L'analyse intégrée des risques au profit des systèmes socio-techniques en lien fort avec l'environnement

Carole Duval, Geoffrey Fallet-Fidry, Alain Sibler, Benoît Iung

L'analyse intégrée des risques au profit des systèmes socio-techniques en lien fort avec l'environnement

Auteurs : DUVAL, Carole[1] – FALLET-FIDRY Geoffrey [1,2] – SIBLER Alain [1] – IUNG Benoît [2]

[1] EDF-R&D, Département 'Management des Risques Industriels'
1, avenue du Général de Gaulle 92141 Clamart Cedex
Tél. : 01 47 65 46 92
Fax : 01 47 65 51 73
Email : carole.duval@edf.fr, alain.sibler@edf.fr

[2] CRAN – Université de Lorraine – UMR 7039 CNRS– Campus Sciences – BP 70239 – 54506 Vandoeuvre
Tél. : 03 83 68 51 27
E-Mail **:** benoit.iung@cran.uhp-nancy.fr, geoffrey.fallet@edf.fr

Résumé

Depuis moins de dix ans, le contexte européen en gestion des risques industriels évolue et propose des agendas d'actions qui mettent en avant la nécessité de faire progresser la connaissance tant sur les phénomènes dangereux que sur les approches pour étudier ces phénomènes plus spécifiquement dans une vision système. Certains cadres de gestion de risques adressent plus précisément les systèmes socio-techniques complexes fonctionnant sous contraintes environnementales et soumis à des risques multiples. En effet, l'environnement physique et réglementaire influence fortement les différents enjeux d'un système socio-technique, sa performance et aussi sa sûreté. Cependant ces systèmes ne peuvent être étudiés comme un ensemble de sous-systèmes indépendants de par leur complexité et par conséquent, l'analyse de risques classique ne leur est pas applicable. Il est nécessaire de développer des analyses de risques couvrant globalement tous les risques dans une même vue à partir des modèles systèmes (fonctionnels, organisationnels,…), leur maintien dans la durée, le rôle potentiel de la maintenance, les actions humaines…

Par rapport à ce besoin, EDF qui manage des systèmes socio-techniques complexes de production d'énergie a proposé une approche d'analyse intégrée des risques (nommée AiDR) en phase avec cette vision globale. L'approche intégrée des risques fait le lien entre plusieurs disciplines (la sûreté de fonctionnement, la fiabilité humaine, l'analyse organisationnelle) et est conçue pour développer des méthodes et des outils permettant de réaliser une analyse de risques innovante de ces systèmes complexes. Par conséquent, ce papier présente les principes fondateurs de cette approche et met en évidence son intérêt sur le cas d'un sous système critique d'une unité de production d'énergie : une Source Froide.

Summary

For less than a decade, the European context evolves in order to propose frameworks enabling to improve knowledge of both hazardous events and systemic analysis. Some frameworks are addressing more precisely socio-technical systems considered as complex systems operating under environmental constraints and for which multiple risks can occur. Indeed, the physical environment and the regulatory one influence strongly the different stakes of a socio-technical system mainly its availability but also its safety. Nevertheless as these systems cannot be studied like a set of independent sub-systems due to complexity, the conventional risk analysis is not applicable to them. It is required to develop more integrated risk analysis covering globally all the risks in a same view taking into account system models (functional, organizational …), system life cycle phase, system environment, the potential role of maintenance, the human actions …

In relation to this context, Electricité de France (EDF), which is managing socio-technical systems dedicated to Energy Production, took the opportunity to contribute to this issue. Thus this paper is defending a "System Thinking"-based integrated risk analysis approach called IRA. IRA is covering different disciplines (i.e. Dependability, Human Reliability, and Organizational Analysis) and designed for developing methods and appropriate tools in order to support innovative risks analysis of such systems. Its main concepts and principles are demonstrated by applying them to an industrial case which is a sub-set of an EDF Energy Power Plant.

Introduction

Relativement à la problématique globale de maîtrise des risques, dans son rapport 2004 intitulé « les risques émergents au 21ème siècle » [1], l'OCDE proposait un agenda pour action qui mettait en avant la nécessité de faire progresser la connaissance tant sur les phénomènes dangereux que sur une vision globale des risques de type analyse systémique. La Commission Européenne a pour sa part lancé un appel à projet sur le management intégré des risques dans le 7ème PCRD. Parallèlement, de nombreux travaux référencés dans [2] fondent l'intérêt exprimé par un grand nombre d'industriels et de laboratoires de recherche pour la modélisation de systèmes qui deviennent de plus en plus complexes. Dans ce contexte, EDF doit faire face à des changements réglementaires qui l'orientent à traiter plusieurs risques conjointement (cas de la Directive Cadre sur l'Eau) tout en continuant d'optimiser ses systèmes de production et de transport en garantissant les enjeux de sûreté mais aussi de disponibilité et de maintien du patrimoine dans la durée. C'est pourquoi EDF a considéré que le management de ses systèmes en lien fort avec l'environnement devait être régulièrement réadapté, remis à jour …. Les analyses de risques telles que définies dans l'ISO 31000[1] sont souvent révisées. En effet, l'environnement physique et réglementaire influence fortement les différents enjeux d'un système socio-technique : principalement la disponibilité mais aussi la sûreté. Cela implique de considérer **dans une même vue** :

[1] ISO 31000:2009 (F) : Management du risque – principe et lignes directrices

- les risques affectant le système technique, les effets de l'incertain sur les enjeux comme définis dans l'ISO 31000 et définis dans l'approche AiDR proposée comme la combinaison des conséquences d'un événement avec sa vraisemblance ;
- les influences de l'environnement physique et réglementaire sur l'occurrence des risques techniques, leur probabilité d'occurrence et la gravité de leurs conséquences sur les enjeux du système étudié, considérés ensemble : la sûreté mais aussi la disponibilité pour rester compétitif en maintenant le patrimoine dans la durée ;
- l'impact potentiel des actions de maintenance et de conduite sur la défaillance des composants du système étudié, leurs impacts sur les enjeux mentionnés précédemment sachant que les actions humaines peuvent elles-mêmes être analysées dans leur contexte organisationnel si besoin.

Cette vue globale des risques considérée par ces systèmes en lien fort avec l'environnement permet de les prioriser de façon partagée entre les acteurs de l'analyse et contribue ainsi à la communication sur les risques. Cette priorisation les aide à gérer leurs risques en exploitation et à se projeter dans des horizons plus lointains prenant en compte des changements de contexte (par exemple, le changement climatique). Cette approche peut être généralisée à d'autres secteurs comme la chimie et le transport. En effet, une application en a déjà été réalisée sur une installation de stockage de produits chimiques [3] et les différents modèles de risques qui sont intégrés dans l'approche sont déjà utilisés dans ces différents secteurs (sûreté de fonctionnement technique, prise en compte de la maintenance, analyse organisationnelle d'accidents dans ces différents secteurs…). Cet article renforce cette capacité à généraliser l'approche et en fait un challenge à poursuivre.

