# Un cadre conceptuel pour la comparaison sûreté et sécurité de filières industrielles

Gilles DELEUZE[1]

[1]EDF R&D, Management des Risques Industriels, 1 Avenue du Général de Gaulle, 92141 CLAMART CEDEX

gilles.deleuze@edf.fr

**Résumé** – Cette communication fait suite à des travaux présentés au WISG 07 [15], au séminaire ImdR-IEC 2007 [14] et dans le cadre du projet 6ème PCRD NEEDS [10][11] et d'autres sources [16]. En première partie, nous proposons des définitions de plusieurs « concepts » ou « attributs » employés dans la littérature à propos des risques industriels, naturels et de malveillance, avec l'idée de proposer un cadre conceptuel commun à trois aspects de la « sécurité globale »: le risque d'accident industriel, le risque de catastrophe naturelle majeure et du risque d'acte de malveillance majeur affectant les biens matériels et les personnes (chapitres 2.1 à 2.4.). Nous présentons le cadre conceptuel, qui illustre et nous l'appliquons au cas du risque d'accident industriel, du risque de catastrophe naturelle majeure et du risque d'acte de malveillance majeur.

En seconde partie, nous proposons une déclinaison du modèle à une problématique particulière (comparaison de transport et production d'énergie en Europe en 2040) posée dans le cadre du projet 6ème PCRD NEEDS ([11]), pour élaborer des « indicateurs de risque » pouvant être représentatifs d'un niveau de sécurité globale, voire agrégés en un « indice de sécurité globale », pouvant être employés pour diverses décisions (comparaison de sites, prospective technologique…) et diverses infrastructures (transport de données, de personnes…).. Enfin, la conclusion résume les apports et les limites de l'approche proposée. Cet article est proposé à des fins de recherche, il n'est représentatif d'une politique EDF en matière de sécurité.

**Abstract** – In this paper, we propose a conceptual framework, elaborated from previous studies (WISG 07 [15], ImdR-IEC 2007 [14], 6th PCRD NEEDS project [10][11], other authors [16]) illustrating the relationships between safety and security of industrial plants and technologies. We present a conceptual framework illustrating relationships between various concepts related to risk, from which we analyse similarities and differences between industrial accidents, natural events and malevolent actions. We explain then how risk indicators can be elaborated from the framework, and illustrate it in an example of global security assessment of critical technological infrastructures. We conclude with the benefits and limits of the approach. This paper is written in a scope of discussion on modelling issues. It is based on R&D exploratory studies. It does not represent the current EDF policy regarding security management

## 1. Introduction

Le but des travaux présentés dans cette communication est de fournir un cadre conceptuel permettant d'élaborer des indicateurs de risque applicables à l'évaluation d'une technologie, d'un projet d'aménagement d'infrastructure… associant plusieurs aspects de la « sécurité globale »

Nous définissons la sécurité comme « absence de risque inacceptable » (ISO CEI 51), et adoptons une définition de sécurité globale proposée par l' INHES au WISG 07: « capacité d'assurer à une collectivité donnée et à ses membres, un niveau suffisant de prévention et de protection contre les risques et les menaces de toute nature et de tout impact, d'où qu'ils viennent, dans des conditions qui favorisent le développement sans rupture de la vie et des activités collectives et individuelles ».

Nous ne traitons pas ici des risques sanitaires chroniques ou épidémiques, ni de cybersécurité.

Cette communication est fondée sur des travaux exploratoires de l'auteur menés à des fins de discussion technique, elle ne représente pas une position EDF concernant la gestion des risques industriels.

## 2. Partie I : Le cadre conceptuel

### 2.1 Les concepts de l'analyse de risque.

A partir d'une recherche bibliographique nous proposons les définitions suivantes des « attributs », ou « concepts » employés par les analyses de risque, à enjeu sûreté ou sécurité et les mettons en relation dans un « cadre conceptuel » commun : Scénario, Danger: Menace, Intensité, Alea, Enjeu, Vulnérabilité, Conséquence, Risque [5][6][4][2].

*Scénario* : succession (liens de causalité) et combinaison (corrélations) d'événements. Comme le nombre de scénarios possibles est énorme, les chaînes d'événements sont regroupées en scénarios de référence, moyens ou de pire cas, pouvant être ensuite quantifiés voire probabilisés. Une attaque est une forme de scénario.

*Danger* : Situation ou objet pouvant générer des dommages. Un concept équivalent est celui de "menace". [1]

*Intensité* : Caractéristique physique, dépendante du danger et du scénario (exemple : température, dose chimique, énergie thermique…).

*Alea* : Combinaison de la probabilité et de l'intensité d'un scénario. Un aléa est la probabilité conditionnelle qu'un événement donné ait une intensité donnée dans un endroit donné. Un exemple d'aléa est la probabilité d'un séisme de magnitude 5 selon l'échelle de Richter dans une région défini[2]e.

Cet indicateur est indépendant d'une présence humaine à l'endroit ou le risque se manifeste, on peut le considérer comme « objectif ».

*Enjeu* : Objet significatif pouvant être affecté par la menace. L'importance est définie par un groupe social, selon des critères "subjectifs". Un concept équivalent est celui d'"actifs". Les objectifs d'une organisation représentent un enjeu.

*Vulnérabilité* : Sensibilité à un risque d'un groupe social ou d'un système technique. Ce concept a son origine dans la défense et la cybersécurité.[3]. Il s'est étendu à la gestion des catastrophes naturelles. Il est complémentaire des concepts de résilience, robustesse qui représentent la capacité d'un groupe social ou d'un système technique à surmonter une crise ou un risque. La vulnérabilité d'un groupe social ou d'un système a plusieurs dimensions possibles : économique, technologique, sociale, institutionnelle et culturelle. Elle est réduite par des parades agissant à plusieurs niveaux: anticipation, mesures de protection, préparation aux situations de crises, gestion de crise, résilience, réhabilitation...

*Conséquence* : Combinaison de l'intensité d'un événement, des actifs touchés par l'événement et de la vulnérabilité du groupe social affecté. Les conséquences sont fonction de la valeur de l'enjeu, elles sont donc « subjectives », fonction de l'utilité économique ou symbolique, que le groupe social lui donne.

