L'analyse de risques pour les débutants

Par Jean-Claude JACQUIOT consultant CASE France & Future Tech Systems Inc. Paris-Seattle, Juillet 2010 - jean-claude.jacquiot@case-france.com

Le risque est au cœur de nos préoccupations quotidiennes, mais qu'est-ce que l'analyse de risques ?

Plus précisément :

- *Qu'est-ce qu'un risque ? Un danger ?*
- *Comment s'y prendre pour faire une analyse de risques ?*
- *Avec quel outil et quelle méthode ?*
- *Comment identifier des scénarios de risques ?*
- *Comment négocier des objectifs pour évaluer les risques ?*
- *Comment définir des barrières de protection ?*
- *Comment faire un plan d'actions ?*

Ce document explique aux néophytes ce qu'est l'analyse de risques avec le module A de la méthode MOSAR. Il s'adresse aux nombreuses parties prenantes qui de près ou de loin doivent comprendre, analyser, gérer l'arrivée d'événements non souhaités pour assurer la sécurité d'installations ou la sûreté de systèmes afin d'éviter des accidents.

CASE France
2, allée de Londres
91969 Courtaboeuf Cedex - France
Tél. 01 69 86 95 46
Fax. 01 69 07 03 43
www.case-france.com

La théorie

Synthèse d'après le cours de M. Périlhon - CEA Grenoble
Concepteur de la méthode MOSAR

1 INTRODUCTION ET DEFINITIONS

RISQUE, un mot que l'on entend régulièrement et pourtant sa compréhension et son utilisation par le grand public sont le plus souvent erronées. La confusion vient de la définition des mots risques et dangers. Nous allons essayer d'y remédier dans ce document.

D'abord, pour cerner le sujet, quelques exemples de risques dont on parle souvent :

- Les effets secondaires d'un médicament ou d'une opération chirurgicale
- Les accidents de la circulation
- La contamination de sang, de rivières, de l'environnement…
- Les accidents dans la pratique d'un sport ou d'une activité
- L'explosion d'une usine de produit dangereux
- Le crash d'un avion ou le déraillement d'un train
- Le mauvais (défaut de) fonctionnement d'un appareil, d'un service ou d'un système
- La mauvaise exécution d'une tâche
- Les cataclysmes naturels
- Les prises de position à la bourse (risques financiers)
- L'intrusion de virus informatiques (risques informatiques)
- Etc. etc.

Bien que ces risques soient de natures très différentes, leur analyse procède d'une même démarche théorique. Cependant, des différences d'interprétations et de vocabulaire sont couramment observées dues essentiellement à des écoles de pensées liées à des métiers particuliers. L'approche que nous allons étudier émane de la « science du danger » et enseignée en France, dans les grandes écoles d'ingénieurs. Elle est couramment utilisée par des entreprises comme le CEA et EDF.

1.1 Définition du « risque »

D'une part, les scientifiques, qui ont créé la science du danger appelée « **CINDYNIQUE** » et d'autre part, les professionnels tels que les assureurs, en donnent une même définition :

R associe D * P * G * A

Ce qui veut dire en clair :

Le **RISQUE** est l'association d'un **DANGER**, de sa **PROBABILITE**,

de sa **GRAVITE** et de son **ACCEPTABILITE**.

Le risque est un ensemble de quatre éléments indissociables. Un peu comme une équation mathématique. Cependant, ces quatre éléments ne sont pas de même nature. C'est pour cela qu'il n'est pas possible de mettre un signe = entre R et les autres éléments.

Comme il est dit dans l'introduction, attention à l'amalgame entre les mots **RISQUE** et **DANGER**. Pour éviter de définir le risque par rapport au danger et le danger par rapport au risque (débouclage de définition, le danger étant une potentialité de risque), il est nécessaire de donner une définition originale du danger :

DANGER : On va dire qu'il est défini par *un* ***ensemble de processus*** (au sens ***systémique*** du mot processus, ce qui nous obligera à développer cette définition ci-dessous), qui déroule l'enchaînement d'événements conduisant à un **EVENEMENT NON SOUHAITE** (**ENS**) pouvant avoir ***un impact,*** en général destructeur, sur une ou plusieurs des quatre ***cibles*** possibles :

- un ou des individus,
- une ou des populations,
- un ou des écosystèmes,
- un ou des systèmes matériels ou symboliques.

Définitions des autres termes utilisés dans la définition du risque :

PROBABILITE : Elle est définie par la probabilité d'enchaînement des événements conduisant à **l'ENS**. Dans certain cas, on peut aussi utiliser le terme « FREQUENCE ».

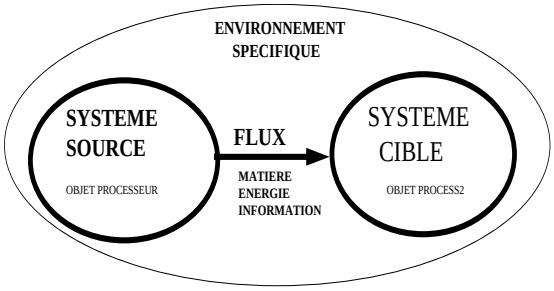
GRAVITE : Elle est définie par l'effet des **ENS** sur les cibles.

ACCEPTABILITE : Elle est définie par l'acceptabilité de **l'ENS** par les acteurs dont les cibles. Nous constatons ainsi que les définitions révèlent des niveaux différents. Il est possible de définir scientifiquement le danger, sa probabilité bien sûr et sa gravité mais il n'est pas possible de définir scientifiquement son acceptabilité car à ce niveau, les ***subjectivités*** individuelles et collectives sont prépondérantes. « Le risque est un construit individuel et social ».

PROCESSUS : C'est toute transformation dans le temps, l'espace, la forme (ou nature), de matière, d'énergie, d'information. Un processus s'établit entre un objet processeur, ou système processeur, ou source, ou système source et un objet « processé », ou système « processé », ou puits, ou système cible, par échange d'un flux de matière, d'énergie, d'information.

Il est donc possible de modéliser le réel par des systèmes emboîtés dont l'activité et les relations sont gérées par des processus.

.



LE PROCESSUS

1.2 Définition de « l'Analyse de Risques »

En reprenant chacun des termes de la définition du risque proposée ci-dessus, même si elle est réductrice, on peut donner une première définition de l'analyse de risques (A.R.).

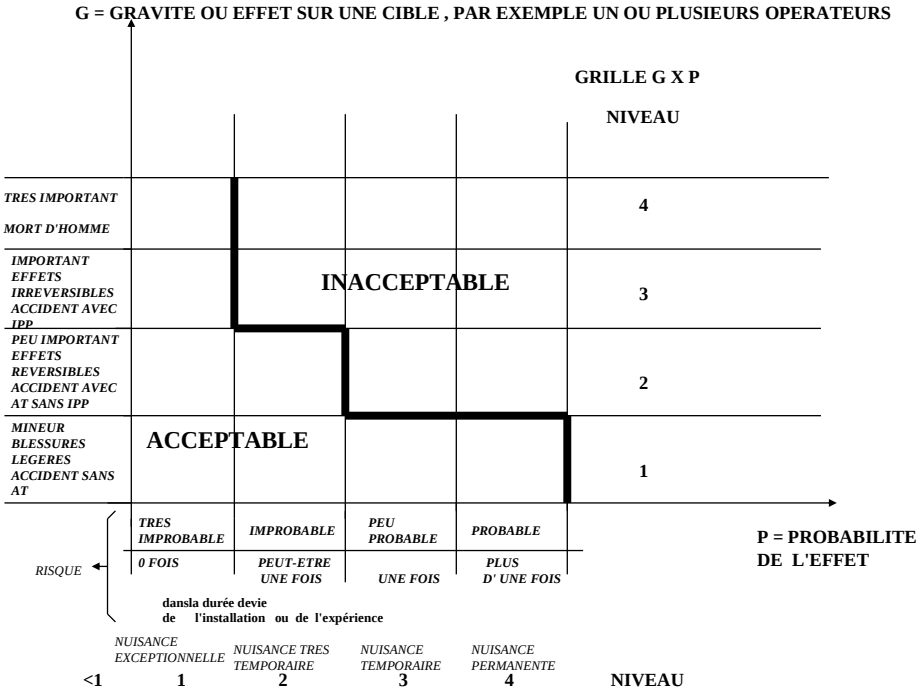
L'A.R. en 5 étapes :

1- Traiter le Danger et pour cela identifier les processus de dangers c'est-à-dire l'enchaînement d'événements issus de systèmes sources de dangers et pouvant conduire à des ENS.
Ce travail d'évaluation peut se faire en mettant en œuvre le modèle MADS défini ci-après.