1. Enjeux de la modélisation des risques des systèmes socio-techniques complexes

Dans ce contexte évolutif de la gestion des risques industriels, EDF/R&D développe une approche qui vise à traiter des systèmes complexes soumis à des risques de natures différentes. En effet, les méthodes développées et utilisées jusqu'à aujourd'hui pour gérer les risques sont le plus souvent sectorielles. Elles ont été réalisées jusque dans les années 70 sur le système technique seul [4], puis les interventions humaines ont été caractérisées en considérant ces actions comme sources d'erreur par assimilation aux défaillances techniques ([5], pour les systèmes de production nucléaire, modèle de Swain ou behaviorisme). Enfin, à partir des années 80, des travaux ont été menés en vue de prendre en compte ces actions dans le contexte organisationnel, l'équipe, le service, l'unité... dans lequel elles sont réalisées [7]. Depuis 2004, quelques industriels et universitaires se sont engagés pour mieux représenter les systèmes complexes. En ce sens, ce papier se réfère à Le Moigne [8] pour caractériser ces systèmes par les items suivants : ils ne sont pas décomposables, les approches de la Sûreté de Fonctionnement classique ne sont donc plus applicables, et il peut y avoir émergence du « nouveau », principalement lié au comportement humain qui peut se reconfigurer ou s'écarter des procédures dans certaines conditions incidentelles ou accidentelles. L'enjeu est de savoir traiter des systèmes socio-techniques pris dans leur environnement physique et réglementaire. Ce sont des systèmes complexes au sens de Le Moigne. L'approche développée, appelée Analyse intégrée Des Risques (AiDR), repose sur une vue de l'ensemble des risques affectant le système à la place des analyses de risques sectorielles couramment menées. L'originalité de l'approche repose sur son caractère intégré.

2. Principes de l'Analyse intégrée Des Risques

Cette nouvelle approche dite « intégratrice » entre plusieurs disciplines, la Sûreté de Fonctionnement, l'Analyse de risque, la Fiabilité Humaine, l'Analyse Organisationnelle vise à **développer les méthodes, choisir les outils adaptés et les faire évoluer pour** faire l'**analyse de risques de ces systèmes techniques** :

- en lien fort avec l'**environnement** physique et réglementaire,
- **intégrant des actions humaines** de maintenance, de surveillance et de conduite prises **dans leur contexte organisationnel**,
- en **garantissant les enjeux clés du système** : sa disponibilité prise avec sa sûreté, son maintien du patrimoine dans la durée, son impact sur l'environnement,
- **pour hiérarchiser ces risques de natures différentes vis-à-vis de ces enjeux dans le but de prioriser les moyens à mettre en œuvre pour les réduire,**
- **et contribuer ainsi à une meilleure culture du risque** [9] **et une meilleure communication sur les risques.**

La démarche développée est « à tiroirs » : elle peut couvrir deux ou trois de ces domaines ou l'ensemble suivant l'appréciation du client de l'étude et les risques suspectés. Le cadre conceptuel de cette approche (Figure 1) est fondé sur ceux développés dans l'approche SAM de Paté-Cornell et Murphy [10] qui considère que l'organisation influence les actions humaines et, par le biais de ces actions, le fonctionnement du système technique (Figure 2).

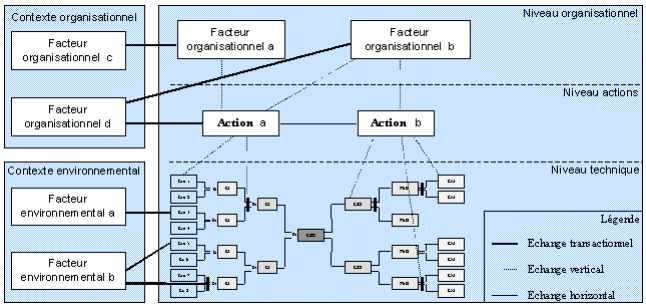

Figure 1 : Cadre conceptuel

Dans cette approche, le système est divisé en trois couches représentatives qui interagissent par le biais d'échanges horizontaux et verticaux (Figure 2) : les couches technique, humaine et organisationnelle. Ce système est ensuite influencé, par le biais d'échanges transactionnels, par des contraintes externes : les contextes de l'environnement naturel et de l'organisation [3].

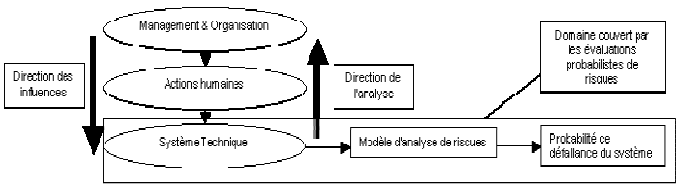

Figure 2 : Structure des effets des hommes et de l'organisation sur le risque

Ainsi, pour évaluer les risques associés à ces systèmes socio-techniques complexes, l'intégration de ses différentes dimensions dans un même modèle a été choisie. Cette intégration est possible en utilisant les connaissances particulières à chaque dimension et les relations qui les lient à travers un outil particulier : les réseaux Bayésiens. Un réseau Bayésien consiste en un graphe acyclique orienté qui permet de représenter des densités de probabilité jointes ([11], Table 1) :

$$P(A,B) = P(A/B) \times P(B) = P(B/A) \times P(A)$$

Avec : A, un événement ; B, un parent de A ; P(A,B), la probabilité jointe de l'événement ($A \cap B$) ; P(A/B), la probabilité conditionnelle de A sachant B ; P(B), la probabilité marginale de B ; P(B/A), la probabilité conditionnelle de B sachant A ; P(A), la probabilité marginale de A.

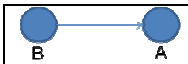		A			
		a_1	a_2	…	a_k
B	b_1	$P(A=a_1/B=b_1)$	$P(A=a_2/B=b_1)$	…	$P(A=a_k/B=b_1)$
	b_2	$P(A=a_1/B=b_2)$	$P(A=a_2/B=b_2)$	…	$P(A=a_k/B=b_2)$
	…	…	…	…	…
	b_r	$P(A=a_1/B=b_r)$	$P(A=a_2/B=b_r)$	…	$P(A=a_k/B=b_r)$

Table 1 : Table de Probabilité Conditionnelle de la variable A

Cet outil permet aussi de traiter ensemble des données qualitatives (issues de jugement d'experts) et quantitatives (taux de défaillance évalués sur la base d'un grand nombre de données) [11].

3. Les règles de modélisation

Dans cette approche ont été définies les différentes dimensions considérées dans les systèmes étudiés ainsi que la façon retenue pour unifier et intégrer les connaissances de natures associées à ces différentes dimensions.

3.1 Description des dimensions du système

Pour la dimension technique, l'approche retenue permet de (a) décrire les scénarios d'accidents en partant de leurs initiateurs jusqu'à leurs conséquences, (b) d'introduire des barrières de sécurité (barres verticales dans la Figure 1) qui permettent de réduire la probabilité d'occurrence du scénario d'accident ou de limiter ses conséquences, (c) de quantifier de façon probabiliste les risques. Elle agrège une approche déductive à travers un arbre de défaillance et une approche inductive à travers un arbre d'événements et le nœud papillon [12].

Pour la dimension humaine, le choix de l'intégration des différentes dimensions dans une même vue globale de l'ensemble des risques a impliqué le choix d'une vision simplifiée de ces aspects ([3,13]). Ainsi les actions de maintenance et de conduite sont représentées par un ensemble de caractéristiques[2] et de phases (Table 2) et leur efficacité ont une influence sur la disponibilité des barrières.

Etapes de l'action	Caractéristiques de l'action
Préparation	Délégation, Aides, Formation
Réalisation	Expérience, Capacité à respecter le cahier des charges, Facteurs d'environnement, Gestion collective et dynamique de groupe
Clôture	Contrôle en temps réel, Retour d'expérience

Table 2: Définition des phases de l'action et de ses caractéristiques

La représentation de la dimension organisationnelle est fondée sur la métaphore médicale ([14, 15]) : pour savoir si une organisation est en bonne santé, il est beaucoup plus simple de connaître les causes de sa maladie… Il est plus facile de définir un ensemble de facteurs organisationnels pathogènes que de lister de façon exhaustive les facteurs organisationnels nécessaires et suffisants pour garantir un bon niveau de sûreté dans l'organisation.