*Risque* : Combinaison de la probabilité d'un scénario et de ses conséquences. Des propositions récentes définissent le risque comme étant l'ensemble des incertitudes qui affectent l'atteinte des objectifs d'une organisation. Elle mène à un cadre de même structure dans lequel le concept d'incertitude remplace celui de probabilité et le concept d'objectif remplace celui d'enjeu.

A partir de ces définitions, nous proposons en figure n°1 un schéma conceptuel illustrant l'articulation des concepts entre eux. Nous déclinerons ensuite ce cadre général au risque d'accident industriel, au risque de catastrophe naturelle et au risque sécurité/malveillance en identifiant des relations de «causalité» «d'influence» ou de «corrélations» entre les éléments.

Au sujet de l'articulation des concepts, nous observons dès cette étape générale de description des couplages entre attributs. Par exemple, l'étude de l'histoire d'accidents technologiques majeurs (TMI, Bhopal, Seveso, Tchernobyl..) ou de catastrophes naturelles (Katrina, Kobe..) met en évidence le couplage entre l'enjeu (richesse économiques, population,..), la résilience (moyens de prévention et de protection, organisation de la gestion collective et privée des risques et de la crise, ampleur des conséquences, capacité de récupération après le désastre) et le contexte social, culturel et politique. Ce qui émerge ici est l'importance des vulnérabilités sociales, politiques et culturelles, en tant qu'indicateur de risque. Nous en reparlerons au moment de sélectionner des indicateurs.

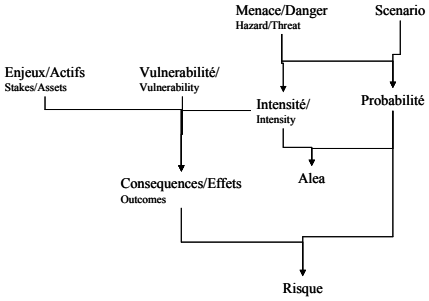


Figure n°1. Relations fondamentales entre concepts employés en analyse de risque.
Les traits continus sont des liens de cause à effet, toujours présents.

## 2.2 Le risque d'accident industriel

Nous sommes dans le domaine de la sûreté de fonctionnement[4]. Dans ce cas, le nombre de corrélations est limité et il n'y a pas d'influence mutuelle entre le danger et la vulnérabilité: le graphe est acyclique. Les scénarios peuvent être évalués par des combinaisons de probabilités conditionnelles (exemple : probabilité d'un initiateur, probabilité de succès d'une parade…). Les probabilités peuvent présenter des incertitudes dues à la

[1] Certaines sources définissent le risque comme étant une « matérialisation du danger » ou « l'exposition d'une cible à un danger ». Ces définitions ne sous semblent pas appropriées.

[2] Alea et intensité sont particulièrement employés pour les risques naturels

[3] Défini comme une erreur ou une faiblesse dans une conception. La menace est un adversaire motivé pour exploiter une vulnérabilité d'un système et capable de le faire. Le risque est la vraisemblance que la vulnérabilité sera exploitée, ou qu'une menace se manifeste. (d'après Vicky Bier, SRA).

[4] Définie par l'ISO comme un ensemble des propriétés qui décrivent la disponibilité et les facteurs qui la conditionnent: fiabilité, maintenabilité et logistique de maintenance. Il est intéressant de l'élargir à la propriété d 'un *système* telle ses utilisateurs puissent placer une *confiance justifiée* dans le service qu 'il leur délivre (LAAS)

variabilité intrinsèque des phénomènes ou dues au manque de retour d'expérience, mais il n'y a pas de difficultés fondamentales pour identifier les sources de danger et identifier les scénarios. Les démarches de représentation du risque employées dans ce domaine sont de type «causes-effets » avec des méthodes graphiques (arbres d'évènements), et une estimation limitée des «couplages »[5] entre éléments.

L'analyse est faite dans les plans physique et « informationnels » : des modèles physiques sont employés pour évaluer le danger et les conséquences, ces dernières en général de façon moins détaillée ; les actions humaines sont en grande partie définies et encadrées par des procédures, les possibilités d'erreur et de récupération sont bornées, ce qui permet pour les systèmes les plus critiques une représentation quantitative du facteur humain. Les opérateurs dévient par rapport à des procédures dans un champ du possible assez limité, leur « vision du monde »[6] est homogène [8].

Les règles de hiérarchisation nécessaires à la décision et à la gestion des risques sont du type coût bénéfice ou coût avantage.

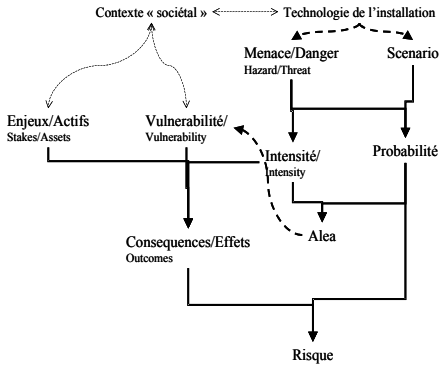


Figure n°2. Cadre conceptuel de l'analyse de risque appliquée aux accidents technologiques. Les lignes continues indiquent des relations de cause à effet entre éléments pris en compte par les analyses de risque pour ce cas. Les lignes pointillées indiquent des « couplages » plus ou moins pris en compte.

La technologie de l'installation a une influence prépondérante et elle détermine la nature du danger et les scénarios, qui sont couplés. Il existe d'autres couplages possibles, mais ils ne sont pas pris en compte dans les études de sûreté de fonctionnement. Par exemple, l'aléa peut, dans certains contextes réglementaires, impacter dans un sens favorable l'enjeu et la vulnérabilité par des règles d'urbanisme éloignant l'enjeu des zones dangereuses. Nous pourrions aussi faire l'hypothèse que le contexte social, politique et culturel peut interagir avec une technologie et être influent sur le scénario de l'accident [3][2]. En d'autres termes, probabilités, vulnérabilité et enjeu sont faiblement couplés dans le cas du risque industriel.