2- Représenter l'enchaînement des événements conduisant à l'ENS, conduit à des représentations du type arbres logiques ou réseaux.
Ce travail met en œuvre des outils du type Arbres de Défaillances (ADD), Arbres d'Evénements, Arbres Causes-Conséquences, Réseaux de Pétri, Chaînes de Markov, qui permettent aussi de calculer les probabilités de ces événements dans certains cas.

3- Pour déterminer la Gravité des ENS on détermine leur impact sur les cibles. Celui-ci peut être immédiat mais aussi différé traduisant des états de la cible dans le temps. Certains de ces états différés sont difficiles à prévoir, d'où le principe de précaution.

4- La détermination de l'acceptabilité se fait par négociation de tous les acteurs concernés dont les cibles. Dans certains cas, des limites peuvent être imposées par une réglementation (cas du nucléaire) ou par une règle spécifique (cas des installations classées).
*Parmi les outils possibles voici les grilles Gravité *Probabilité. Ce sont des outils simples et assez faciles à mettre en œuvre. Elles permettent de situer les scénarios d'accidents et de les hiérarchiser. On en trouvera un exemple ci-après.*



La négociation de ces grilles se fait à deux niveaux : tout d'abord négocier comment l'on gradue les axes et ensuite négocier la position de la frontière entre l'acceptable et l'inacceptable.

5- La neutralisation des risques se fait par la recherche de toutes les barrières de prévention et de protection qu'il est possible d'identifier pour éviter la production d'événements et leur enchaînement.
*Ces barrières sont de nature technique et opératoire. Il est nécessaire de les qualifier dans le temps pour s'assurer de leur pérennité. Une fois ces barrières établies on peut vérifier si le risque est devenu acceptable en resituant les scénarios dans les grilles G * P.*

Dans toutes ces approches il faut cependant bien garder à l'esprit qu'il est très difficile, voire impossible de prendre en compte toutes les dimensions du risque : **spatiale** et **temporelle.**

Nous sommes par ailleurs toujours dans une situation **de conflit.** Conflit homme/nature, justice/profit, pauvreté/richesse....

Démontrer par la systémique, le risque est d'autre part le **moteur de l'évolution**, ce qui pose le problème de savoir s'il faut l'éliminer ou non.

Enfin, la maîtrise du risque est au cœur des **processus de décision** comme participant aux choix et aux arbitrages dans la **gestion des conflits** par tout **décideur**, afin de **minimiser** les occurrences et les effets des dangers possibles.

2 METHODE MADS

Méthode d'Analyse de Dysfonctionnement des Systèmes

2.1 Introduction à la méthode

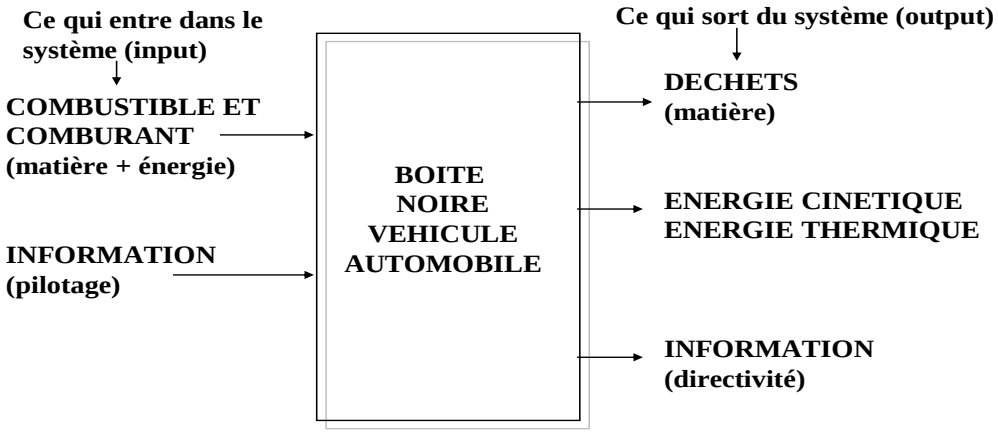
Il s'agit d'une approche systémique (qui utilise la notion de système) qui est particulièrement adaptée aux risques généraux liés aux systèmes complexes, par exemple, là où il y a danger sur les êtres humains. La systémique est une science, mais entrer ici dans le détail dépasse l'objectif de ce document. L'amateur éclairé pourra lui-même s'informer s'il le désire. Ceci n'étant pas absolument nécessaire pour la compréhension de ce document.

La systémique fait l'objet d'une bibliographie abondante (nous consulter pour l'obtenir). L'un des ouvrages auxquels nous nous sommes beaucoup référés est celui de J.L LE MOIGNE : Introduction à la Théorie du Système Général. PUF

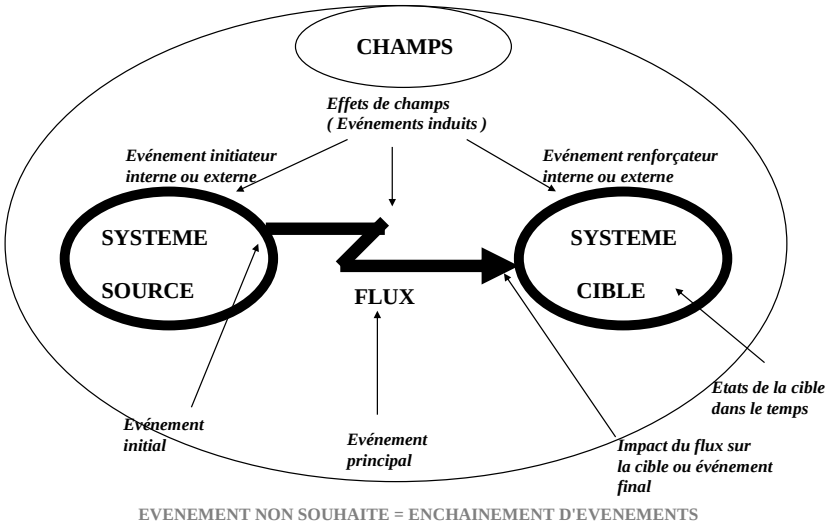
Le modèle MADS est issu d'un groupe de travail qui comprenait :

- Trois enseignants de l'IUT de BORDEAUX TALENCE : Jean DOS SANTOS alors directeur de l'IUT Hygiène, Sécurité, Environnement, Michel LESBATS, Yves DUTUIT, enseignants dans cet IUT.
- Trois ingénieurs du Commissariat à l'Energie Atomique : Jean-Michel PENALVA, Laurent COUDOUNEAU, Pierre PERILHON.

Tout système étant un transformateur dans le temps, l'espace, la forme, de matière, énergie, information et un véhicule automobile pouvant être modélisé comme un système, on peut aussi le représenter sous forme d'une boîte noire. On ne cherche plus à savoir ce qui se passe à l'intérieur (c'est à dire que l'on peut s'affranchir de son fonctionnement), mais on peut identifier qu'est-ce qui entre dans le système et qu'est-ce qui en sort: de la matière, de l'énergie et de l'information.



2.2 Explication du modèle MADS (processus de danger)



EVENEMENT NON SOUHAITE = ENCHAINEMENT D'EVENEMENTS

D'après le modèle ci-dessus, le danger est l'ensemble des processus qui conduisent à un processus principal pouvant être généré par un système source de danger.