C'est pourquoi les facteurs organisationnels pathogènes suivants issus de l'analyse organisationnelle d'une petite centaine d'incidents, accidents, crises sont utilisés pour caractériser l'état de l'organisation influençant l'efficacité des actions humaines [15] :

- Difficulté à faire vivre un Retour d'Expérience (REX)
- Défaillance de la Gestion Quotidienne de la Sûreté (GQS)
- Faiblesse des Organismes de Contrôle (OC)
- Mauvais Traitement de la complexité organisationnelle (MT)
- Pressions de Production (PP)
- Faiblesse de la Culture Organisationnelle de Sûreté (COS)
- Absence de Réexamen des hypothèses de conception (AR).

3.2 L'unification et l'intégration

Les barrières de sécurité, représentées Figure 1 et 2, unifient trois types de connaissances (techniques, humaines, organisationnelles et environnementales) et intègrent deux types d'influence (liens entre l'organisationnel et l'humain et entre l'humain et le technique) [13]. Ces barrières sont caractérisées par leur efficacité prise dans leur contexte organisationnel [3,13]. Les modalités des variables sont de deux types : « absent » et « présent » pour les Facteurs Organisationnels Pathogènes et « Efficace » et « Inefficace » pour les étapes des actions et leur efficacité. La quantification et la structuration des tables de probabilité conditionnelle sont basées sur la notion de porte « Leaky Noisy-OR » [16,17]. Ce type de porte permet de représenter l'ensemble des influences de variables parents sur une variable enfant par le biais de facteurs d'aggravation ainsi définis [3] :

[2] Certaines de ces caractéristiques sont (a) spécifiques du collectif (délégation, expérience, gestion collective et dynamique de groupe), (b) relatives aux outils et procédures (aides, capacité à respecter le cahier des charges, contrôle en temps réel, retour d'expérience), (c) associées à l'influence de facteurs externes sur le collectif pendant la réalisation de l'action (facteurs d'environnement).

$$P(A|B_k) = a_0 \times \prod_{i:B_i \in B_k} \alpha_{i-A}$$

Avec A, un événement, Bk∈B, l'ensemble des parents de A étant dans un état dégradé, a0∈[0,1], la probabilité de non-dégradation de la modalité de A; αi-A∈[0,1], l'influence de l'état dégradé du parent Bi sur l'état non dégradé de A.

Pour les dimensions techniques et humaines, l'enjeu principal est d'estimer la disponibilité des composants techniques de sûreté pris dans leurs contextes humain et organisationnel et d'évaluer leurs impacts sur le système [3].

Les variables et modalités associées sont les suivantes : "Absent" et "Présent" pour la présence de la barrière technique (variable décision); "Disponible", "Indisponible" et "Absent" pour les disponibilités intrinsèque (fournie par le fournisseur du dispositif), initiale (après influence de l'opération de maintenance) et opérationnelle (après influence de l'opération de conduite). La quantification et structuration des Tables de Probabilités Conditionnelles sont basées sur [3] (Tables 3 et 4) :

Installation du dispositif technique (barrière)	**Disponibilité intrinsèque**		
	Disponible	Indisponible	Absent
Présent	x_1	$1-x_1$	0
Absent	0	0	1

Table 3 : TPC de la disponibilité intrinsèque

Disponibilité intrinsèque/initiale	**Efficacité de l'action de maintenance/contrôle**	**Disponibilité initiale/opérationnelle**		
		Disponible	Indisponible	Absent
Disponible	Efficace	1	0	0
	Inefficace	β_a	$1-\beta_a$	0
Indisponible	Efficace	$1-\beta_b$	β_b	0
	Inefficace	0	1	0
Absent	Efficace	0	0	1
	Inefficace	0	0	1

Table 4 : TPC de la disponibilité initiale/opérationnelle

Avec : $x_1 \in [0,1]$, la disponibilité du dispositif donnée par le fournisseur; β_a, le facteur d'aggravation due à l'inefficacité de l'action de maintenance/contrôle ; β_b, le facteur d'amélioration due à l'efficacité de l'action de maintenance/contrôle.

3.3 Mise en œuvre de la méthode

Sur la base des principes préalablement définis, la mise en œuvre de la démarche unifiée se structure sur 4 phases :

- Compréhension du fonctionnement et du dysfonctionnement du système étudié. Cette étape s'appuie sur une analyse fonctionnelle (définition des sous-systèmes, identification des interactions et définition des fonctions principales) suivie d'une Analyse des Modes de Défaillances et de leurs Effets (AMDEC) éventuellement générale (et non détaillée) comme dans le cas d'application qui suit ; les enjeux retenus dans l'AiDR sont la sûreté, la disponibilité, l'environnement et le maintien du patrimoine dans la durée ;

- Modélisation du système. Les groupes fonctionnels précédents et leurs modes de défaillance constituent les nœuds (variables) du modèle et les liens de causes et d'effets entre modes de défaillances et les enjeux du système, les arcs (probabilités conditionnelles entre les variables) de la représentation par réseaux Bayésiens.

- Quantification du modèle. Cette étape consiste à collecter les données nécessaires au modèle qui est représenté par les réseaux Bayésiens. Les données collectées sont de types: des données environnementales (données de débit et température), des données concernant les actions les plus critiques et leur contexte organisationnel (analyse des actions et de l'organisation), les probabilités de défaillance intrinsèques des composants (ou sous-systèmes, en fonction de la granularité retenue pour l'étude), les phénomènes physiques qui peuvent impacter leur fonctionnement. Le résultat principal de cette étape est une représentation quantifiée du modèle précédent et partagée par les acteurs de cette étude (analyste, acteurs du terrain, fonction centrale…).

- Exploitation du modèle et validation des résultats. L'objectif est ici de hiérarchiser les risques vus par le système étudié et de prioriser ainsi les moyens à mettre en œuvre pour les réduire.

4. Cas d'application

EDF a appliqué cette approche à un système d'un site de production d'énergie en lien fort avec l'environnement : la source froide. L'objectif était de mettre à jour une analyse de risques faite six ans auparavant et d'y intégrer les barrières humaines telles que décrites précédemment. La fiabilité de ses composants majeurs peut être ainsi fortement impactée, et par voie de conséquence, peut avoir une influence sur la disponibilité du système donc la disponibilité de la centrale associée.

Sur ces composants, sont appliquées des actions de conduite et de maintenance/surveillance qui permettent de réduire l'occurrence de ces risques. La vision intégrant ces risques de natures technique, environnementale et humaine a pour but de hiérarchiser ces différents risques et de prioriser les barrières de réduction de ces risques, ces barrières pouvant être de remplacer des composants techniques par d'autres ou de renforcer les caractéristiques des actions humaines décrites.

4.1 Description du système étudié

Les phénomènes physiques impactant les matériels majeurs du système ayant un rôle sur son indisponibilité sont décrits ainsi que les barrières permettant de réduire l'impact de ces phénomènes physiques sur ces composants.
Ces matériels sont :

- la Prise d'Eau sur le fleuve (PE),
- le Canal amenant l'eau du fleuve vers la Station de Pompage (C),
- les Filtres de la Station de Pompage (FSP),
- les échangeurs du système de refroidissement de secours (Echangeurs 1),
- et les échangeurs du système de refroidissement normal (Echangeurs 2).