## 2.3 Le risque de catastrophe naturelle

L'analyse du risque emploie des modèles physiques pour évaluer le danger et les conséquences, et des estimations des fréquences des évènements redoutés en général fondés sur des statistiques. Les méthodes cause effet et probabiliste de la sûreté de fonctionnement sont peu employées, sauf dans les quelques cas ou il y a besoin d'estimer des fréquences d'initiateurs technologiques. les scénarios sont complexes en terme de phénoménologie, mais souvent assez simple en terme de combinaison d'éléments.

L'analyse est donc faite dans le plan physique, les représentations des facteurs humains sont peu employées, l'homme a un rôle réduit dans le scénario, que ce soit en tant que source d'erreur ou barrière de défense. Les règles de hiérarchisation nécessaires à la décision et à la gestion des risques sont du type coût bénéfice ou coût avantage.

Le cas de défaillance d'infrastructure serait une combinaison du cas du risque naturel (de par l'interaction entre l'infrastructure et son environnement) et du risque industriel (la représentation de l'infrastructure est du ressort des outils habituels de la sûreté de fonctionnement).

Par rapport au cas du risque industriel, nous observons des couplages plus nombreux et significatifs entre vulnérabilité, menace et enjeu. Par exemple, la présence d'un risque naturel chronique dans une région (inondation, région sismique, passage fréquent de tempêtes, feux de foret …) a une influence sur l'habitat et l'activité économique (enjeu) et parfois sur sa capacité à gérer une crise (vulnérabilité). Réciproquement, dans certains cas, l'enjeu a un effet sur le scénario. Par exemple, le développement urbain a une influence sur le comportement d'un bassin hydraulique et peut augmenter à la fois le risque de crue et l'ampleur des conséquences.

Une autre différence majeure est la présence de phénomènes dynamiques d'évolution du danger (évolution d'un bassin fluvial, changement climatique, croissance végétale, habitat en évolution…) qui influencent la menace, les scénarios et la vulnérabilité. La mise à jour des analyses est rendu difficile de ce fait.

[5] Nous désignons dans cet article sous le terme « couplage » un ensemble de relations différentes de relations causes-effet : corrélations, influences, causes communes, mode communs, interdépendances….

[6] Dans cet article, nous désignons sous ce terme la culture, l'imaginaire, l'implicite, l'informel….en complément à l' »informationnel », qui désigne les données, les procédures, la formation…

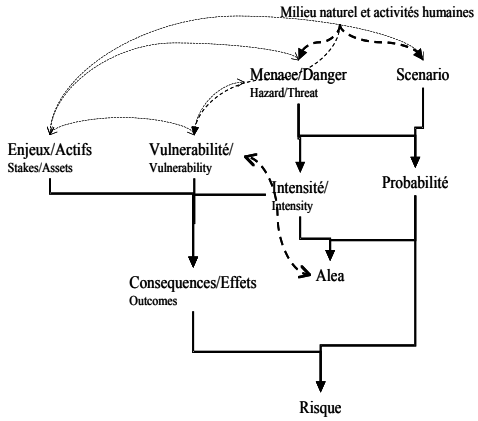


Figure n°3. Cadre conceptuel de l'analyse de risque appliquée aux catastrophes naturelles. Les lignes continues indiquent des relations de cause à effet entre éléments pris en compte par les analyses de risque pour ce cas. Les lignes pointillées indiquent des « couplages » plus ou moins pris en compte..

## 2.4 Le risque sécurité/malveillance

L'ampleur de ce risque pour les sites industriels pourrait être significatif . L'analyse des accidents industriels répertoriés en France par la base BARPI montre qu'environ 8% des sinistres sont attribués à la malveillance, mais il est possible que la proportion soit beaucoup plus élevée, une partie des 30 à 40% des accidents restant inexpliqués pouvant aussi être attribuée à la malveillance [14].

Par rapport aux deux cas précédents, le caractère volontaire, réfléchi et prémédité de l'acte de malveillance implique d'une part une interaction continue entre menace, scénario, vulnérabilité, enjeu et conséquences ; et d'autre part une dynamique permanente d'évolution de la menace[7].

En effet, dans ce cas, la menace est capable d'anticipation ; elle est en interaction continue avec les défenses mises en place sur l'installation ou dans son environnement. D'une part, elle choisit ses cibles selon l' utilité qu'elle lui donne ou qu'elle pense être donnée par le groupe social qu'elle vise: militaire, économique, symbolique. D'autre part, elle considère les chances de succès qu'elle perçoit a priori de son scénario, et de l'expérience acquise par elle ou d'autre. Enfin, le « niveau de risque » qu'elle accepte de prendre, va être dépendant de sa culture et de sa situation stratégique. Ce choix est donc une combinaison complexe des informations dont dispose la menace et de sa « vision du monde ». La vulnérabilité est elle aussi dotée de réflexivité, de capacité d'apprentissage et anticipe la menace en fonction des informations dont elle dispose et de sa propre « vision du monde ».

L'analyse doit donc être menée dans le plan physique, mais aussi dans un plan « informationnel » et dans un plan « visions du monde ».

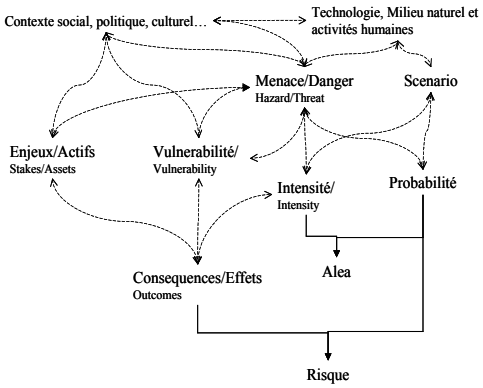


Figure n°4. Cadre conceptuel de l'analyse de risque appliquée aux actes malveillants. Des différences majeures apparaissent avec le cas de l'accident technologique. Les influences sont plus nombreuses, et mutuelles (dans les deux sens), car menace et vulnérabilité sont toutes deux capables de réflexivité et d'adaptation.