Le flux de danger est généré par une source de flux de danger à partir du système source de danger et il est constitué de matière, d'énergie, d'information. Si ce flux peut atteindre un système cible et avoir des effets sur ce dernier on parle alors de ***risque***.

L'ensemble des processus est situé dans un environnement spécifique (partie de l'environnement qui le concerne) générateur de champs « processant » des effets sur ces processus.

La source de flux de danger est générée par un processus initiateur d'origine interne ou externe (et donc provenant de l'environnement spécifique). Symétriquement, il peut y avoir un processus renforçateur du flux sur la cible, d'origine interne ou externe (et donc provenant de l'environnement spécifique).

Certains champs sont plus spécifiquement des champs de danger dans la mesure où ils génèrent des processus origines ou renforçateurs des autres processus de danger.

L'ENS est la rencontre du processus principal avec un système cible.

Si l'on définit les processus comme des événements, le modèle peut se représenter comme suit :

On appelle :

- Evénement Initial, la Source de Flux de Danger
- Evénement Principal, le Flux
- Evénement Final, l'impact du flux sur la cible

- Etats de la Cible, les états qu'elle va prendre dans le temps
- Evénements Induits ou Effets induits, les effets de champs avec notamment l'événement initiateur issu du processus initiateur et événement renforçateur, l'événement issu du processus renforçateur,

Le modèle montre l'enchaînement des événements qui, partant de l'événement initiateur, conduit aux différents états de la cible.

Si l'on se réfère au schéma précédent, que faudra-t-il faire pour analyser à priori les risques ?

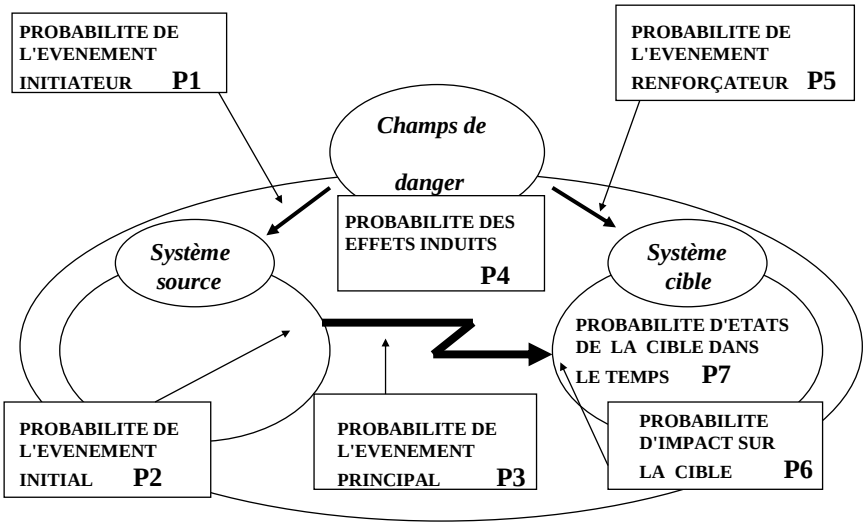
Il faudra :

1- Représenter sous forme de systèmes (des boites) tous les objets significatifs de votre environnement de danger, personnes comprises (système complexe).

REMARQUE : Pour certains types de risques, par exemple : financiers ou informatiques, il sera « peut être » préférable de modéliser les sources de danger avec des fonctions (analyse fonctionnelle) plutôt qu'avec des systèmes. Mathématiquement parlant, une « application » (par exemple informatique) est une généralisation d'une fonction, ce qui nous ramène au cas précédent. Egalement, une activité (par exemple financière ou commerciale) est représentée par une fonction.

2- Identifier les processus de dangers c'est à dire l'enchaînement d'événements issus de systèmes sources de danger et pouvant conduire à des ENS. Pour ce faire, nous mettrons en œuvre le modèle **MADS.**

3- Construire et représenter l'enchaînement des événements conduisant à l'ENS.
Ceci nécessite l'élaboration de scénarios pour laquelle nous utiliserons aussi la démarche



P évènement non souhaité = P1 x P2 x P3 x P4 x P5 x P6 x P7

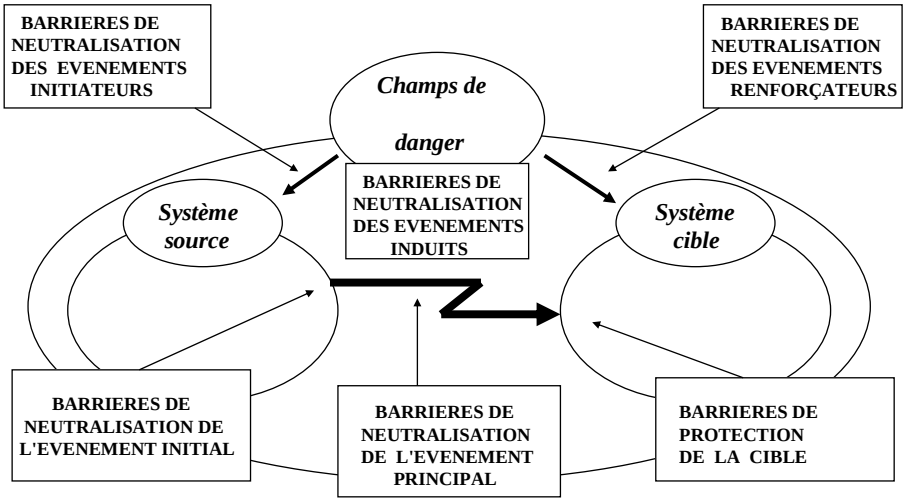
APPROCHE PROBABILISTE

systémique.
La probabilité d'enchaînement des événements est une probabilité composée comme le montre le schéma ci-dessous.
Ce modèle montre bien la difficulté de l'évaluation probabiliste de l'ENS qui nécessite la connaissance de la probabilité de chaque événement.

4- Evaluer l'effet des ENS sur les cibles, qui se traduira par un ***impact immédiat*** et parfois par un ***impact différé***. Ces impacts induisent ***des états*** de la cible dont certains seront donc différés et difficiles à prévoir.

5- La détermination de l'acceptabilité se fait ***par négociation*** de tous les acteurs comme nous l'avons vu ci – avant.

6- La recherche des moyens de neutraliser les événements conduisant à l'ENS constitue la prévention des risques et consiste à identifier les barrières de prévention au niveau du système source, de l'événement principal et des effets induits, et les barrières de protection au niveau des systèmes cibles.



APPROCHE DETERMINISTE OU DE DIMENSIONNEMENT

Le modèle est directement opérationnel, à savoir qu'il permet d'identifier l'enchaînement des événements conduisant à un ENS.

D'autre part il est réversible car un système source peut devenir un système cible et vice-versa. Ceci permet de faire apparaître des scénarios par enchaînement de processus de danger et de rassembler ces scénarios dans la construction d'arbres logiques centrés sur un même ENS. Cette technique est mise en œuvre dans la méthode MOSAR.

3 LE DEVELOPPEMENT DE TYPOLOGIES

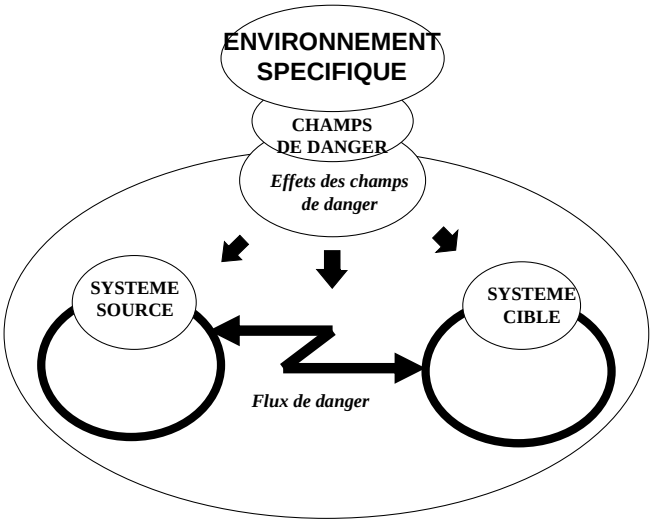
Le modèle MADS permet de décrire et développer :

- Des typologies des systèmes sources de danger propres à chaque contexte
- Des typologies des cibles
- Une typologie générale des événements principaux
- Une typologie générale des champs. La structure des champs dépend des couples systèmes sources - systèmes cibles.