Les phénomènes physiques impactant ces matériels ont été décrits sous forme d'une fiche d'identité (dite 'fiche de risque') selon les trois notions suivantes à laquelle un item commentaire est ajouté :

- La définition du risque, du matériel ou de la barrière concernée ;
- Les phénomènes initiateurs du risque, du matériel ou de la barrière concernée ;
- Les conséquences du risque, du matériel ou de la barrière concernée ;
- Des commentaires utiles à la bonne compréhension et donc modélisation de l'étude. Il peut s'agir aussi bien de données qualitatives (compréhension) que de données quantitatives (modélisation).

Ces fiches de risques s'appuient sur les verbatims réalisés sur le site.

Les phénomènes physiques pris en compte dans l'étude sont les suivants :

- Ensablement : L'ensablement de la prise d'eau correspond à la formation ou au dépôt d'une dune de sable dans la prise d'eau elle-même, derrière la drome flottante (protégeant la prise d'eau en évitant l'accumulation d'embâcles à l'entrée de cette dernière), ou devant l'ouvrage de prise d'eau.
- Isolement de la prise d'eau (PE) : L'isolement de la PE correspond à un débit insuffisant à son niveau.
- Prise en glace : Passage de l'eau de l'état liquide à l'état solide. Les blocs de glace peuvent bloquer l'écoulement d'eau au niveau de la prise d'eau à l'embâcle (obstruction par amas de glace) ou à la débâcle (rupture de la glace à la surface).
- Frasil : Le frasil correspond à l'apparition spontanée de paillettes de glace sous forme de disques de quelques millimètres de diamètre au sein de l'eau par phénomène de surfusion (l'eau reste liquide bien qu'étant sous sa température de solidification, avec risque de passage rapide à l'état solide).
- Obstruction de la PE : Obstruction par des troncs d'arbres, des feuilles ou des débris végétaux.
- Boues et salissures :
    - Salissures : organismes vivants (colonie de bryozoaires, coquillages asiatiques Clam) qui se développent dans la vase des bassins froids du système interne de la Source Froide.
    - Bouchons de vase : en période d'étiage, des bouchons de vase accumulés dans le canal d'amenée peuvent apparaître.
    - Sédiments : feuilles en décomposition et de boues présentes dans l'eau, qui viennent s'accumuler dans le canal d'amenée.

Les barrières permettant de réduire les impacts de ces phénomènes physiques ont été identifiées sur la base de verbatims récoltés sur le site. Elles sont les suivantes :

- Dragage de la Prise d'Eau
- Dragage du Canal
- Intervention contre son isolement, en maintenant un niveau d'eau suffisant à la Prise d'Eau
- Intervention contre la prise en glace de la Prise d'Eau
- La mise en place d'un traçage électrique des grilles de la Prise d'Eau contre le frasil (échauffement)
- Maintenance des grilles contre l'obstruction de la Prise d'Eau.

Les trois premières barrières ont été décrites en utilisant le formalisme de barrières décrit dans [3]. Pour l'évaluation de l'efficacité de ces barrières qui sont de nature humaine, il a été caractérisé ces actions sur la base des facteurs décrits dans le chapitre 3. Les trois autres actions humaines ont été prises en compte de manière simplifiée : leur intégration consiste à baisser la probabilité de défaillance du matériel sur lequel porte l'action humaine (selon la grille d'élicitation d'expert présentée ci-dessous).

Les impacts étudiés concernent le système Source Froide :

- L'état du système lorsque l'un au moins de ses utilisateurs (humain ou matériel) n'est plus fourni en eau froide, ce qui survient lorsque au moins un des systèmes suivants est totalement indisponible : prise d'eau, canal, filtres de la station de pompage, échangeurs.
- Ce même état lorsque l'un au moins de ses utilisateurs n'est plus fourni et que la barrière de réduction de cet impact est elle-même inefficace.

Ces états dépendent de l'influence des phénomènes physiques sur les défaillances matérielles. L'occurrence de ces phénomènes physiques dépend du débit et des températures de l'environnement. La figure 3 illustre ces différents liens d'influence entre l'environnement et l'état du système étudié par l'intermédiaire des phénomènes physiques.

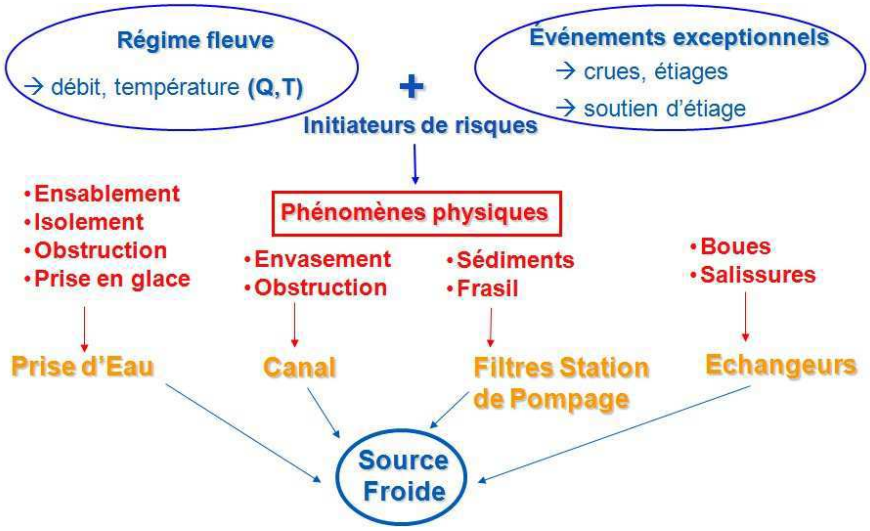

Figure 3 : Synthèse des différents risques et liens entre ces risques et les enjeux du système

4.2 Quantification du modèle de risques représenté par les réseaux Bayésiens

Au delà de la construction de cette structure du modèle de risques, l'étape suivante consiste à quantifier les différentes variables (risques, aléas, barrières) et arcs les reliant pour remplir les tables de probabilité conditionnelles. Ces quantifications sont réalisées sur :

- la base du retour d'expérience,
- les dires d'experts.

Ainsi :

- Pour les risques de nature technique et environnementaux, le REX collecté chez l'industriel et le suivi des données environnementales mènent à des grandeurs caractérisées par un grand nombre de données. Il est donc possible de construire des distributions de probabilités pour ces variables.
- Pour les autres grandeurs, risques techniques (comme des probabilités de défaillances de composants) ou les caractéristiques des actions humaines (Délégation, Formation…), des grilles d'élicitation d'experts ont été définies :
  - Pour les distributions initiales sur les caractéristiques de l'action suivant la grille schématisée en Table 5.

Niveau de définition d'une variable	Valeur initiale de la probabilité de défaillance
Bien définie	0.01
Moyennement définie	0.05
Mal définie	0.50

Table 5 : Table d'élicitation d'expert utilisée pour évaluer les distributions initiales des variables dans la représentation d'un modèle intégré de risques utilisant les réseaux Bayésiens

Des études de sensibilité ont été réalisées sur les valeurs de ces bornes (influence de 0,99 au lieu de 0,999). Aucune influence n'a été observée sur la hiérarchisation des risques.

- Pour les poids des caractéristiques des actions humaines (Délégation, Formation…) sur l'efficacité de l'action, suivant la grille présentée dans la Table 6.

