numérique de l'AR présentés au paragraphe suivant pourraient aider à répondre à ces nouvelles problématiques.

*A.2. Management numérique de l'AR*

Depuis 2014, l'INERIS, avec plusieurs partenaires industriels (tout particulièrement avec les 15 dépôts d'hydrocarbures du Service national des oléoducs interalliés -le SNOI-), développe une démarche sur l'utilisation du numérique pour améliorer les AR et leurs usages. L'enjeu est de mieux intégrer les AR dans les systèmes de pilotage des ICPE. L'idée est la suivante. Plus les AR seront intégrées dans les pratiques d'une sécurité opérationnelle, au plus proche des installations, plus elles pourront s'améliorer en se frottant aux connaissances empiriques des opérateurs (conception, maintenance, production, logistique, etc.). Dans le même temps, plus les AR seront critiquables et amendables, plus elles pourront se couler dans les subtilités des réalités singulières, et plus elles pourront aider aux décisions quotidiennes des opérateurs. Reste à savoir comment faire ?

L'informatique peut aider à articuler et à faire évoluer de concert les études de risques (DDAE – demande d'autorisation d'exploiter, notice de réexamen des EDD, cahiers de démonstration spécifiques, SGS – système de gestion de la sécurité, …) et les documents opérationnels (procédures, modes opératoires, gammes, plans, enregistrements, contrats de sous-traitance, etc.)

Prenons l'exemple de la gestion de détecteurs de niveau de bacs de stockage d'hydrocarbures. Plusieurs dimensions sont à articuler :

- Les prescriptions réglementaires, notamment l'article 7 de l'arrêté du 4 octobre 2020, et les prescriptions de l'arrêté d'autorisation d'exploiter.
- Les études de risques qui précisent :
    - Les fonctions remplies par ces détecteurs au sein d'une barrière, et le caractère critique de leur bon fonctionnement compte tenu de l'architecture globale de la sécurité.
    - Les exigences propres à ces détecteurs, qu'il faut respecter pour les qualifier comme éléments techniques fiables.
- Les règles de gestion de ces détecteurs, tout au long de leur cycle de vie.
- Les preuves du respect de ces règles.
- Les retours d'expériences incidentels.
- Les modifications.

L'outil informatique peut faciliter les **contrôles qualitatifs**, contrôles de la cohérence d'ensemble, en facilitant la navigation rapide entre toutes ces dimensions, pour permettre de répondre, par exemple, aux questions suivantes. Le temps de réponse des détecteurs, précisé dans l'analyse de la barrière (ou à définir à partir de cette analyse), est-il bien pris en compte dans les choix d'achat du matériel ? Et dans un programme de surveillance conforme à l'article 7 de l'arrêté du 4 octobre (selon un guide professionnel reconnu par le ministre chargé de l'environnement, ou sur la base d'une méthodologie développée par l'exploitant) ? Et dans les formations des opérateurs qui en ont la charge ? Par ailleurs, compte tenu des contraintes d'achat et de maintenance, le choix de ce sous-système comme élément d'une barrière est-il pertinent ? La gestion opérationnelle permet-elle d'assurer une maîtrise satisfaisante de l'ensemble des exigences de la barrière ?

L'outil informatique peut faciliter les **contrôles quantitatifs**, par exemple la vérification que, sur une période donnée, les actions de maintenance non réalisées ou les éventuels dysfonctionnements des détecteurs ne mettent pas en cause l'atteinte d'une criticité acceptable du point de vue des risques accidentels et chroniques. Ici, l'informatique s'appuie sur les données d'exploitation (GMAO et base d'incidents) pour estimer l'ensemble des jours de "non-confiance" ou d'indisponibilité des détecteurs, afin de refaire les calculs de probabilité.

Enfin, l'outil informatique peut faciliter la **gestion des modifications**, permettant de naviguer facilement dans l'historique des études de risques et des documents opératoires, afin de préparer et tracer les modifications.