Les effets des phénomènes dynamiques d'évolution de la menace sont plus importants que dans le cas du risque de catastrophe naturelle. La connaissance et la représentation des temps de détection de l'agression, des temps de réponse des barrières, le temps d'adaptation des parades aux menaces nouvelles, doivent être pris en compte dans les études de sécurité.

Enfin, certains effets de la mise en place de barrières sont dans ce cas ambigus, à cause de la réflexivité de la menace face à la vulnérabilité. Par exemple, le renforcement des défenses protégeant des cibles voisines peut rendre une installation relativement plus attractive. Le renforcement d'un élément d'une installation par des murs met en évidence la présence d'un point vulnérable et peut attirer l'attention. La construction d'une route, d'un bâtiment etc. peuvent augmenter la visibilité d'un site…

Pour toutes ces raisons, les outils habituels de la sûreté de fonctionnement (arbres de causes, arbres d'événement, nœuds papillons, graphes de Markov..) semblent inadaptés. Premièrement, ils supposent la prédominance de liens cause-effet et le découplage entre évènements initiateurs et entre barrières. Deuxièmement, la

[7] Terme employé peut être plus couramment que danger dans ce domaine

probabilisation des scénarios d'actes malveillants est problématique, dès qu'il s'agit d'actes rares, sans données statistiques. Le champ des possibles des comportements humains dans les actes de malveillance est incomparablement plus large que dans le cas du risque humain en milieu industriel. Le domaine de la sécurité a d'ailleurs beaucoup moins développé l'emploi de calculs probabilistes évolués que le domaine de la sûreté de fonctionnement. De ce fait, la sécurité repose sur des analyses « déterministes » (barrières de défenses successives supposées efficaces et complémentaires) complétées par des systèmes de management, des procédures spécifiques, etc.

Enfin, à cause de la difficulté d'estimer les probabilités d'occurrence des actes de malveillance majeurs, et à cause de la difficulté d'estimer l'utilité des conséquences potentielles pour la menace, la hiérarchisation nécessaire à la décision et à la gestion des risques dans le domaine de la sécurité à base d'analyse type « coût bénéfice » et « coût –efficacité » est très difficile ; et il n'est pas sûr qu'une priorisation des vulnérabilités suffise ou soit pertinente. Il n'y a pas à notre connaissance sur ce sujet de méthode reconnue.

Les outils de la sûreté de fonctionnement peuvent être employés utilement pour une partie de l'analyse sur le plan physique, mais à condition d'être intégrés dans un cadre plus large, englobant une représentation de l'adaptation mutuelle et continue menace/vulnérabilité selon trois approches : physique (quelles parties du système sont vulnérables ?), informationnelle (quelles données disponibles aux deux parties ?) et représentation du monde (quelles visions du monde vont orienter les priorités de chaque partie ?). L'articulation pluridisciplinaire solide entre les approches reste à imaginer.

# 3. Partie II : Un exemple d'application.

## 3.1 La question posée.

Dans le cadre d'un étude prospective, la question posée est d'identifier des indicateurs de risque permettant de comparer des filières technologiques de transport d'énergie à l'horizon 2040, les décisions faites sur ce domaine ayant des impacts à très long terme. Cette question a été posée par exemple dans le cadre du projet européen NEEDS (6emePCRD,[11]).

Nous avons vu l'importance du contexte social, au sens large, sur trois aspects de la sécurité globale. Or, la difficulté est que nous n'avons pas d'idée de ce contexte en 2040, en particulier des attentes et des représentations risques [7][9], des européens à ce moment là. La question posée nous mène de façon assez paradoxale, à considérer des indicateurs prenant en compte le contexte, tout en intégrant le moins possible de notions « subjectives » et évolutives telles que des coûts, des utilités, des représentations des risques….

## 3.2 Représentation du système.

Le niveau d'analyse et de décision est celui de l'Union Européenne dans son périmètre actuel, sachant que quelques variantes pourraient être faites sur le périmètre européen en 2040.

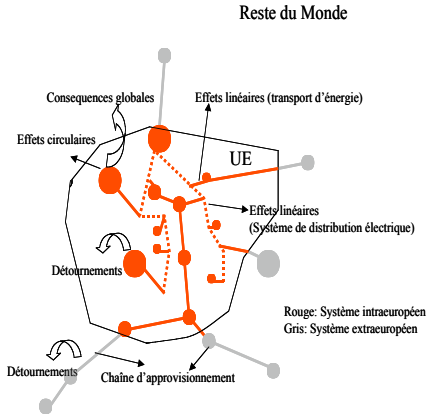


Figure n°5: Le système étudié. Il s'agit d' une infrastructure de transport d'énergie (sous forme d'électricité, de fluide, de gaz, mixte…) distribuant dans le périmètre de l'Union Européenne, supportée par une chaîne d'approvisionnement globale... Elle est formée de « nœuds » (installations de stockage, conversion, production extraction) qui ont des effets dits « circulaires » et des « routes » de transport ayant des effets dits « linéaires ». Pour certaines filières, une partie du réseau se situe hors de l'Union Européenne.

Nous retenons comme niveau de décomposition minimal pour cette application, la région, au sens administratif de chaque nation, considérant qu'à l'horizon 2040, les anticipations à un niveau inférieur sont trop incertaines. Les indicateurs de risque vont être quantifiés au niveau de l'Union Européenne, et au delà pour les risques concernant la chaîne d'approvisionnement.

Pour comparer des infrastructures qui seront en pratiques des combinaisons de technologies variées, par exemple, réseau hydrogène + éoliennes, nucléaire + gaz, etc…il faut élaborer une sorte d' « unité de compte » (énergie produite, énergie transportée…), que nous nommons ici EPU (Equivalent Production Unit) ou ETU (Equivalent Transport Unit)

Les indicateurs de risque sont alors calculés pour une unité de compte.

Dans cet exemple, l'évaluation des indicateurs de risque, se fait pour une EPU de 250 MW. Nous allons donc comparer par exemple, le risque global généré par 10 éoliennes de 25 MW ou une centrale gaz de 250 MW ou

une « demi » centrale charbon fluidisé de 500 MW et leurs chaîne d'approvisionnement équivalentes associées.