Poids	Valeurs
Pas d'impact	0.99
Peu d'impact	0.755
Impact	0.5
Impact majeur	0.255
Impact total	0.01

Table 6 : Table d'élicitation d'expert utilisée pour évaluer les poids des variables caractérisant l'efficacité des actions humaines dans la représentation d'un modèle intégré de risques utilisant les réseaux Bayésiens

Ces poids multiplieront les distributions initiales introduites au niveau des caractéristiques des actions (Délégation, Formation…) pour fournir des tables de probabilités conditionnelles à entrer dans le réseau Bayésien comme détaillé ci-dessus et dans [3].

Le tableau 7 présente l'estimation des caractéristiques d'une action humaine pour les différentes actions. Parmi leurs phases, les experts ont identifié les caractéristiques qui pouvaient avoir le plus d'influence sur ces actions en relatif entre actions.

Le tableau 7 présente les estimations des différentes caractéristiques des actions humaines pour les différentes barrières. Les poids se réfèrent aux différents niveaux définis dans la table d'élicitation présentée dans le tableau 6.

Impact de … sur efficacité phases de l'action pour la LDD suivante	Intervention contre isolement	Dragage PE	Dragage GSF-PS-CA	Surveillance gillesPE * Moins complexe que dragage GSF-PS-CA ➔ assimilée à dragage PE
Délégation	= (impact moyen)	=	=	=
Aides	- (peu d'impact)	-	=	-
Formation	-	-	=	-
Expérience	-	-	=	-
Capacité à respecter le cahier des charges	-	-	=	-
Facteurs d'environnement	+ (impact fort)	+	+	+
Gestion collective et dynamique de groupe	-	-	=	-
Surveillance de fin de chantier	=	-	=	-
Collecte du REX	=	-	=	-

Table 7 : Synthèse des estimations des différentes caractéristiques des actions humaines pour les différentes barrières

4.3 Exploitation du modèle – résultats obtenus

Le réseau Bayésien ainsi constitué est ensuite utilisé pour :

- Simuler les scénarios d'intérêt : en année moyenne qui correspond à la répartition moyenne des débits et des températures sur la période considérée, pour une crue 10 ans et un étiage 2 ans calculés sur une base de données de débit.
- Effectuer un diagnostic des contributeurs les plus importants aux variables d'intérêt.

Les variables d'intérêt sont la probabilité que l'un au moins de ses utilisateurs n'est plus fourni en eau et celle que, dans ce cas, la barrière de réduction de cet impact est elle-même inefficace, respectivement notées dans la suite Prob util_non_fourni et Prob util_non_fourni&barrière_inefficace.

4.4 Exploitation des résultats

A partir des simulations, il est possible ensuite de s'intéresser à ces variables d'intérêt. Ces valeurs ne correspondent pas à des fréquences annuelles car elles reposent sur des probabilités conditionnelles s'appuyant sur des avis d'experts qualitatifs (par exemple, sachant que l'on est au mois de janvier, quel est le niveau de probabilité d'occurrence de tel phénomène physique ?). En complément, des résultats sont présentés sous la forme de cartographies des risques de dégradation de la disponibilité et d'indisponibilité du système. Les cartographies présentent :

- La **probabilité** d'occurrence de l'événement selon le scénario choisi (année moyenne, crue, étiage) en abscisse;
- La **gravité** de cet événement, i.e. la probabilité d'indisponibilité de la source froide si le dit événement était présent avec certitude en ordonnée.

Gravité (X) = Probabilité (Source Froide indisponible / X réalisé)

La **criticité** de l'événement est définie par la formule :

Criticité (X) = Probabilité (X réalisé) * Gravité (X)

⇒ Ces cartographies traitent à la fois des phénomènes physiques (ensablement, prise en glace, etc.) et des matériels constitutifs de la source froide (PE, canal, etc.).

4.5 Probabilités Prob_util_non_fourni et Prob_util_non_fourni&barrière_inefficace

Les probabilités que l'un au moins de ses utilisateurs n'est plus fourni en eau et celle que, dans ce cas, la barrière de réduction de cet impact est elle-même inefficace sont plus fortes en étiage qu'en année moyenne ou en crues. Ces valeurs ne sont pas, par rapport aux hypothèses initiales posées, des fréquences annuelles d'indisponibilité mais conditionnelles aux scénarios étudiés. Elles conduisent à la hiérarchisation définie dans les tables 8 et 9.

	Prob_util_non_fourni&barrière_inefficace (%)		
	Année moyenne	Crue 10 ans	Etiage 2 ans
Etude 2009 avec mise à jour environnement	0,94	3,95	4,62

	Prob_util_non_fourni (%)		
	Année moyenne	Crue 10 ans	Etiage 2 ans
Etude 2009 avec mise à jour environnement	22,58	31,75	100

Tables 8 et 9 : Hiérarchisation des scénarios année moyenne, crues et étiage sur la probabilité que l'un des utilisateurs du système assurant une partie du refroidissement et n'est plus fourni en eau et sur celle que, dans ce cas, la barrière de réduction de cet impact est elle-même inefficace

Ces évaluations sont complétées par les cartographies suivantes de risques qui hiérarchisent les phénomènes physiques y conduisant et les barrières qui permettent de réduire leurs effets sur la défaillance des matériels prépondérants sur le système de refroidissement étudié.

4.6 Cartographies des risques

La hiérarchisation des phénomènes physiques est la suivante (Figure 4, Figure 5, Figure 6) :

1. En scénario d'année moyenne : criticité principale de l'isolement de la Prise d'Eau, la prise en glace et de l'intervention contre l'isolement ;
2. En scénario de crues : criticité principale de l'obstruction de la Prise d'Eau;
3. En scénario d'étiage : criticité principale de l'isolement de la Prise d'Eau et de l'intervention contre l'isolement.