Pour l'étude et la gestion d'un seul détecteur, l'informatique n'est pas utile (il serait même contre-productif). Mais lorsqu'il faut en gérer des dizaines, avec des spécificités liées par exemple aux constructeurs ou aux contextes d'utilisation, avec des dizaines d'études, des dizaines de procédures ou modes opératoires, et des centaines d'enregistrements annuels… et lorsqu'il faut gérer ainsi des milliers d'équipements… les documents papiers obscurcissent la lisibilité, les contrôles, la traçabilité. Et puis, quoi de mieux que de pouvoir aller sur le terrain avec une tablette mettant à disposition l'historique des données sur les équipements, ainsi que les procédures et les études de risques liées, et la possibilité de saisir, directement, au bon endroit dans le système informatique, les résultats des contrôles, et d'enregistrer des photos montrant les conformités ou les éventuels défauts ?

Dans cette perspective, en aucun cas l'informatique remplace les études ou les documents opérationnels. Il ne permet que de faciliter le contrôle de leur cohérence, et ainsi leur élaboration. Ce point est important, car il précise le scope de l'outil, sa plus-value, mais aussi le rythme de son implémentation et de son évolution. L'usage de l'outil informatique, sur lequel l'INERIS conduit actuellement sa recherche opérationnelle, est centrée sur l'aide à la réalisation des études de risques. L'outil n'est mis à jour qu'à chaque nouvelle étude de risques.

Reformulons. L'INERIS travaille (depuis 2014) sur l'élaboration d'une application WEB dans laquelle les « molécules » de connaissance des études de risques (et des prescriptions ICPE) sont éclatées, gérées en un seul exemplaire informatique, et recombinées jusqu'à permettre l'édition "automatique" :

- des études de risques au format PDF ;
- d'écrans qui aident les multiples acteurs à interroger, à construire et à tracer la cohérence d'ensemble.

Concrètement, aujourd'hui, l'outil informatique développé avec le SNOI permet de :

- Gérer les prescriptions réglementaires à travers des doctrines et des preuves
- Recalculer tous les semestres la maîtrise du risque de pertes de confinement des réservoirs en s'appuyant sur des données de terrain (possibilité de faire des calculs d'actualisation des risques sur tous les nœuds papillons)
- Préparer les réunions du COPIL et gérer les comptes rendus
- Préparer les inspections en aidant les équipes à faire le point sur les preuves
- Gérer l'adéquation entre les travaux prévus et les mesures de maîtrise des risques définies dans les EDD
- Gérer la liste des équipements considérés dans les études de risques, les géolocaliser et les visualiser sur les plans de masse et dans un SIG
- Gérer les APR
- Gérer les connaissances des notices de réexamen des EDD, et les éditer.

D'autres développements sont prévus en 2020 et 2021 pour progresser dans l'intégration des études de risques (EDD, POI, SGS, etc.).

Le problème le plus difficile à résoudre est celui de la traduction des études de risques entre elles et avec les documents opératoires, à cause des différents niveaux d'abstraction à articuler dès lors que l'on veut lister systématiquement les exigences importantes pour la gestion des risques avec les explications liées à leurs raisons d'être. Déjà, ce travail n'est pas évident à partir d'une seule étude. A la lecture d'une étude de dangers par exemple, il est difficile d'établir une liste unique des mesures à mettre en œuvre, parce que ces mesures y sont exprimées dans des termes différents, à plusieurs endroits de l'étude (dans les exclusions, dans l'APR, dans les hypothèses de modélisation, etc.), et surtout avec des niveaux d'abstraction différents (un même détecteur peut être concerné par des mesures valables pour tous les détecteurs du site, pour tous les détecteurs d'un même type de bac, pour tous les détecteurs jouant un rôle dans des MMRi, pour tous les détecteurs d'une même zone, etc.). Il est encore plus difficile de garder la trace des fonctions de sécurité et des exigences qui pèsent sur ce détecteur. Même les rédacteurs peuvent s'y perdre.

Les industriels auraient tout à gagner à travailler sur cette problématique. D'une part parce que la cohérence de leur système est un gage d'une meilleure maîtrise. D'autre part parce que, s'appuyant sur les probabilités développées dans les AR, ils pourraient avoir un management plus fin, accepter des défaillances tout en préservant un niveau de risques satisfaisant. Ils pourraient ainsi, sans doute, en accord avec l'inspection, diminuer des coûts de maintenance ou de gestion des modifications en cas de dysfonctionnements, et favoriser une remontée transparente des incidents.