## 3.3 Choix des indicateurs de risque

Le cadre conceptuel présenté en première partie permet d'identifier quatre familles d'indicateurs. L'idée est de retenir des indicateurs répondant à la question posée et prenant en compte la contrainte de représenter le contexte sans intégrer de notions « subjectives ». Nous proposons ici une liste d'indicateurs, extraite d'une liste beaucoup plus large [10][11], respectant la double contrainte d'absence de connaissances exactes sur le société européenne en 2040 et de prise en compte du contexte, sans se limiter à des indicateurs associés au seul aléa, trop peu informatifs. Cette liste évite de trop spéculer sur les préférences des populations futures, en ne conservant que quelques fondamentaux sur lesquels les incertitudes sont limitées, comme les ordres de grandeurs de densités de population moyennes sur des régions, les longueurs des lignes d'approvisionnement, les impacts matériels...

### 3.3.1 La probabilité n'est pas un indicateur pour comparer des technologies

Nous excluons dès ce niveau de l'analyse la probabilité en tant qu'indicateur. Nous considérons d'abord que, dans le cas de risques majeurs et rares, elle est un objectif de conception, une incertitude sur une objectif de zéro accident, plutôt qu'une valeur prévisionnelle de ce qui va se passer réellement.

Pour des technologies futures, nous proposons de considérer que la probabilité est une donnée de sortie, orientée sur les tendances historiques des technologies en matière de sûreté, que l'on peut toujours atteindre, moyennant des moyens économiques (un « consentement à payer »). Autrement dit, nous faisons l'hypothèse que, dans l'Europe des années à venir, les capacités technologiques permettront d'ajuster la probabilité à un niveau déterminé par les conséquences, et c'est le prix à payer pour cela qui fera la viabilité de la technologie. La probabilité n'est donc pas un élément de comparaison de technologies.

Enfin, de point de vue de la décision, l'emploi d'indicateurs de probabilité pour des situations rares pose le problème de la combinaison d' une probabilité faible et d' une gravité élevée qui correspond à une proposition souvent indécidable.

## 3.4 Indicateurs associés aux dangers

Ils peuvent être représentés par exemple, dans le cas de risques technologiques, par une quantité d'énergie libérable lors d'un accident (sous forme d'une combinaison d'énergie thermique, mécanique) ou d'un potentiel toxique, en situation normale, ou accidentelle. Ces indicateurs sont fonction de la source du danger, du scénario, et indépendants du lieu et de la date. Nous proposons ici de considérer des scénarios moyens. Tous les indicateurs sont ramenés à une EPU ou une ETU (cf 3.2)

### 3.4.1 « Globalité »[8] des conséquences suite à un accident grave ou à des effets chroniques.

- Argument: Quelle que soit la capacité économique et technologique d'une société future à surmonter les conséquences d'accidents, il sera plus difficile de gérer des conséquences globales, à l'échelle d'un continent ou du monde, que des conséquences locales. Les conséquences globales possibles sont l'émission de gaz à effet de serre, la diffusion de pollution dans les océans, la pollution diffuse le long d'une chaîne logistique lors du transport. Les études d'accidents, les études d'impacts, les modèles de dispersion, les analyses de cycle de vie peuvent être emplois pour évaluer l'ampleur des effets globaux.
- Quantification: Pour cet exemple simplifié, un indicateur binaire (oui/non) est employé: **Potentialité d'effets globaux**

### 3.4.2 Irréversibilité des conséquences suites à un accident grave ou à des effets chroniques.

- Argument: Quelle que soit la capacité économique et technologique d'une société future à surmonter les conséquences d'accidents, il sera plus coûteux de gérer des conséquences ayant des durées indéfinies que des conséquences à échéance prévisible. Nous considérons ici qu'un effet est irréversible s'il faut plus d'une vie humaine pour réduire son activité à 10% de son niveau initial. Nous considérons ici une durée de vie humaine de 75 ans.
- Quantification: Pour cet exemple simplifié, un indicateur binaire (oui/non) est employé: **Potentialité d'effets irréversibles**.

### 3.4.3 Potentialité de détournement de matière à des fins malveillantes

- Argument: Quelles que soient les motivations des actes malveillants potentiels et la stabilité politique future des sociétés européennes, une infrastructure employant ou générant des matières ayant un potentiel explosif ou NRBC significatif sont plus coûteuse à gérer que les autres. Il sera toujours possible d'éviter le détournement de matière, mais à un coût peut être important. L'analyse du cycle de vie permet d'obtenir des indications, sur la présence de produit en quantités suffisantes.
- Quantification:. Nous ne considérons dans cet exemple que la quantité en équivalent TNT produite ou consommé, sans évaluer la difficulté pour le faire. Pour cet exemple simplifié, un indicateur binaire (oui/non) est employé : **Présence en quantité significative de matières ayant un potentiel explosif**

[8] continentales, mondiales

## 3.5 Indicateurs associés à l'enjeu

Ce sont les biens à protéger, les objectifs pour lesquels le groupe social se mobilise ; ils peuvent être matériels (production agricole et industrielle, biodiversité locale, valeur foncière et immobilière, revenus des activités touristiques) ou immatériels (indices de développement humain, lieux symboliques. …). Les valorisations que l'on peut en faire sont dépendantes du contexte social et économique et sont influencées par les hypothèses faites sur le futur. Dans notre proposition de retenir des indicateurs les moins dépendants du contexte possible, nous ne retenons finalement que le nombre d'habitants dans la zone exposée au risque.