Les outils d'analyse de risques proposent des listes prédéfinies de typologies pour tous ces éléments de danger. Ceci permet la standardisation, la normalisation et rendent les analyses de risques multiples cohérentes (nous consulter pour obtenir les listes de typologies).

4 LES CHAMPS DE DANGER

Le risque n'apparaît que s'il y a entrée d'une cible dans un champ de danger.



LE MODELE MADS EST REVERSIBLE

Voici un exemple de typologie générale des champs :

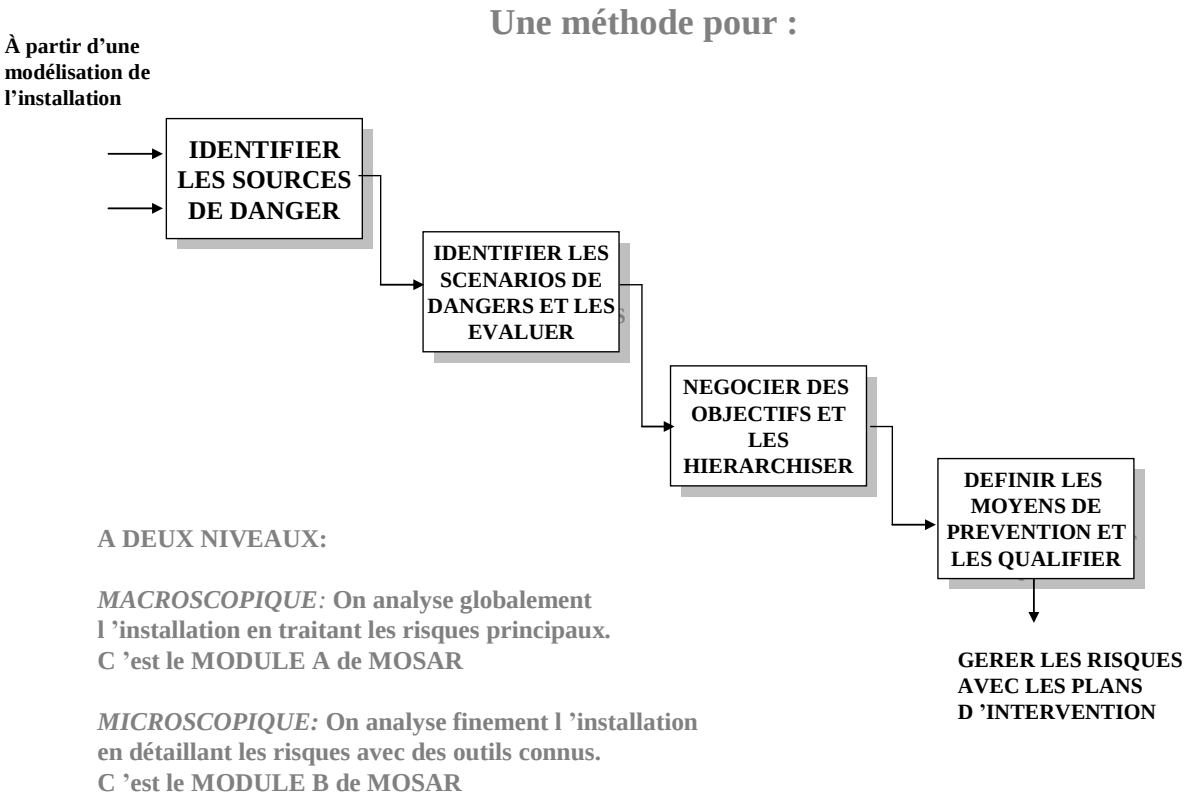
- Champs physico-chimiques naturels ou artificiels (scientifiques et techniques)
- Champs psychologiques
- Champs économiques
- Champs sociologiques
- Champs politiques
- Champs juridico-réglementaires (ce sont des champs transversaux)
- Champs culturels
- Champs organisationnels

En entrant dans les champs on entre aussi dans un domaine de complexité. Des études poussées ont été réalisées par des chercheurs sur la notion « d'hyperespace de danger ». Intéressant, mais sans lien pratique pour notre vulgarisation de l'analyse de risques. Vous pouvez lire :

> ***L 'HYPERESPACE DU DANGER***
>
> ***La rupture de l'axe téléologique dans les récentes affaires***
>
> ***(d'après C. FRANTZEN)***

5 DEMARCHE DE LA METHODE MOSAR

5.1 Méthode Organisée et Systémique d'Analyse de Risques



Les explications arrivent avec le chapitre suivant…

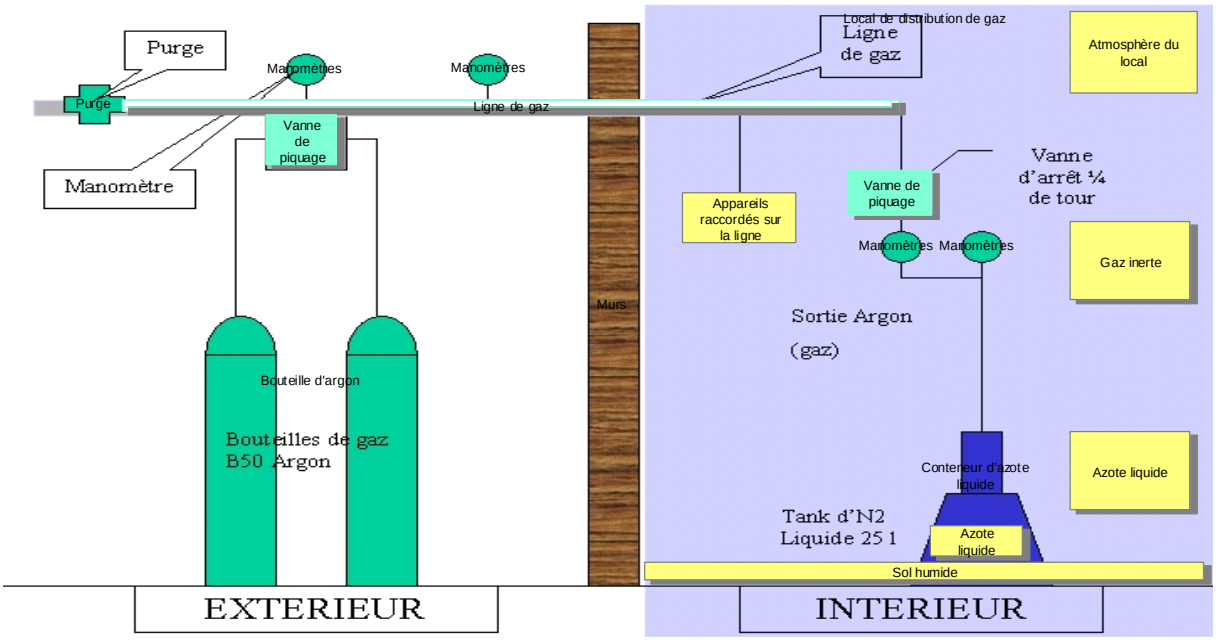
La pratique

Il est maintenant possible d'illustrer cette démarche sur un exemple concret.

6 EXEMPLE : Un local de distribution d'argon

Voici la démarche pour l'exemple.