Les inspecteurs gagneraient aussi à travailler cette problématique. Ils gagneraient du temps, dans la mesure où ils se perdraient moins dans les documents. Ils auraient surtout des listes systématiques et claires de points à contrôler sur le terrain, élaborées à partir des études qui ont conduit à l'autorisation d'exploiter, avec un accès direct à toutes les dimensions à interroger.

Cette approche numérique du management permet ainsi de pallier certaines carences aujourd'hui identifiées des SGS réglementaires. Si l'analyse de risques est un exercice prospectif dont l'objectif est d'imaginer des séquences d'évènements qu'il s'agit de limiter ou d'arrêter avant l'occurrence de l'évènement redouté, leur transformation en savoirs et pratiques gestionnaires est en effet censé se concrétiser dans le cadre du système de gestion de la sécurité. Défini dans le cadre des différentes directives Seveso comme un amoncellement de processus gestionnaires, les SGS ont du mal à aller au-delà de l'obligation réglementaire pour pénétrer la réalité des pratiques organisationnelles. En d'autres termes, et en considérant que tout dispositif gestionnaire a comme finalité première un apprentissage collectif, il est légitime de s'interroger aujourd'hui sur la capacité des SGS à générer des apprentissages collectifs.

Il nous semble que la définition et la pratique des SGS aujourd'hui échouent face à une telle finalité en raison des éléments suivants :

- Réglementairement tout d'abord, les SGS ne sont pas définis comme les compagnons indéfectibles des AR. Ainsi, si les Seveso Seuil haut se doivent de déployer conjointement une AR et un SGS, les seuil-bas ont une obligation de SGS sans AR. Or, quels SGS pouvons-nous espérer si celui-ci ne se base pas sur une connaissance aussi approfondie que possible des scénarios accidentels ?
- Au-delà de cette disjonction réglementaire entre AR et SGS, les modalités de définition des SGS soulèvent des difficultés majeures quant à leur application. Réglementairement, les différentes versions de la directive Seveso ne fournissent jamais une définition claire. Le lecteur est ainsi renvoyé à l'annexe 3 où tout SGS est censé contenir une liste d'éléments, qui sont autant de processus gestionnaires, allant de l'organisation du personnel à la gestion des modifications ou l'élaboration des plans d'urgence. Aucun schéma d'articulation ou de coordination de ces processus n'est fourni ou suggéré laissant aussi bien les gestionnaires HSE que l'inspection dans l'impossibilité de faire appel à un référentiel commun qui servirait aussi bien à la conception des SGS qu'à leur évaluation. L'approche numérique introduite plus haut est une piste dans ce sens. En l'état actuel des choses, la définition réglementaire des SGS laisse de côté l'ensemble systémique des SGS permettant de comprendre les modalités d'interaction entre processus gestionnaires internes au SGS et les modalités externes d'interaction entre SGS et autres dispositifs gestionnaires de l'organisation
- Enfin, tout outil gestionnaire, SGS compris, se doit d'avoir comme finalité première l'initiation et la conduite d'apprentissages collectifs. Un des axes de cet apprentissage devrait bien évidemment être celui de la révision ou l'actualisation des AR au regard, non seulement des évènements (qu'ils soient précurseurs, incidentels ou accidentels), mais aussi des pratiques positives déployées au quotidien par le personnel à différents niveaux pour permettre au système de continuer de fonctionner dans des limites acceptables. Dans l'autre sens aussi, il devrait être faisable et surtout traçable de procéder aux modifications nécessaires dans le SGS du fait de l'évolution des connaissances développées dans le cadre de l'AR.

*B. Les Natech*

Le changement climatique est une autre catégorie de transition qui nécessite une réflexion sur l'adaptation de la pratique de l'AR. Ce contexte a notamment pour conséquences d'entraîner des phénomènes météorologiques extrêmes dans certaines régions du globe, l'impact des aléas naturels sur les risques technologiques (Natech) est une préoccupation grandissante depuis plusieurs années déjà. A l'image de l'OMS qui dans un récent rapport souligne l'augmentation de la fréquence et de l'intensité des catastrophes naturelles comme conséquence du changement climatique, de nombreuses instances internationales, telles que l'OCDE ou l'UNECE par exemple, se sont saisies de la problématique pour alerter les décideurs publics et les gestionnaires du risque. Si des études relativement datées ont montré que les accidents Natech ne constituaient que 5% des accidents industriels reportés dans les bases de données d'accidents [9], cette valeur est probablement sous-estimée du fait que certains événements mineurs n'y sont pas comptabilisés [10]. Au vu de la tendance à l'augmentation des catastrophes climatiques, l'occurrence des accidents Natech augmentera probablement en conséquence [11].