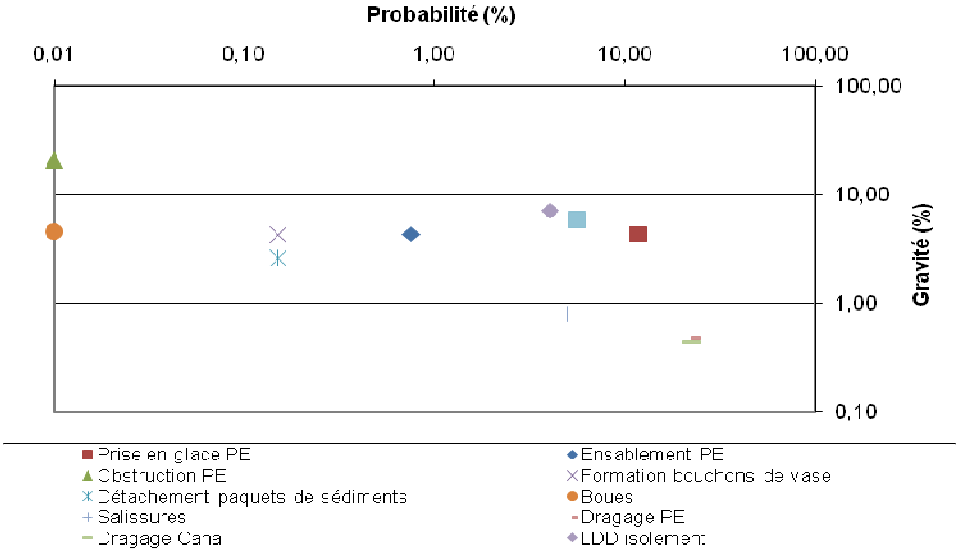

Figure 4 : Cartographie des risques – Phénomènes – Année Moyenne

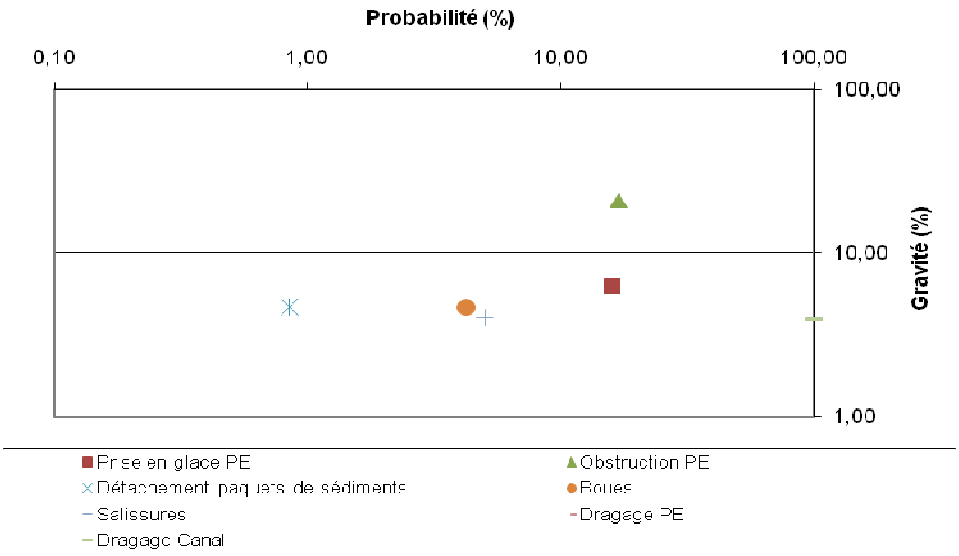

Figure 5 : Cartographie des risques – Phénomènes – Crue 10 ans

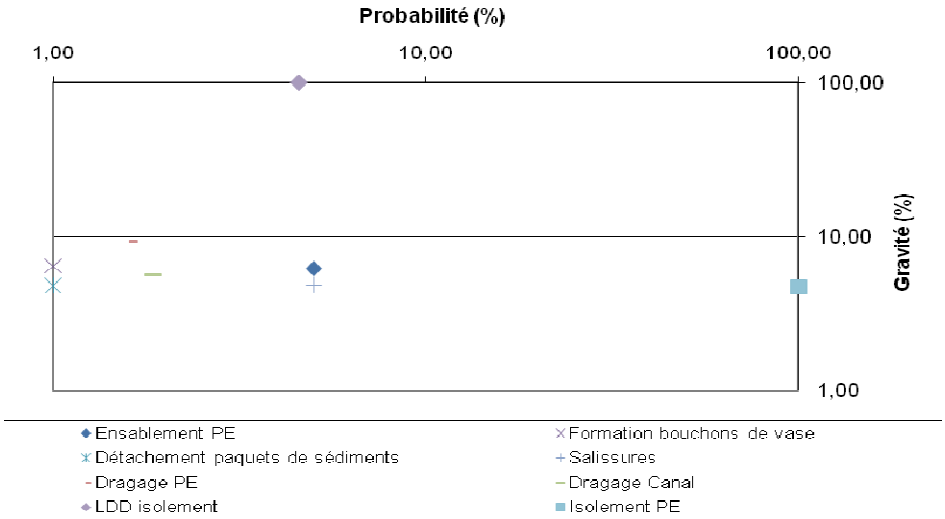

Figure 6 : Cartographie des risques– Phénomènes – Etiage 2/5 ans en Août

Cette hiérarchisation des phénomènes physiques et barrières est conservée par rapport à l'étude menée en 2003.

Néanmoins, par rapport à cette ancienne étude, la modélisation fine des barrières incluant les caractéristiques de l'efficacité de chacune des actions (délégation, formation, aides, expérience,…) permet de faire ressortir les contributeurs principaux suivants (Tables 10 et 11) :

- **En année moyenne,** les Facteurs d'Environnement des actions de dragage (Prise d'Eau ou Canal), de maintenance des grilles de la Prise d'Eau et l'intervention contre l'isolement de la PE sont les facteurs prépondérants de l'éventuelle inefficacité des lignes de défense modélisées.

  Après il faut considérer les caractéristiques de la phase de réalisation autres que celles représentant l'environnement de l'action (Expérience, Respect du cahier des charges, Gestion Collective de l'action) pour les actions de dragage Prise d'Eau et du Canal.

  Ce n'est pas le cas de l'action de maintenance des grilles alors que la quantification faisait apparaître ces caractéristiques de la phase de réalisation comme étant prépondérants.

  Pour l'intervention contre l'isolement de la PE, après le Facteur d'Environnement et la décision associée, ce sont aussi les autres items de la réalisation (Expérience, Gestion collective de l'action et Respect du cahier des charges) qui impactent le plus l'efficacité de l'action puis dans une moindre mesure, la Délégation en phase de préparation et le Contrôle et le REX, en phase de clôture de l'action.

	Probabilités de dégradation des caractéristiques des actions pour chaque barrière (%)			
Caractéristiques de l'action	Dragage PE	Dragage Canal	Maintenance grilles	Intervention isolement PE
De	1	1	1,02	1
Ai	1	1	1,01	1
Fo	1	1	1,01	1
Ex	1	1	1,07	1
Rcc	1	1	1,07	1
Fe	100	100	100	1
Gcdg	1	1	1,07	1
Ac	1	1	1,01	1
Rex	1	1	1,01	1

Table 10 : Hiérarchisation des caractéristiques des actions en année moyenne

	Probabilités de dégradation des caractéristiques des actions pour chaque barrière (%)			
Caractéristiques de l'action	Dragage PE	Dragage Canal	Maintenance grilles	Intervention isolement PE
De	1	1	1	4,84
Ai	1	1	1	3,57
Fo	1	1	1	3,57
Ex	1,06	1,03	1	6,02
Rcc	1,06	1 ,03	1	6,02
Fe	1,19	1,04	1	21,88
Gcdg	1,06	1,03	1	6,02
Ac	1	1	1	4,84
Rex	1	1	1	4,84

Table 11 : hiérarchisation des caractéristiques des actions en étiage 2/5 ans

- **En cas de crues,** les actions de dragage sont critiques au regard des facteurs d'environnement. Cela s'explique par le fait que, même si la probabilité d'ensablement est nulle en crue, le dragage a 100% de chance de ne pas se faire pour raison de sécurité car les débits sont supérieurs à 800m^3/s, débit limite supérieur d'intervention.

- **En cas d'étiage,** le facteur d'environnement est prédominant et implique la prise de décision de mettre en œuvre des moyens matériels particuliers lourds. Les autres items de cette action sont en retrait avec une prépondérance des items liés à la phase de réalisation (Expérience, Respect du cahier des charges et Gestion collective de l'action) sachant que l'exercice n'a jamais été fait in situ puis la Délégation et l'ensemble de la phase de clôture (pour la même raison). Les actions de dragage sont aussi présentes à travers leur phase de réalisation.