6.1 Décomposition en sous-systèmes

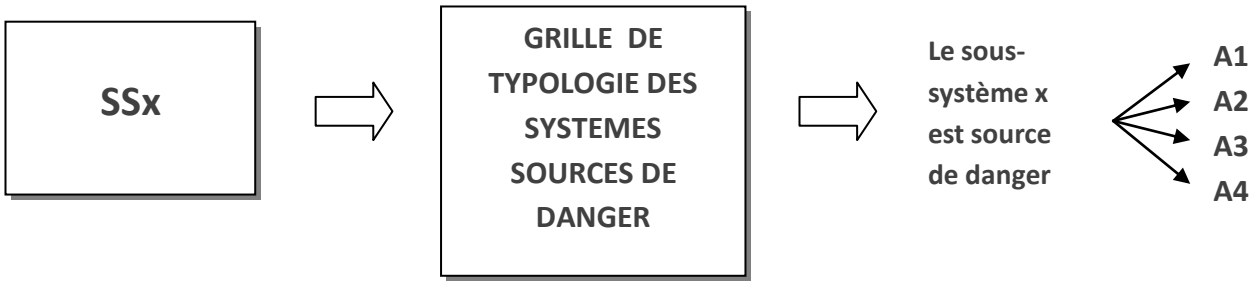


Avec l'aide d'un outil graphique qui nous permet de décrire graphiquement la scène, on effectue le recensement des systèmes et sous-systèmes qui la composent et qui sont significatifs pour l'analyse de risques en cours. Chaque système peut être décrit selon les besoins.

6.2 Identification des sources de danger

On identifie les sources de danger de chaque sous-système (ou identifier en quoi chaque sous-système peut être source de danger).

Pour effectuer ce travail, on lit chaque sous-système à travers la grille de typologie des systèmes sources de danger (nous contacter pour obtenir la grille complète).

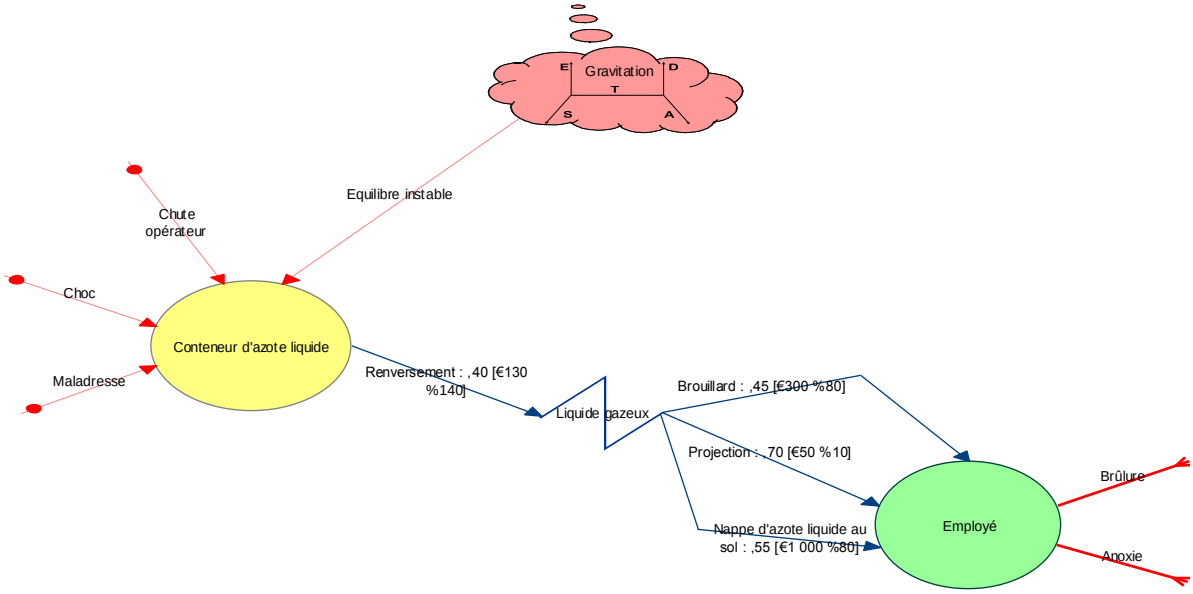


En faisant cette identification pour tous les sous systèmes, on obtient donc ***une liste exhaustive des sources de dangers*** typées de l'installation : **A1, A2, A3, …**
Dans l'exemple ci-dessus, nous obtenons une source de danger pour le système « Conteneur d'azote liquide » : « **A1 sous pression** »

6.3 Identification des processus de danger

Ce travail se fait avec l'aide d'un outil graphique supportant le modèle MADS. Ici on crée un diagramme de processus de danger pour chaque source de danger :

Ici source de danger : A1 sous pression – Conteneur d'azote liquide



Ce travail se fait avec un éditeur graphique spécialisé qui facilite le dessin, l'entrée des données (attributs des objets) dans la base de données du projet et vérifie la syntaxe générale avant de pouvoir l'enregistrer en toute « sécurité ».

Tout d'abord précisons qu'un ***flux de danger*** est composé de 3 parties distinctes :

- L'événement initiateur : ici « Renversement » (un seul par diagramme)
- Le flux de danger lui-même : ici « Liquide gazeux »
- Le ou les événements principaux (appelé également finaux) : ici « Brouillard », « Projection », « Nappe d'azote liquide au sol » par rapport à un système cible : ici : « Employé »

Le but est de rechercher tous les événements (flèches rouges en pointillées et noires) qui constituent le processus de danger.
On commence par la recherche des événements initiaux (dans l'exemple : première partie de la flèche noire « Renversement »). S'il y en a plusieurs, on préférera faire des diagrammes séparés afin de bien séparer les flux de danger pour en faciliter la gestion ultérieure. Ces derniers peuvent provenir soit du ***contenant*** c'est à dire de l'enveloppe du système source (ici bulle jaune), soit de son ***contenu***. Un attribut de l'outil permet de le préciser.

On recherche ensuite les événements initiateurs (flèches rouge en pointillées) qui peuvent engendrer les événements initiaux par l'intermédiaire du système source de danger. Ces événements peuvent être d'origine interne ou externe au système source de danger. Dans ce dernier cas ils sont générés par les champs (ici : « Equilibre instable » du champ « Gravitation »).

La chaîne : ***événements initiateurs*** -> ***événements initiaux*** génère des ***événements principaux***

Ici « brouillard », « projection », « Azote liquide au sol » sur le système cible (en vert).

L'arrivée d'ENS produits des effets (flèches rouges pleines). Ici « Brulure » et « Anoxie ».

Avec ce type de représentation graphique, vous voyez clairement le processus de danger, ce qui n'est pas le cas lorsqu'on utilise uniquement du texte ou des tableaux. Vous le voyez dans son ensemble, ce qui favorise l'exhaustivité du processus et son analyse.

Toujours pour des besoins de simplicité et de gestion ultérieure, il est recommandé de créer un diagramme par événement initial produit par un système source de danger (voir diagramme ci-dessous), ceci n'est bien sûr qu'une convention. Pour faciliter ce travail l'outil propose le copier/coller et/ou l'utilisation d'une bibliothèque de diagrammes de processus de danger génériques (« Templates »). Cette dernière permet la capitalisation (ou thésaurisation) du risque.

Un attribut ***« phases de vie »*** permet de préciser certains dangers. Par exemple dans le cas de la distribution d'argon, si l'on fait l'analyse dans la phase **exploitation** normale, il n'y a pas de danger de renversement du containeur d'azote liquide. Par contre, dans les phases **d'entretien** il apparaît un danger de manutention du containeur d'azote liquide.

Il est donc possible de faire l'analyse soit phase par phase, soit en cherchant à identifier les principaux dangers apparaissant dans les différentes phases.

CONSEILS :

Deux phrases mnémotechniques pour s'aider à trouver des réponses dans la recherche des processus de danger et stimuler son imagination :

- Qu'est-ce qui est et qui pourrait ne pas être ? Par exemple, il y a du courant électrique et il pourrait ne pas y en avoir.
- Qu'est-ce qui n'est pas et qui pourrait être ? Plus difficile. Par exemple il n'y a pas de fuite mais il pourrait y en avoir une.