### 3.5.1 Personnes exposées aux conséquences des accidents graves

- Argument: Quelle que soit la capacité économique et technologique d'une société future à surmonter les conséquences d'accidents graves (ayant des impacts hors des périmètres des installations), il sera d'autant plus difficile de gérer les conséquences que le nombre de personnes exposées au danger est important. Il est tout à fait concevable que les sociétés sauront à l'avenir de traiter les conséquences sanitaires des effets chroniques ou accidentels, mais cela aura quand même un coût économique et social.
- L'hypothèse est que la répartition globale et les densités moyennes de population en Europe au niveau des régions ne vont pas changer de façon significative sur les 40 prochaines années.
- Quantification. Cet indicateur représente l'ensemble des conséquences au niveau local des effets accidentels.
- **Nombre moyen de personnes pouvant être affectées par les effets accidentels à proximité des noeuds et le long des routes de la chaîne d'approvisionnement (cf formule en annexe).**

### 3.5.2 Nombre de personnes pouvant être affectées par les risques chroniques.

- Argument: Quelle que soit la capacité économique et technologique d'une société future à surmonter les conséquences chronique d'activités industrielles, il sera d'autant plus difficile de gérer des conséquences que le nombre de personnes exposées et la variété des effets sont importants. Il est tout à fait concevable que les sociétés sauront à l'avenir de traiter les conséquences des effets chroniques mais cela aura quand même un coût économique et social.
- Les risques chroniques sont causés par les rejets en fonctionnement normal ou lors des accidents mineurs. Ils sont d'ordre sanitaire (accidents du travail, effets toxique, chimique, bruit..), symbolique (dégradation des paysages…) et incluent les activités d'extraction et de transport éventuelles.
- Quantification. Cet indicateur représente l'ensemble des conséquences au niveau local des effets chroniques. On ne considère que l'effet auquel le plus de personnes sont exposées.
- **Nombre moyen de personnes pouvant être affectées par les effets chroniques à proximité des noeuds et le long des routes de la chaîne d'approvisionnement (cf formule en annexe).**

## 3.6 Indicateurs associés à la vulnérabilité

Unknown 22/11/07 15:35
**Mis en forme**

Cet attribut est très dépendant du contexte et ses indicateurs difficiles à estimer dans un cadre prospectif sans faire d'hypothèses fortes. Nous ne retenons dans cet exemple comme indicateur associé que la vulnérabilité de la chaîne d'approvisionnement.

### 3.6.1 Complexité de la chaîne d'approvisionnement globale (hors de l'UE)

La chaîne d'approvisionnement comporte par exemple une extraction, une transformation, un transport par canalisation, un transfert sur navire, un transfert dans des réservoirs, puis un transport par canalisation…

- Argument: L'idée est qu'une chaîne d'approvisionnement est d'autant plus vulnérable aux risques accident, catastrophe naturelle et malveillance qu'elle traverse des pays nombreux et qu'elle comporte de nombreuses ruptures de moyens de transports ou des stockages intermédiaires. Une chaîne vulnérable pourra toujours être sécurisée, mais cela a un coût économique et politique pour l'UE (dépenses de défense, diplomatique, aide au développement…).
- Quantification. L'indicateur de complexité proposé intègre la longueur de la chaîne, les ruptures de chaînes (frontières, transferts…). Lorsqu'une technologie peut employer plusieurs routes en parallèle, on considère la plus complexe parmi celles qui représentent plus de 10% de l'energie transportée. L'idée est de considérer qu'une perturbation sur 10¨% de l'approvisionnement suffit pour impacter l'ensemble de l'économie de la filière technologique. Cet indicateur requiert de faire des hypothèses sur les chaînes qui seront employées en 2040 par l'EU selon la technologie.

- **Indice de complexité de la chaîne d'approvisionnement hors CE= $\Sigma$ (Li *Ni)**

Avec

- Li: longueur de la route de type i en milliers de km (route terrestre, voie maritime, canalisation, ligne électrique…)
- Ni = Nombre de ruptures de chaîne (passage d'y=un type i à j) sur la route i (port, dépôt, usine de transformation..)

# 4. Exemple de calcul d'indices de risque

## 4.1 Calcul d'un indice de risque pour un élément d'infrastructure

Nous considérons ici le cas d'une turbine à combustible (gaz naturel) de 250 MW.

- Potentiel de conséquences globales lors d'accidents: Non (émissions marginales de gaz à effet de serre)
- Potentiel de conséquences globales en situation normale: Oui (émissions significatives de gaz à effet de serre)
- Potentiel d'effets irréversibles à l'échelle d'une vie humaine: Non
- Potentiel d'emploi matière à des fins malveillantes: pas significatif.
- Indicateur d'exposition de personnes à des conséquences d'accidents majeurs: 2 (selon formule en annexe)
- Indicateur d'exposition de personnes à des effets chroniques: 107 (selon formule en annexe)

## 4.2 Application à la comparaison entre trois technologies

La comparaison est faite à partir des indicateurs, en classant les technologies par rang (cf. tableau n°1). Trois technologies, notées A, B et C sont comparées au niveau d'une EPU .

Une technique d'agrégation des indicateurs peut ensuite être employée pour évaluer un indicateur de sécurité globale. Une façon simple consiste à faire une moyenne pondérée des rangs, avec des poids ai tels que $\Sigma$ai =1. La difficulté est que l'agrégation implique une hypothèse de la part des décideurs actuels au nom des générations futures. Des hypothèses doivent donc être explicitées, éventuellement plusieurs « visions du futur » sont à élaborer. Nous proposons de considérer qu'en l'absence d'hypothèse, les nœuds sont égaux sur chaque critère : ai= 1/N (N = nombre d'indicateurs).

| | Rang [9] | | |
|---|---|---|---|
| Indicateur | A | B | C |
| Conséquences globales (accident) | 1 | 1 | 3 |
| Conséquences globales (en fonctionnement) | 3 | 1 | 1 |
| Potentiel d'effets irréversibles | 1 | 1 | 3 |
| Potentiel d'emploi matière à des fins malveillantes | 1 | 1 | 3 |
| Indice du nombre de personnes exposées à des conséquences d'accidents majeurs (nœuds) | 2 | 1 | 3 |
| Indice du nombre de personnes exposées à des effets (en fonctionnement (nœuds) | 2 | 3 | 1 |
| Indice du nombre de personnes exposées à des conséquences d'accidents majeurs (routes) | 3 | 1 | 2 |
| Indice du nombre de personnes exposées à des effets (en fonctionnement (routes) | 3 | 1 | 2 |
| Indice de complexité de la chaîne d'approvisionnement. | 3 | 1 | 2 |

[9] (1: technologie ayant l'indice de risque le plus faible sur les trois, 3: technologie ayant l'indice de risque le plus fort sur les trois).