4.7 Prise en compte du changement climatique

Les données environnementales du modèle de risques (débits et températures du fleuve) ont été modifiées pour prendre en compte le changement climatique, sur la base de l'hypothèse d'un doublement de la concentration des gaz à effet de serre vers 2050-2060 (par rapport à la période pré-industrielle), soit une croissance de leur concentration de 1% par an. Ce scénario est proche du scénario A2 du GIEC (deuxième scénario le plus pénalisant en terme dévolution des émissions de CO2, sur les six scénarios préconisés par les experts du GIEC). Les simulations effectuées s'appuient sur un modèle hydrologique pour le calcul des débits du fleuve et sur un modèle thermique pour le calcul des températures du fleuve. Le modèle hydrologique calcule un débit naturel (non soutenu en période d'étiage et non écrêté en période de crue) au droit du site. Le modèle thermique calcule la température naturelle locale d'équilibre du fleuve.

Sous le scénario de changement climatique retenu, six simulations équiprobables ont été effectuées. Les débits et températures du fleuve issus de ces simulations sont volontairement comparés à la simulation équivalente obtenue sous climat actuel plutôt qu'aux données historiques pour s'affranchir des biais de modélisation.

Sur les six simulations, trois annoncent une hausse des débits naturels pendant l'hiver, tandis que les trois autres annoncent une diminution modérée des débits naturels en hiver. Les six simulations annoncent une diminution sensible des débits naturels sur la période été-automne. Le changement climatique semble conduire à des situations d'étiage plus sévères, plus longues et plus précoces. Par ailleurs, les six simulations conduisent à une élévation générale de la température du fleuve.

Un traitement statistique des données calculées a été effectué pour les adapter au modèle de risques : en année moyenne, ajustement des données à des lois normales pour les températures du fleuve et à des lois log-normales ou gamma pour les débits ; en scénarios extrêmes (étiages et crues), ajustement des échantillons des minima et des maxima annuels du débit à des lois spécifiques aux statistiques des valeurs extrêmes (troisième asymptote de Weibull, première asymptote de Gumbel ou « distribution de Fisher-Tippett »).
Les résultats les plus pénalisants sont présentés dans la table 12 et sur les cartographies des risques associées montrées en figures 7, 8 et 9.

	Année moyenne		Etiage		Crue	
	Climat actuel	Chgt clim.	Climat actuel	Chgt clim.	Climat actuel	Chgt clim.
Proba. Util_non_fourni (%) NB : ≠ fréquences annuelles	15,32	21,00	34,36	98,48	21,95	34,40
Évolution / Actuel	+37%		+187%		+57%	

	Année moyenne		Etiage		Crue	
	Climat actuel	Chgt clim.	Climat actuel	Chgt clim.	Climat actuel	Chgt clim.
Proba. til_non_fourni&barrière_inefficace(% NB : ≠ fréquences annuelles	0,53	0,89	2,23	5,11	1,65	4,57
Évolution / Actuel	+68%		+129%		+177%	

Table 12 : Evolution par rapport au climat actuel des probabilités des probabilités que l'un au moins des utilisateurs du système assurant une partie du refroidissement est non fourni et, dans ce cas, que la barrière associée est inefficace

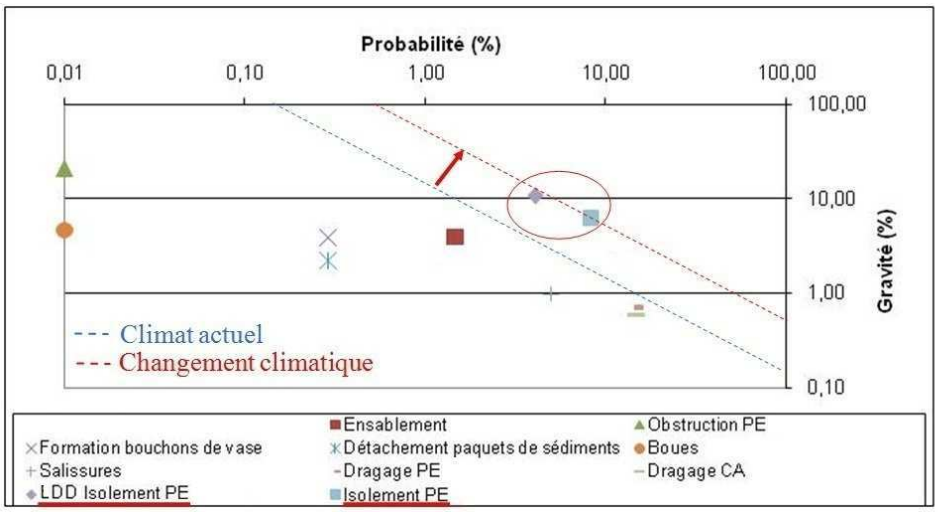

Figure 7 : Cartographie des risques – Année moyenne
Evolution par rapport au climat actuel

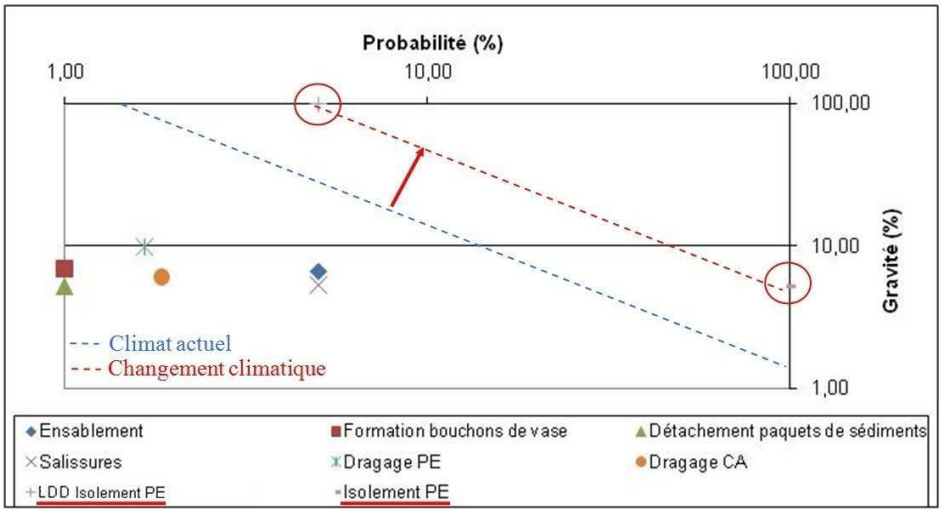

Figure 8 : Cartographie des risques – Etiage
Evolution par rapport au climat actuel

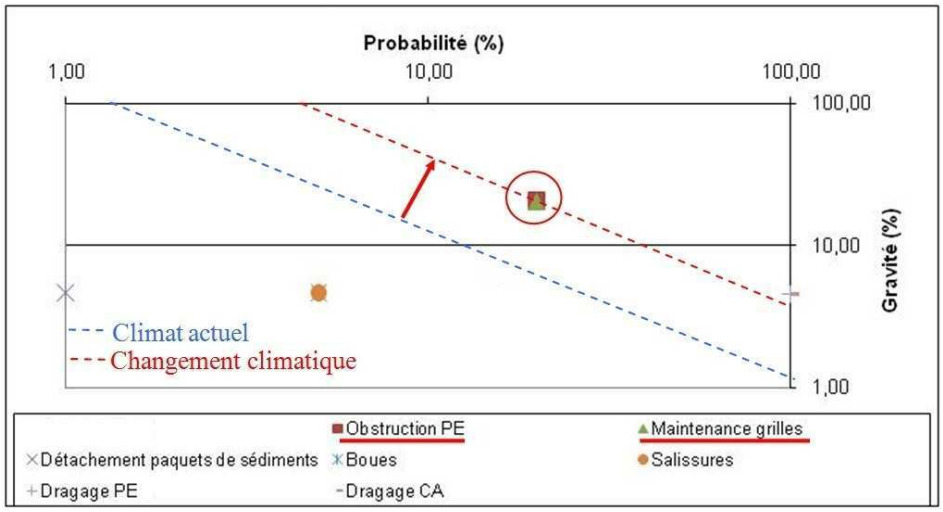

Figure 9 : Cartographie des risques – Crue
Evolution par rapport au climat actuel

En année moyenne et en scénarios d'étiage, le changement climatique affecte de manière significative la criticité de l'isolement de la PE et de la barrière associée. En scénarios de crue, le changement climatique affecte de manière significative la criticité de l'obstruction de la PE et de sa ligne de défense associée (maintenance des grilles PE).