REMARQUE :

- Cette technique nous donne un outil de génération d'un ensemble d'événements. Ce *n'est qu'un outil* qu'il faut utiliser comme tel. Il nous aide à faire apparaître des événements et leurs enchaînements pouvant avoir des effets non souhaités sur *des cibles qui, à ce niveau, ne sont pas encore identifiées*. Il appartient à l'analyste de se servir des identifications d'événements pour construire des chaînes plus ou moins longues d'enchaînements.

- Dans l'identification des événements principaux, il faut prendre garde à ne pas noter des interférences avec les autres sous systèmes sinon la génération de scénarios (voir ci après) deviendra confuse par la suite.

6.4 Identifier les scénarios de dangers

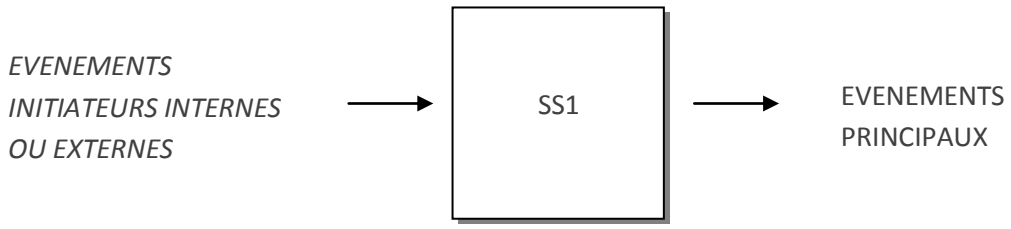
Dans beaucoup de cas on admet que les scénarios d'accidents sont connus notamment grâce au retour d'expérience. Il est cependant intéressant, voire indispensable de pouvoir générer des scénarios d'accidents possibles (ou plus généralement des scénarios d'ENS) et notamment de faire apparaître les principaux. Ceci permet en effet :

- de démontrer leur genèse
- d'identifier leurs multiples variantes
- d'identifier des scénarios insoupçonnés
- d'en faire par la suite l'ossature des arbres logiques montrant l'enchaînement de tous les événements conduisant à un ENS.

La technique développée ci-après permet de faire ce travail.

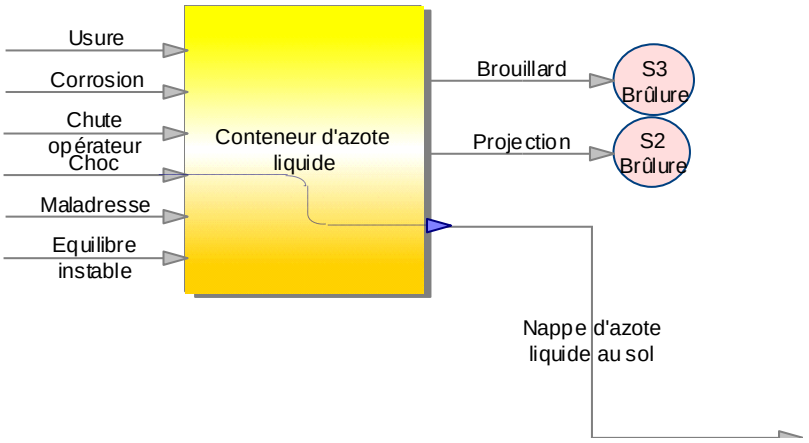
6.4.1 *Mettre chaque sous système sous forme d'une boîte noire*

En reprenant chaque sous système dans les diagrammes de processus de danger on les représente sous forme de boîtes noires (ou autres couleurs) dont les entrées sont les événements initiateurs d'origine interne ou externe et les sorties sont les événements principaux.



Ce travail est une simple compilation des diagrammes de processus de danger facilité par des fonctions de reprise des objets systèmes depuis la base de données.

Pour le sous système « Conteneur d'azote liquide » on obtient la boîte noire (ici jaune) ci-dessous

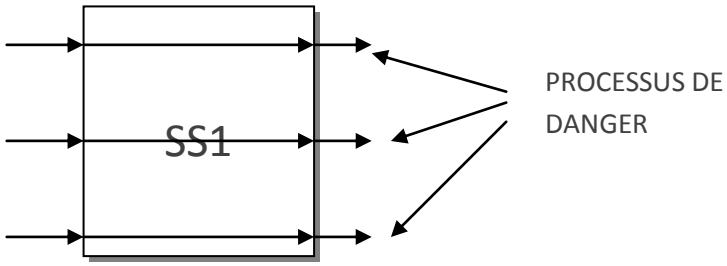


On peut remarquer :

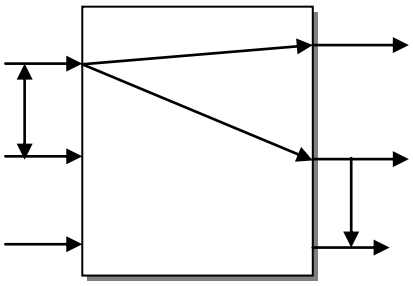
- Que dans les événements de sortie on trouve des événements qui peuvent avoir des ENS différents avec éventuellement des conséquences différentes.

6.4.2 *Génération de scénarios courts et de scénarios d'autodestruction*

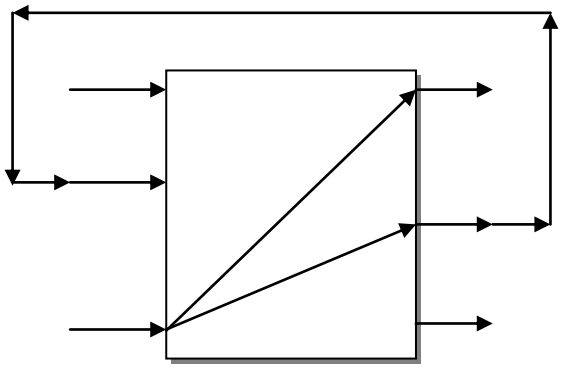
Pour l'instant nous n'avons, dans la génération de processus, fait apparaître que des liaisons directes entre les événements d'entrée et de sortie des boîtes noires.



Il faut maintenant combiner les événements d'entrée entre eux, les événements de sortie entre eux et identifier les retours en bouclage des événements de sortie et des événements d'entrée. Les deux premières opérations mettent en évidence des scénarios courts et la dernière des scénarios qui entraînent une autodestruction du sous système.