Cette tendance globale n'épargne pas les sites industriels français puisque, comme le souligne le BARPI dans son dernier inventaire des accidents technologiques de 2018, 107 d'entre eux ont été impactés par des phénomènes naturels (pluie-inondation, foudre, forte chaleur et froid intense), ce qui représente près de 9 % des événements recensés dans la base ARIA, sur ce même périmètre et cette même année. Dans ce même bilan, le BARPI indique par ailleurs que depuis 2010, le nombre d'événements météorologiques impactant des sites industriels en France est par ailleurs en constante évolution, soulignant dans une certaine mesure, l'augmentation et l'intensité de ces phénomènes.

La démarche de prévention et de maîtrise des risques industriels repose sur une analyse des risques qui se doit de prendre en compte à la fois les risques intrinsèques aux installations industrielles mais aussi les potentiels agresseurs liés au contexte local du site, qu'ils soient anthropiques ou naturels. A la différence des risques inhérents à l'outil de production qui depuis 2003 se doivent d'être quantifiés en

probabilité, la réglementation française actuellement en vigueur autorise un traitement particulier pour certains événements naturels et permet ainsi :

- d'exclure certains événements initiateurs externes et extrêmes (ex : crue supérieure à la crue de référence selon les règles en vigueur, événements climatiques d'intensité supérieure aux événements historiquement connus ou prévisibles pouvant affecter l'installation, selon les règles en vigueur, etc.) ;
- de ne pas considérer certains évènements naturels dans la quantification probabiliste des accidents majeurs si les éléments réglementaires ou les bonnes pratiques associés sont respectés (cas par exemple de la crue si l'industriel fournit la justification du dimensionnement de ces installations pour leur protection contre la crue de référence (telle par exemple que définie à ce jour dans le guide plan de prévention des risques inondations (PPRi) du ministère du développement durable)).

L'intensification de certains événements naturels, en termes de fréquence et d'amplitude, invite à se questionner sur le maintien d'un tel positionnement dans la réalisation de futures analyses de risques. En effet, les niveaux de référence retenus dans les Plans de Prévention des Risques Naturels existants intègrent-ils l'amplification de ces phénomènes ? Si depuis 2011, les Plans de Préventions des Risques Naturels Littoraux doivent intégrer une surcote dans la définition du niveau de référence pour intégrer l'augmentation du niveau de la mer liée au changement climatique, en est-il de même pour les PPRi, TRI, ou autres plans de gestion des inondations au niveau d'un territoire ? Est-on d'ailleurs en mesure de prédire suffisamment l'intensification des événements climatiques pour définir un niveau de référence dans le cas de phénomènes, par essence, extrêmes ? Les séquences accidentelles identifiées pour des inondations prévisibles sont-elles toujours pertinentes dans ce type de situations ? Les mesures de maîtrise des risques identifiées dans le cadre de scénarios accidentels conventionnels peuvent-elles toujours être disponibles et efficaces dans de telles circonstances ? Le dimensionnement des installations et des éventuels ouvrages de protection intègre-t-il une marge de sécurité suffisante ? La planification des situations d'urgence via par exemple l'élaboration de procédures de mise en sécurité en cas d'inondation peut-elle être en mesure de s'adapter à des phénomènes à cinétique et intensité variable ? Quand elles existent, de telles procédures sont-elles suffisamment robustes et efficaces ? Les systèmes d'alerte existants sont-ils adaptés ?

C'est sur la base des travaux antérieurs réalisés et animés par ces questionnements que l'Ineris poursuit ses travaux pour une meilleure prise en compte des Natech dans l'analyse des risques des systèmes industriels.