4.8 Synthèse des résultats

Le personnel du site a bien accueilli ces résultats qui lui ont permis de peser à nouveau l'ensemble des risques potentiels pouvant survenir sur le système dont il a la charge et ce, en fonction des périodes de l'année, et d'évaluer la criticité des barrières envisagées pour les réduire.
Des études de sensibilité ont été menées pour identifier l'influence des poids entre caractéristiques des actions et efficacités des barrières sur le système. La première conclusion, concernant la collecte des connaissances en amont de la construction du modèle et de sa quantification, est primordiale. Le projet IMdR 09-2 l'illustre [18].
De plus, l'étude a permis d'identifier un besoin nouveau de l'exploitant et de l'ingénierie d'obtenir des valeurs réalistes des fréquences d'occurrence d'indisponibilité et de sa dégradation. Ceci implique de quantifier précisément la probabilité de défaillance d'une action humaine prise dans son contexte organisationnel, en prenant en compte non seulement ses aspects pathogènes mais aussi résilients.

Conclusion et Perspectives

L'objectif global de ce papier était de mettre en évidence l'intérêt de l'intégration des risques dans une même vision. Ceci se traduit sous la forme d'une approche modulaire qui permet de prioriser les risques vus par un système socio-technique pris dans son environnement physique et sociétal pour prioriser à leur tour les mesures envisagées pour les réduire, et ce vis-à-vis d'enjeux multiples : sûreté, disponibilité, maintien du patrimoine dans la durée…
Les limites identifiées sont liées à la simplification induite par l'intégration au niveau de l'évaluation de l'efficacité des actions humaines de maintenance et de conduite.
Pour palier les effets de cette simplification, il est prévu d'améliorer : la robustesse de la caractérisation de l'efficacité d'une action humaine en s'appuyant sur des méthodes de la fiabilité humaine, la caractérisation de l'organisation en travaillant sur les facteurs de la résilience en complément des facteurs pathogènes et la phase d'estimation des risques. La piste de l'interopérabilité entre le modèle existant et ceux de la fiabilité humaine est laissée ouverte quand il sera nécessaire d'avoir des probabilités de défaillances réaliste d'action de conduite en situation incidentelle ou accidentelle par exemple. Enfin, la caractérisation des incertitudes spécifiques à cette approche qui intègre des données issues du REX et disponibles en grand nombre (sur lesquelles des distributions de probabilité peuvent être construites) et des données qualitatives suivie de leurs propagation dans un modèle réseaux Bayésiens est en cours de résolution dans le cadre de la thèse co-encadrée EDF-CRAN [19, 20, 21].

REFERENCES

[1] LES RISQUES ÉMERGENTS AU XXIe SIÈCLE – ISBN 92-64-10121-7 – © OCDE 2003.
[2] Medina-Oliva, G., Weber, P., Simon, C., Iung, B., Overview on Bayesian networks Applications for Dependability, Risk Analysis and Maintenance areas, IFAC EAAI Journal - Engineering Application of Artificial Intelligence; Online publication complete: 16-JUL-2010; DOI information: 10.1016/j.engappai.2010.06.002
[3] Léger A., Weber P., Levrat E., Duval C., Farret R. and Iung B. Methodological developments for probabilistic risk analyses of socio-technical systems. Journal of Risk and Reliability, 223-4, 313-332, 2009.
[4] Villemeur, A,. 'Reliability, Availability, Maintainability and Safety Assessment - Volume 1': Methods and Techniques. Wiley & Sons, 1992.
[5] Swain, A.D. and Guttman, H.E. 'Handbook of human reliability analysis with emphasis on nuclear power plant applications'. NUREG/CR-1278, US Nuclear Regulatory Commission, 1983.
[6] Rasmussen, J., 'Human errors: a taxonomy for describing human malfunction in industrial installations', Journal of Occupation and Accidents', 4, p.311-333.
[7] Reason, J., 'Human error', Cambridge University Press, 1990.
[8] Darek M. Eriksson, 'A Principal Exposition of Jean-Louis Le Moigne's Systemic Theory', Department of Informatics and Systems Science, School of Business, Administration and Social Sciences, Luleå University of Technology, Sweden, published in "Cybernetics and Human Knowing". Vol. 4 no. 2-3 1997.
[9] AIEA, collection sécurité n°75-INSAG-4, 1991.
[10] Paté-Cornell, M.E., and Murphy, D.M,. 'Human and Management factors in probabilistic risk analysis: the SAM approach and observations from recent applications'. In Reliability Engineering and System Safety, 1996, 53, pp.115-126.
[11] Jensen J.C. Bayesian networks and decision graphs, Springer editions, 2001.
[12] Andersen H., Casal J., Dandrieux A., Debray B., Dianous V.D., Duijm N.J., Delvosalle C., Fievez C., Goossens L., Gowland R.T., Hale A.J., Hourtolou D., Mazarotta B., Pipart A., Planas E., Prats F., Salvi O. and Tixier J. Aramis User Guide, 2004.
[13] Léger A., Duval C., Farret R., Weber P., Levrat E. and Iung B. Modeling of human and organizational impacts for system risk analyses. Ninth International Probabilistic Safety Assessment and Management Conference, Hong-Kong, China, 2008.
[14] Reason J. Managing the risks of organizational accidents, Ashgate, Aldershot, United Kingdom, 1997.
[15] Pierlot S. and Dien Y. From organizational factors to an organizational diagnosis of the safety. European Safety and Reliability Conference, Stavanger, Norway, 2007.
[16] Galàn S.F., Mosleh A. and Izquierdo J.M. Incorporating organizational factors into probabilistic safety assessment of nuclear power plants through canonical probabilistic models. Reliability Engineering and System Safety, 92, 1131-1138, 2007.
[17] Diez F.J. and Druzdzel M.J. Canonical Probabilistic Models for Knowledge Engineering, Technical Report CISIAD-06-01, 2007.
[18] Guyot B, Condamin L., Naïm P., Marle L., Duval C., Anfiani A., Belec Y., Chojnacki E., Riaanudo P., Ziani R., Projet IMdR P09-2 : Validation et représentativité d'un réseau Bayésien en analyse des risques et sûreté de fonctionnement
[19] Fallet G., Duval C., Weber P. and Simon C. Characterization and propagation of uncertainties in complex socio-technical system risk analyses. 1st Workshop on the Theory on Belief Functions, Brest, France, 2010.
[20] Fallet G., Duval C., Simon C., Weber P. and Iung B. Collecting and modeling expert judgment applied to Integrated Risk Analysis. 3rd International Workshop on Dependable Control of Discrete Systems, Saarbrucken, Germany, 2011.
[21] GIS Sûreté, Sécurité et Surveillance des Grands Systèmes, livre à paraître, chapitre Maîtrise et analyse intégrée des risques