Scénario court

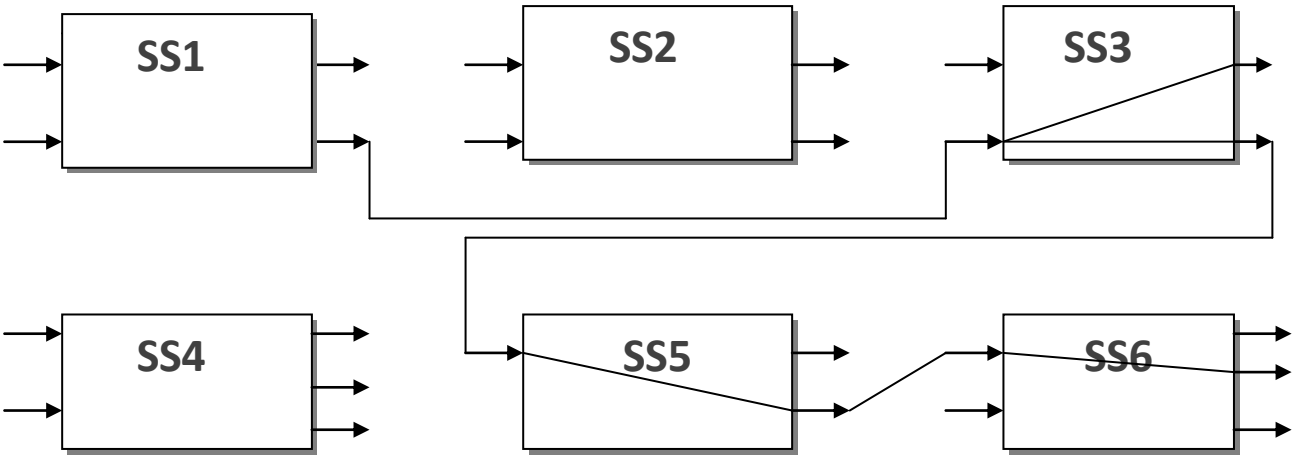


Scénario d'autodestruction

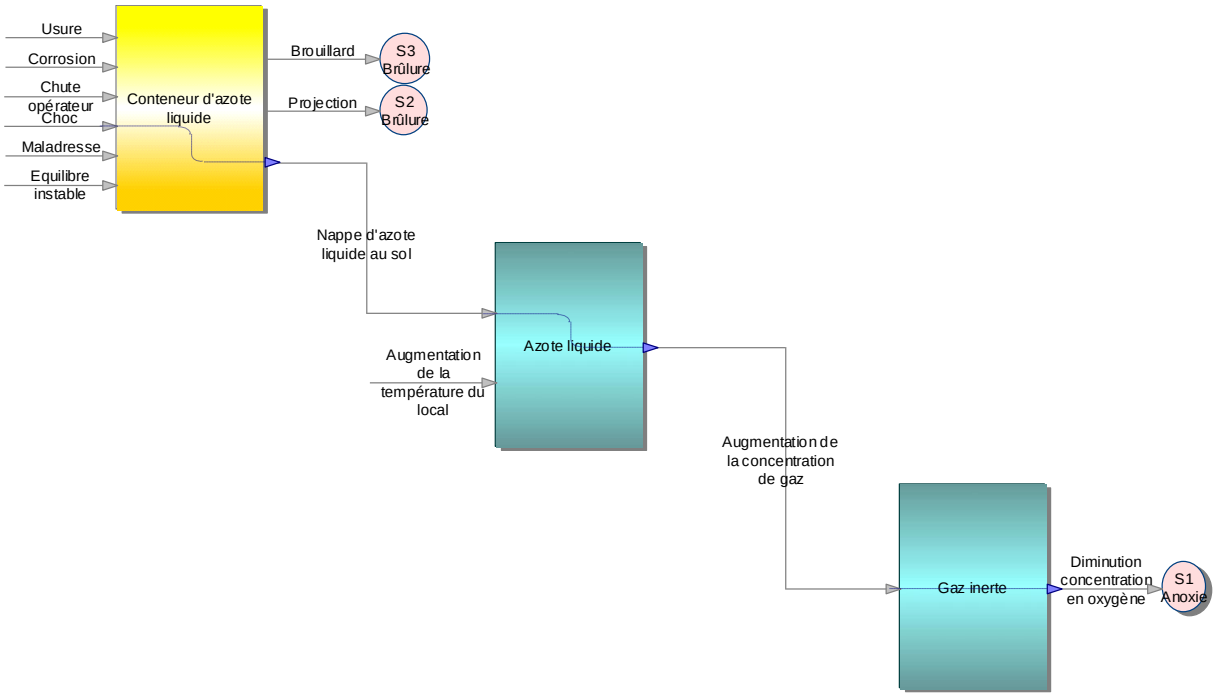
6.4.3 *Génération de scénarios longs, validation de ces derniers et construction d'arbres logiques sur les accidents principaux ainsi identifiés*

Si l'on met toutes les boîtes noires sur une même page, il est possible de relier les sorties de certaines boîtes qui sont de même nature (repérées en principe par les même mots) que les entrées d'autres boîtes.

On obtient ainsi des scénarios longs d'enchaînements d'événements ou scénarios de proximité ou aussi scénarios principaux d'ENS (accidents).



Pour l'installation de distribution d'argon nous avons toutes les boîtes noires suivantes :

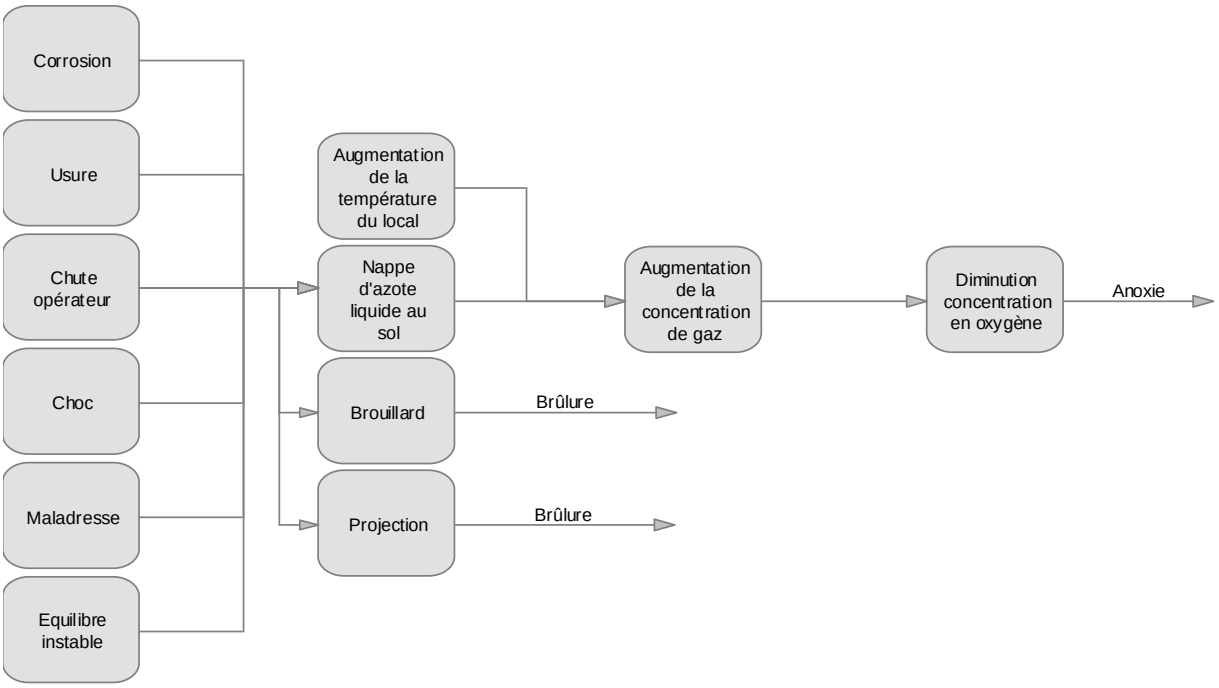


Ainsi nous découvrons qu'il y a un danger d'anoxie.

A partir des scénarios longs et des scénarios courts on peut construire, en les concaténant (rassemblant) sur un même événement, un arbre logique qui est la première représentation des événements s'enchaînant pour générer un ENS.

Par exemple, pour l'installation de distribution d'argon, on peut rassembler quelques scénarios conduisant à l'anoxie de l'employé :

Pour notre exemple, on retient l'arbre logique



REMARQUE :

- l'événement initiateur considéré peut conduire à plusieurs, voire à une multitude de processus. On est donc placé là devant l'incertitude et la difficulté de prévisibilité des risques. Nous pouvons distinguer l'incertitude paramétrique liée à une imprécision des paramètres des processus et l'incertitude systémique liées à l'identification des processus possibles et à l'ambigüité des enchaînements et des combinaisons possibles de ces processus. Les outils présentés nous aident à résoudre ces problèmes.