*C. Conséquences environnementales*

Outre les transitions de l'AR concernant les données d'entrée à considérer, et la façon de la dérouler, les produits de l'AR peuvent aussi être questionnés. En particulier, la sensibilité de l'AR à la dimension environnementale peut être questionnée, dans le contexte actuel de changement climatique, de perte de biodiversité et d'effondrement des populations du vivant. Une réflexion est en cours concernant les études de danger, pour évaluer l'acceptabilité du risque. La Directive Seveso III vise à « *prévenir les accidents majeurs qui pourraient être causés par certaines activités industrielles et à en limiter les conséquences pour la santé humaine et pour l'environnement* ». Cependant, la réglementation française ne tient compte que du nombre d'humains potentiellement touchés (cf la définition des seuils d'effet dans l'arrêté du 29 septembre 2005) il n'y a pas de règle nationale pour estimer la gravité environnementale.

La réflexion de l'Ineris a pour but d'élaborer une méthode qui permette à tout industriel volontaire d'estimer les conséquences environnementales que pourraient avoir un potentiel accident sur son site. La méthode suit les différentes étapes de l'étude de dangers pour pouvoir s'y intégrer aisément. Pour autant, elle doit être autoportante de sorte qu'un exploitant d'un site non soumis à études de dangers puisse aussi la mettre en œuvre.

En préambule de la méthode, il convient d'identifier les substances dangereuses présentes sur le site qui pourraient, du fait d'un accident, se transférer en dehors du site et impacter des récepteurs. Or dès ces trois premières étapes des difficultés techniques émergent.

L'identification des substances dangereuses est intrinsèquement liée à leur caractère inflammable, explosif, toxique, infectieux, etc. Or cette dangerosité varie-t-elle avec sa forme (aqueuse, solide, gazeuse) ? Par rapport à quoi mesurer son niveau de dangerosité lorsqu'il s'agit d'une substance toxique ou infectieuse (ex : sera-t-il le même pour un lapin et un chêne) ? La substance en se transférant dans le milieu réagira-t-elle ? Et cette substance éventuellement produite sera-t-elle dangereuse ?

Les voies de transfert peuvent être multiples selon le scénario considéré : fumées (particules dans l'air), nuage (substance sous forme gazeuse), cours d'eau (substance solide dissoute ou transportée en petites particules), élution dans les sols (substance liquide ou solide dissoute ou transportée en petites particules), etc. L'étendue du transfert dépend alors d'une infinité de paramètres : conditions météorologiques, nature des sols, caractéristiques des cours d'eau, etc. A ce stade, outre la difficulté d'englober l'ensemble des couples substances / transferts, nous nous heurtons aux limites des connaissances scientifiques actuelles (ex : l'élution des pesticides n'est pas encore systématiquement connue).

L'identification et la prise en compte des éléments vulnérables est aussi complexe. Tous les récepteurs d'une zone peuvent-ils être identifiés ? Ne faut-il que considérer ceux qui relèvent d'espèces protégées ou menacées ? Faut-il se positionner à une échelle plus macroscopique en tenant compte uniquement des espaces protégés, des réserves nationales, etc ? Peut-on n'estimer que des tonnages d'animaux morts et des hectares de végétation, comme cela est fréquemment fait en post-accidentel ? Quelles sont les ressources à prendre en compte (ex : des terres agricoles

polluées se traduisent-elles en nombre d'agriculteurs au chômage ou bien doit-on considérer autrement la dégradation de cet espace de vie artificialisé ?) Comment intégrer les dimensions de tolérance et résilience du milieu ?

Viendront ensuite les problématiques relatives à la cotation et à la détermination de l'acceptabilité. Comment hiérarchiser les impacts sur la faune, la flore et les ressources ? Est-il opportun d'appliquer la même échelle que celle utilisée par le BARPI ? Comment procèdent les autres pays européens qui ont proposé des méthodes estimant les conséquences environnementales de potentiels accidents industriels ?

Dès à présent, il ressort que pour enrichir l'AR usuellement réalisée dans les études de dangers, en y intégrant la préservation effective de l'Environnement, les obstacles techniques et scientifiques devront soit être levés soit faire l'objet d'approximations. De même, la méthode soulève des questions d'ordre éthique et les principaux concernés ne peuvent être intégrés aux discussions. Pour autant les atouts de cette méthode en devenir semblent multiples : facilement intégrable dans la démarche d'AR avec laquelle les industriels sont familiers, outil de communication pédagogique, et support à l'amélioration continue pour la préservation de la biodiversité, qu'il est urgent de protéger.