Tableau n°1. Rang des indicateurs de risques obtenus par les technologies A,B et C.

## 4.3 Application à la comparaison de trois infrastructures

En réalité, quelle que soit la décision prise, l'infrastructure complète sera une combinaison de technologies. Nous proposons ci une comparaison entre trois infrastructures, des combinaisons des technologies A,B,C, appelées Mix X, Y et Z.

| | Mix X(%) | Mix Y (%) | Mix Z (%) |
|---|---|---|---|
| Technologie A | 80 | 0 | 0 |
| Technologie B | 0 | 50 | 100 |
| Technologie C | 20 | 50 | 0 |

Tableau n°2. Exemples de combinaisons des technologies

La comparaison est faite à partir des indicateurs, de chaque technologie A,B,C en classant les technologies par rang (cf. tableau n°3).Pour les indicateurs binaires, on retient le pire cas de chaque combinaison, pour les indicateurs quantifiées en nombre de personne exposées ou en complexité, on pondère par le poids de chaque technologie de base dans la combinaison.

| Criteria | Mix A | Mix B | Mix C |
|---|---|---|---|
| Conséquences globales (accident), Conséquences globales (en fonctionnement), Potentiel d'effets irréversibles, Potentiel d'emploi matière à des fins malveillantes, indice de complexité de la chaîne d'approvisionnement | Pire cas entre A et C | Pire cas entre A et C | Pire cas entre A et C |
| Indice du nombre de personnes exposées à des conséquences d'accidents majeurs (nœuds), exposées à des effets (en fonctionnement (nœuds), à des conséquences d'accidents majeurs (routes), à des effets (en fonctionnement (routes) | =0.8* EPU A + 0.2* EPU C | =0.5* EPU B+ 0.5* EPU C | = EPU B |

Tableau n°3. Règles employées pour évaluer les critères d'une combinaison de technologies

| | Rang [10] | | |
|---|---|---|---|
| Indicateur | Mix X | Mix Y | Mix Z |
| Conséquences globales (accident) | 3 | 1 | 1 |
| Conséquences globales (en fonctionnement) | 1 | 2 | 3 |
| Potentiel d'effets irréversibles | 3 | 1 | 1 |
| Potentiel d'emploi matière à des fins malveillantes | 3 | 1 | 1 |
| Indice du nombre de personnes exposées à des conséquences d'accidents majeurs (nœuds) | 2 | 1 | 3 |
| Indice du nombre de personnes exposées à des effets (en fonctionnement (nœuds) | 1 | 2 | 3 |
| Indice du nombre de personnes exposées à des conséquences d'accidents majeurs (routes) | 1 | 2 | 3 |
| Indice du nombre de personnes exposées à des effets (en fonctionnement (routes) | 1 | 3 | 2 |
| Indice de complexité de la chaîne d'approvisionnement. | 1 | 3 | 3 |

Tableau n°4. Rang des indicateurs de risques obtenus par les combinaisons de technologies X,Y et Z.

Une technique d'agrégation des indicateurs peut ensuite être employée pour évaluer un indicateur de sécurité globale (cf 4 .2.).

## 5. Conclusion

Dans cette communication, nous avons tenté de montrer les différences entre les approches « sûreté » et « sécurité » d'un système industriel au niveau des concepts mobilisés.

Nous avons proposé en première partie un "cadre conceptuel" reliant des concepts employés pour plusieurs types d'analyses de risque, permettant de représenter les particularités du risque technologique, du risque naturel, du risque malveillance et de les comparer. Ce cadre nous permet de mettre en évidence les différences fondamentales entre ces trois aspects de las sécurité globale, et la difficulté à utiliser les techniques d'analyse du risque d'un domaine à un autre, tout en mettant aussi en évidence l'intérêt qu'il y a à le faire.

[10] 1: technologie ayant l'indice de risque le plus faible sur les trois, 3: technologie ayant l'indice de risque le plus fort sur les trois.

La gestion du compromis entre performance des barrières de sûreté et performance économique d'une installation industrielle est aujourd'hui un sujet de recherche. Il serait appelé à se renforcer, si la sécurité devient un enjeu sociétal caractérisé par un niveau de pression réglementaire comparable à celui de la sûreté. Or, notre analyse tend à montrer que la compatibilité entre ces objectifs n'est pas acquise [15], mais pas exclue [16], et qu'elle requiert des connaissances et des méthodes d'analyse qui restent à développer.

Des problèmes particuliers de prise de décision émergent. Par exemple, l'affectation des ressources nécessaires aux parades doit-elle être hiérarchisée par la menace (probabilité d'acte malveillant), par la vulnérabilité (sensibilité d'un enjeu au risque) ou par le risque (produit de la probabilité et des conséquences) ? Existe-t-il une « aversion au risque de malveillance» ? Est-elle de même nature que celle relative aux risques d'accidents et aux risques chroniques ?

Les outils de la sûreté de fonctionnement peuvent être employés utilement pour l'analyse de risque, notamment sur le plan physique, mais à condition qu'ils soient intégrés dans un cadre plus large, englobant une représentation de l'adaptation mutuelle et continue menace/vulnérabilité selon trois approches : physique (quelles parties du système sont vulnérables ?), informationnelle (quelles données disponibles aux deux parties ?) et représentation du monde (quelles visions du monde vont orienter les priorités de chaque partie ?). Cependant, une articulation pluridisciplinaire solide reste à imaginer. Les particularités d'une analyse de risque orientée « sécurité globale » nous incitent à investiguer sur plusieurs domaines : sciences humaines et sociales, avec notamment les approches socio-organisationelles, la sociologie de la violence, la théorie des jeux, la modélisation des interdépendances, l'économie du risque, les approches mathématiques, avec les outils possibilistes et bayésiens, sortant su champ des probabilités habituellement employées dans les analyse techniques, ou bien les approches de sûreté de fonctionnement non probabilistes….