*D. Effets Dominos*

Le dernier thème considéré est celui des effets dominos. La bonne connaissance des effets dominos et de leur maîtrise constitue en effet un véritable enjeu tant au sein d'un établissement industriel qu'au sein des zones industrielles, qui font se côtoyer plusieurs installations ou établissements mettant en œuvre des substances dangereuses. En effet, parmi tous les accidents industriels, les accidents impliquant des effets dominos sont parmi les plus destructeurs et peuvent entraîner de graves conséquences sur la population, les biens et l'environnement naturel au voisinage des installations impliquées. Pour preuve, on peut notamment citer les accidents de Feyzin (1966), de San Juan Ixhuatepec au Mexique (1984) et de Tianjin en Chine (2015) pour un cas plus récent.

On entend par effet domino l'action d'un phénomène dangereux (effet thermique, surpression et de projection) survenant sur un premier équipement, impactant un second équipement et entrainant un second phénomène dangereux sur ce dernier équipement, engendrant une aggravation des conséquences générées par le premier équipement.

Depuis plus d'une dizaine d'années, l'Ineris a pris la mesure de cette problématique. Des réflexions ont été menées pour intégrer les effets dominos à l'analyse des risques des procédés industriels, des travaux plus poussés ont été menés sur la résistance des structures aux sollicitations accidentelles. L'Institut a élaboré une méthode d'évaluation des effets dominos, qui apporte notamment :

- des outils pour mieux évaluer la vulnérabilité des équipements industriels aux sollicitations accidentelles ;
- la possibilité de quantifier les séquences d'effets dominos en probabilité d'occurrence et en gravité des conséquences, avec des critères pour évaluer si le risque est acceptable ou non ;
- la possibilité de mettre en œuvre une démarche d'amélioration et de réduction du risque, avec une série de mesures à choisir en fonction des scénarios.

La démarche pour l'identification des séquences d'effets dominos consiste ainsi, dans un premier temps, à identifier les équipements industriels agresseurs susceptibles d'être le siège de phénomènes dangereux tels que des incendies, des explosions et de causer des dommages à d'autres équipements situés à proximité, ainsi que les équipements industriels susceptibles d'être agressés et pouvant entraîner à leur tour des phénomènes dangereux. Cette étape d'identification des équipements agresseurs / agressés peut s'appuyer sur les résultats des démarches d'analyse de risques existantes, des rapports de sécurité des sites industriels...

Les séquences d'effets dominos possibles sont ensuite déterminées en croisant l'intensité des effets des phénomènes dangereux qui se produisent sur les équipements agresseurs et la vulnérabilité des équipements susceptibles d'être agressés. Pour ce faire, des seuils forfaitaires de vulnérabilité des équipements peuvent être utilisés, en première approche (par exemple, les seuils des effets dominos de 8 kW/m2 pour les effets thermiques et de 200 mbar pour les effets de surpression), mais il est aussi possible d'avoir recours à une analyse plus complexe reposant sur des abaques ou des modélisations plus précises du comportement des équipements agressés en fonction des caractéristiques des agressions potentielles. Cette étape est cruciale dans l'identification des séquences d'effets dominos, mais à ce jour, elle est basée, dans la majorité des cas, sur des seuils forfaitaires, les données numériques permettant d'évaluer plus précisément cette vulnérabilité, en fonction du type d'équipement étudié, étant encore peu disponibles et utilisées.

Le risque associé à chacune des séquences d'effets dominos identifiées peut alors être caractérisé, en déterminant la gravité des conséquences et la probabilité d'occurrence des accidents associés.
Le positionnement des différents accidents dans une grille de croisement gravité / probabilité va permettre de juger de l'appréciation des séquences d'effets dominos, et d'engager, s'il y a lieu, une démarche de réduction du risque. Pour les séquences d'effets dominos jugées inacceptables en première approche, il peut être recherché d'affiner l'évaluation des risques en affinant les hypothèses d'évaluation de la vulnérabilité ou d'évaluation des effets thermiques ou de surpression par exemple et / ou en étudiant les mesures mises en place ou à mettre en place pour réduire les risques (mise en place de barrières, etc).

En plus de la démarche d'évaluation des risques, le travail d'identification des effets dominos potentiels s'avère aussi très intéressant dans le cadre de l'élaboration des plans d'urgence des sites industriels, car il permet d'établir une priorité dans les actions à mener en cas de situation d'urgence. La notion de dynamique, c'est-à-dire le temps pour qu'un premier phénomène dangereux sur un

équipement puisse entraîner d'autres phénomènes dangereux sur des équipements voisins, prend également ici tout son sens mais est difficile à évaluer. L'analyse des effets dominos peut s'avérer aussi complexe dès lors que le nombre d'installations et de phénomènes dangereux à analyser est important, d'où la nécessité d'outils pour automatiser certaines étapes de la démarche.

## IV. DISCUSSION ET CONCLUSION

Cet article a débuté par un questionnement sur l'évolution des AR dans le domaine des ICPE, rappelant que les dernières grandes modifications réglementaires et de pratiques dataient de la dynamique lancée en 2003 (loi Bachelot) consécutive à l'accident de Toulouse, en 2001. Cet article a ensuite introduit des travaux questionnant les limites des AR, montrant qu'elles reposent sur des choix de scénarios, des modèles de causalité et des principes de calculs qui sont toujours questionnables.

Ces limites nous interrogent sur la nature et l'ampleur des ajustements potentiels des pratiques et usages des AR actuelle. Plusieurs questions peuvent être posées à la suite de la présentation des différents thèmes (cybersécurité, natech, management numérique, effets dominos et conséquences environnementales). Quelles évolutions à court ou moyen terme ces problématiques et travaux associés sont susceptibles d'entrainer ? Sont-ils compatibles ? Peut-on les articuler ? Redéfinissent-ils substantiellement les contours de l'analyse de risques ou sont-ils des compléments à l'existant ? Eclairent-ils sous un nouveau jour la question des limites des analyses de risques ?

Un premier point à noter est que les thèmes abordés couvrent plusieurs des limites identifiées par Downer (tableau 2). Le dimensionnement des scénarios est traité notamment par les effets dominos et les conséquences environnementales. Les dimensionnements des scénarios dépendent en effet de ce qui est considéré dans les modélisations des effets des phénomènes d'explosion, de surpression ou de dispersion toxique, or ces modélisations sont susceptibles d'être affinées certes mais aussi potentiellement revues à la hausse en prenant en compte effets dominos et conséquences environnementales.

Le problème du calcul de probabilité et de la conformité est couvert par l'approche numérique. Le rapport entre AR et réel des pratiques est en effet au cœur de l'idée d'un support du digital au processus de gestion de la sécurité, de même qu'une approche suivant de manière informatique ces réalités permet d'alimenter une approche plus juste des calculs grâce aux données de suivi disponibles. Enfin, les limites sous l'angle des nouveaux scénarios sont traitées par les thématiques de la cybersécurité et des natech.

Tableau 2 : limites AR et thèmes discutés

| Limites | Description | Thèmes |
|---|---|---|
| Dimensionnement des scénarios | Evénement identifié mais intensité sous-estimé | Effets dominos, conséquences environnementales |
| Calculs de probabilité | Problème dans les données | Management numérique de la sécurité |
| Conformité des pratiques aux attendus de l'AR | Les mesures de prévention et protection mises en œuvre ne correspondent pas dans la réalité à ce qui était prévu | Management numérique de la sécurité |
| Scénario non pris en compte | Evénement inconnu ou dont la probabilité est jugée négligeable | Cybersécurité, natech |

Un second point qui se dégage est la nature systémique des thèmes. La cybersécurité nécessite de maintenir une vue d'ensemble des installations car les attaques sont susceptibles de concerner de manière simultanée tous les dispositifs de prévention et de protection (jusqu'aux moyens de secours). De même, les natech (par exemple une inondation) exposent potentiellement l'ensemble d'un site industriel de manière quasi simultanée plutôt qu'une partie de celui-ci (de même qu'ils peuvent contrecarrer l'intervention des secours).