Réciproquement des progrès dans la représentation du risque de malveillance permettraient d'enrichir les analyses de risques industriels, naturels et liés à la défaillance de grandes infrastructures, en mettant plus en évidence l'influence du contexte sociétal et naturel sur les scénarios et la vulnérabilité. Les travaux permettraient d'établir des liens entre risque industriel, risque naturel, malveillance, défaillance de grandes infrastructures.

En seconde partie, nous avons appliqué le cadre conceptuel avec une finalité particulière, pour définir des indicateurs de « sécurité globale » sur une infrastructure technique.

Après une discussion sur le choix d'indicateurs, nous en proposons une série adaptée pour illustrer une question particulière ayant une dimension prospective.

Nous identifions les effets globaux, les effets irréversibles, les effets circulaires et les effets linéaires, ainsi que la vulnérabilité de la chaîne

d'approvisionnement. Ces indicateurs permettent la comparaison de filières technologiques, moyennant des hypothèses à faire sur l'anticipation des préférences des générations futures face à des risques varies.

Ces travaux sont des premiers jalons vers un possible indicateur de "sécurité globale" permettant de comparer des technologies ou des infrastructures critiques dans un cadre prospectif.

## 6. Remerciements.

L'auteur remercie Ludovic Pietre Cambacedes (EDF R&D) pour sa relecture attentive de l'article et nos discussions enrichissantes sur les liens sécurité-sûreté.

## 7. Annexe : Exemple de formules de calcul pour les indicateurs

Quatre indicateurs correspondent aux effets linéaires et circulaires causes par les installations (site d'extraction, de stockage, de transformation) et les lignes d'approvisionnement. Les effets chroniques sont dus aux pollutions locales, au bruit, aux effets esthétique, les effets accidentels aux explosions, nuages toxiques survenant lors d'accidents majeurs

- nombre de personnes exposées à des conséquences circulaires en fonctionnement normal = $Sup(i)\ \Sigma\ (j)\ (3,14*RNi^2*kij*dj)\ j=1,N,\ i=1,I$
- nombre de personnes exposées à des conséquences circulaires accidentelles = $Sup(i)\ \Sigma\ (j)\ (3,14*RA1ij^2*d*0,1 + 3,14*(RA2^2-RA1^2)*d*0,01)\ j=1,N$
- nombre de personnes exposées à des conséquences linéaires chroniques = $Sup(i)\ \Sigma\ (j)\ (Lj\ *RNij*kij*dj)\ j=1,N';\ i=1,I$
- nombre de personnes exposées à des conséquences linéaires accidentelles = $Sup(i)\ \Sigma\ (j)\ (Lj\ *RNij\ *dj*0,1 + Lj*(RNij\ –RA1ij)*dj*0,01)\ j=1,N'$

Avec:

- N, N' : Nombre d'installations et de chaînes d'approvisionnement nécessaires à une Unité de Production Equivalente (EPU)
- I : Nombre d'impacts possibles en situation, accidentelle ou en fonctionnement normal. Par exemple, pollution chimique, bruit, thermique, pression..)
- RNij Rayon d'effet de l'impact type i de la source j en fonctionnement normal. Par défaut, RNij = 500 m
- kij : Proportion d'habitants affectés par l'impact i de la source j en fonctionnement normal. Par défaut kij= 0,1
- dj : densité de population dans la région d'implantation de l'installation ou traversée par la route j (valeur moyenne).
- RA1ij : Distance conventionnelle correspondant à une moyenne de 10% de victimes pour le scénario considéré
- RA2ij : Distance conventionnelle correspondant à une moyenne de 1% de victimes pour le scénario considéré
- Lj: longueur de la route d'approvisionnement j.

## Références

[1]. Socioeconomic vulnerability and adaptation to environmental risk: a case study of climate change and flooding in Bengladesh, R. Brouwer et al., Risk Analysis, pp 313-326, vol 27, N°O 2, 2007.

[2]. Vulnérabilité et risques, l'approche récente de la vulnérabilité, Yvette Veyret, Magali Reghezza, in Responsabilité et environnement, pp 9-13 Juillet 2006, n°23.

[3]. Indicators of disaster risk and risk management. Inter American development bank. Universidad nacional de Colombia, instituto de estudios ambientales, January 2005.

[4]. INERIS, Course on hazard analysis, Mars 2006.

[5]. ISO/CEI 73 Risk terminology

[6]. ISO/CEI 51 Aspects liés à la sécurité : principes directeurs pour les inclure dans les normes

[7]. Sociologie du risque, Patrick Perretti Watel, 2006, Armand Colin

[8]. La conduite de systèmes à risques. Amalberti R., Le Travail Humain. 1996, Paris : PUF.

[9]. Social Theories of risk, Part II, S. Krimsky, D.Golding, editors, Prager, 1992

[10]. Stefan Hirschberg "Preliminary Environmental, Economic and Social Criteria and Indicators for MCDA (RS2b)", 13 June 2006

[11]. Human Development Report 2006, ISBN 0 230 50058 7NEEDS INTEGRATED PROJECT New Energy Externalities Developments for Sustainability, Internal Paper - RS 2b, WP7 *"Risk Indicators proposal based on an analytical framework",* G Deleuze

[12]. Flexibility in the Face of Disaster: Managing the Risk of Supply Chain Disruption. Paul R. Kleindorfer. September 06, 2006 in Knowledge@Wharton

[13]. Accident Epidemiology and the U.S. Chemical Industry: Preliminary Results from RMP. Paul R. Kleindorfer, Harold Feldman, Robert A. Lowe, Working Paper 00-01-15. Center for Risk Management and Decision Processes,Wharton School, University of Pennsylvania. February 3, 2000

[14]. Liens entre sûreté et sécurité : un nouveau champ de recherche ? G Deleuze, E Chatelet, P Laclémence, communication au 1er congrès Institut du Management des Risques-Institut Européen des Cindyniques, Décembre 2007.

[15]. Les paradoxes de la sécurité industrielle, nouveaux champs de recherche, G Deleuze, E. Chatelet, L. Pietre Cambacedes, P Laclémence, communication WISG07, Février 2007.

[16]. Why safety and security should and will merge. A. Pfitzmann, TU Dresde, SAFECOMP 2004, Springer Verlag 2004.