Pour ces deux thèmes, les effets dominos sont aussi au cœur de cette dimension systémique. Chercher à anticiper l'interaction de plusieurs équipements et phénomènes de manière plus ou moins concomitants est au cœur des effets dominos. Si l'on ajoute à cette thématique la question des conséquences environnementales, on constate également que s'étend la dimension systémique du questionnement.

Un événement de type natech est susceptible de produire des effets hors du site d'une manière tout à fait inhabituelle par rapport aux scénarios classiques, et peut nécessiter une réflexion concernant les effets sur l'environnement. De même, une vulnérabilité de type cyber créé de nouvelles catégories de scénarios à envisager en matière de conséquences environnementales, comme par exemple la pollution malveillante d'une nappe phréatique.

On le voit, la pratique de l'AR se trouve impactée par ces nouvelles thématiques. On peut supposer qu'un renouvellement des modes d'anticipation est donc en cours d'élaboration avec ces développements. Cet article n'est qu'une première contribution à une réflexion sur ce point.

D'autre part, l'apport du numérique est désormais central dans l'approche de la pratique et de l'usage des AR. Le potentiel des applications permises par un management articulé des activités concrètes des opérateurs avec les AR ouvre des pistes pour une combinaison fructueuse avec toutes les nouvelles thématiques introduites dans cet article. La cybersécurité figure au premier plan de ces pistes étant donné la sensibilité d'un pilotage de la gestion des risques qui reposent de plus en plus sur les outils digitaux.

Considérés tous ensemble, ces thèmes montrent l'intérêt du questionnement sur les évolutions des AR et les limites de celles-ci, dans un contexte de mutation. Tous ces thèmes sont en effet à la fois des évolutions en cours qui pointent les limites actuelles des AR Ces sujets sont peut-être les événements d'ampleur de demain. Ils participent d'un travail d'anticipation attendu. Dans un contexte de profondes mutations, il nous semble évident qu'il n'est pas possible, à court ou moyen terme, de contourner un débat collectif qui débouchera peut être sur une révision des cadres conceptuels,

méthodologiques et réglementaires actuellement associés à l'analyse de risque.

## REFERENCES


[1] Escande, J., Proust, C., Le Coze, JC. 2016 Limitations of current risk assessment ... Journal of *Loss Prevention* in the Process Industries, n°43, pp.730-735.

[2] Martinais, E. (2010). L'écriture des règlements par les fonctionnaires du ministère de l'écologie. La fabrique administrative du PPRT. *Politix*, vol. 23. n° 90. 193-223

[3] Jasanoff, S. 1993. Bridging the two cultures of risk analysis. *Risk Analysis.* Vol 13, Issue 2, pages 123–129

[4] Wynne, B. (1982). Institutional mythologies and dual societies in the management or risk. In Kunreuther H, Ley E. (eds) *The Risk Analysis Controversy: an Institutional Perspective*. Berlin: Springer Verlag, Berlin.

[5] *owner*, *J*. (*2014*). *Disowning Fukushima*: *Managing* the *Credibility* of *Nuclear Reliability Assessment* in the *Wake* of *Disaster*. *Regulation* & *Governance* 8, 287-309

[6] F. Massé, J.M. Flaus, H. Abdo, "Comment intégrer les cyberattaques dans l'évaluation globale des risques pour les installations classées ? Proposition d'un cadre général d'analyse des risques," Congès Lambda Mu 16-18 ocotobre 2018

[7] H.Abdo, M. Kaouk, J-M. Flaus, F. Massé, "A new approach that consider cybersecurity within industrial risk analysis using a cyber bow-tie analysis", *Computers & security*, vol. 72, pp. 175–195, 2018.

[8] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability engineering & system safety*, vol. 139, pp. 156–178, 2015.

[9] Rasmussen K., 1995, Natural events and accidents with hazardous materials, Journal of Hazardous Materials, 40, 43-54.

[10] Casson Moreno V., Ricci F., Sorichetti R., Misuri A., Cozzani V., 2019, Analysis of Past Accidents Triggered by Natural Events in the Chemical and Process Industry, Chemical Engineering Transactions, 74, 1405-1410 DOI:10.3303/CET1974235

[11] Mahan, P., Liserio, F., 2018. Managing the risk associated with severe wind and flood events in the chemical processing industries, in: Hazards 28. pp. 1–10