- Le nombre de scénarios construits avec les boîtes noires n'est pas infini mais il peut être très grand. Pour éviter une explosion combinatoire et guider le travail on peut choisir les événements majeurs qui apparaissent à la sortie des boîtes noires en tant qu'événements principaux, et rechercher quels sont les scénarios qui aboutissent à cet événement. On raisonne alors par déduction. C'est le cas par exemple de l'anoxie mais aussi de *BLESSURE DE L'EMPLOYE.*

- La liaison entre les sorties et les entrées des boîtes noires est en théorie une liaison directe (on relie les mêmes mots correspondant aux mêmes types de processus, par exemple ''Nappe d'azote liquide au sol'' généré par le containeur d'azote liquide. Cette tâche peut être grandement facilitée par l'utilisation d'un outil spécialisé tel qu'**Envision Risks Mosar**©). Cette vision idéale est cependant rarement opérationnelle. Il faut donc se servir ici de son imagination, de son intuition et de son expérience pour relier des entrées et sortie qui n'apparaissent pas à priori comme directement connectables. Une phase de mise en cohérence des libellés des événements est souvent nécessaire.

- On obtient des scénarios PLAUSIBLES. Pour décider s'ils sont possibles, il est nécessaire de vérifier si les enchaînements sont possibles. Pour cela il faut évaluer quantitativement ou qualitativement les distances qui peuvent être franchies par les événements, les impacts entre les sous systèmes et leurs effets. Ceci fait appel à l'évaluation des scénarios que nous verrons plus en détail ci-après. Il faut aussi évaluer si la probabilité des enchaînements d'événements est possible. Cependant il faut se méfier des scénarios qui pourraient apparaître comme fantasques parce que très peu probables. Le retour d'expérience montre que l'enchaînement d'événements est souvent fantastiquement long et il vaut sans doute mieux travailler sur ces scénarios et vérifier qu'ils sont maîtrisables plutôt que de les éliminer à priori.

6.5 Evaluation des scénarios de risques

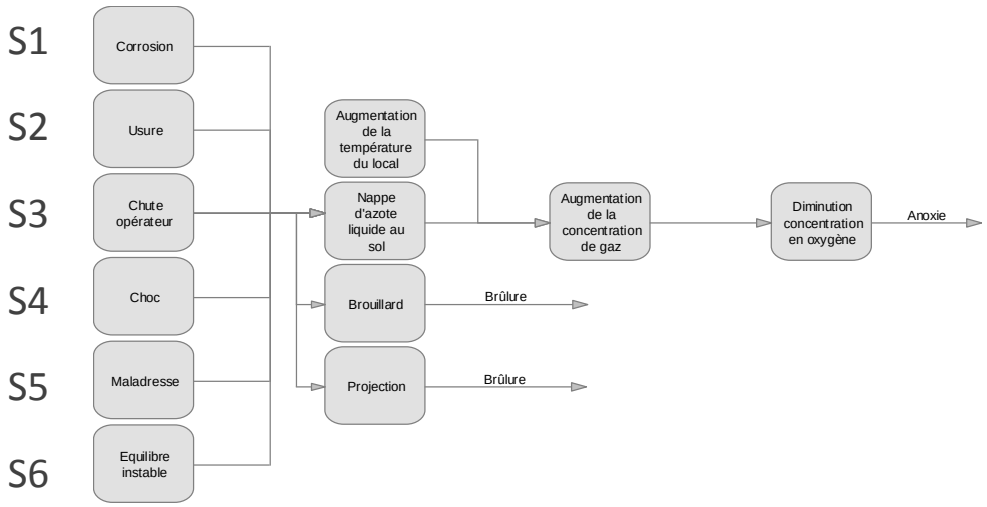
6.5.1 Evaluation quantitative ou qualitative

Comme nous l'avons vu en partie ci-dessus, cette étape permet d'évaluer *quantitativement* si c'est possible (par le calcul éventuellement à l'aide de logiciels) ou *qualitativement* par travail de groupe ou le jugement d'experts si le calcul n'est pas possible, les caractéristiques des différents événements identifiés et leurs interactions avec les sous-systèmes. Il existe de nombreux outils logiciels que l'on peut mettre en œuvre à ce niveau de l'analyse pour calculer des diffusions atmosphériques de produits, calculer les caractéristiques de formations de nappes de produits toxiques et établir l'évaluation de leurs effets en fonction de la distance des cibles, calculer les caractéristiques de formation de nappe de produits inflammables ou explosifs et déterminer leur effets en fonction de la distance des cibles.

Il est aussi nécessaire d'évaluer quelles cibles les événements principaux vont pouvoir atteindre et quel sera leur impact sur ces cibles. L'atteinte des cibles ainsi que leur nature (une ou plusieurs des quatre possibles) dépend des caractéristiques évaluées des scénarios et de leur distances par rapport aux événements finaux.

Dans l'installation de distribution d'argon :

Si l'on reprend l'arbre logique précédent, on peut faire les constats suivants :



- Tous les scénarios (S1…S6) n'ont la même gravité puisque qu'il y a brulure ou anoxie. Ceci n'est pas valable pour tous les cas et dépend des événements finaux choisis. Dans certains cas la gravité est la même pour tous les scénarios.

- Tous les scénarios atteignent une des quatre cibles possibles.

- Pour évaluer leurs caractéristiques, le calcul est possible : calcul des débits de fuite en phase gazeuse ou liquide ou en double phase, calcul de diffusion de l'azote gazeux dans l'air et des caractéristiques des nappes formées, calcul des caractéristiques d'anoxie et de leurs effets. Il existe *des logiciels* permettant de conduire tous ces calculs.

- Les scénarios se distinguent les uns des autres par leur probabilité différente. Par exemple le scénario 1 est bien moins probable que le scénario 3 ou les scénarios 4 et 5. A ce niveau de l'analyse on ne peut pas cependant calculer ces probabilités. D'où l'intérêt de pouvoir disposer d'une grille permettant de hiérarchiser les scénarios, ce que nous allons voir dans l'étape suivante.

- On peut aussi évaluer le coût des accidents.

6.6 Négociation d'objectifs et hiérarchisation des scénarios

6.6.1 Négociation de grilles gravité x probabilité

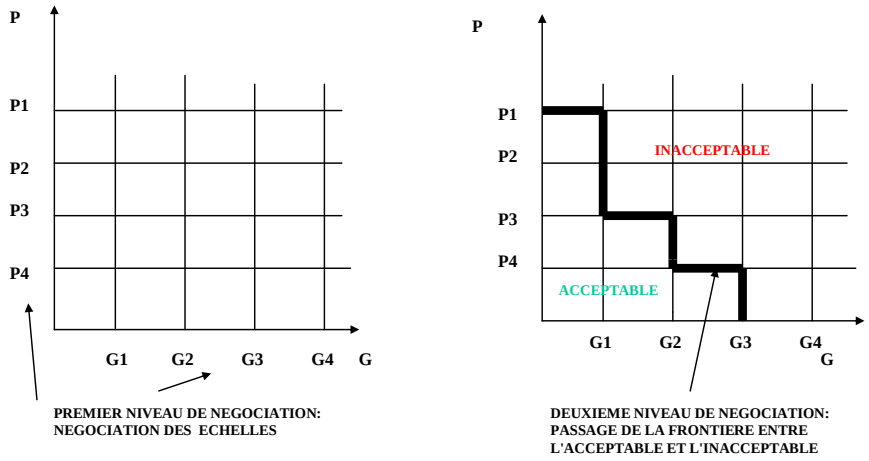
Jusqu'ici nous n'avons pas situé le travail d'analyse par rapport à des *objectifs*. La mise en évidence de scénarios de risques et leur évaluation permet de mieux définir ces objectifs.

Dans un premier temps, il est nécessaire de construire un outil qui permettra de concrétiser ces objectifs. Celui choisi est la grille gravité x probabilité. On peut en construire une par cible.

Prenons le cas d'une grille pour les opérateurs (ici l'employé) :

La première chose à faire est de négocier les niveaux des deux axes de la grille. En principe on construit des axes à 4, 6 ou 8 niveaux (toujours en nombre pair pour éviter la tendance à se situer dans un niveau médian).

La deuxième chose à faire est de situer dans la grille la frontière entre ce qui est considéré comme acceptable et ce qui est considéré comme inacceptable. Ceci constitue un deuxième niveau de négociation.

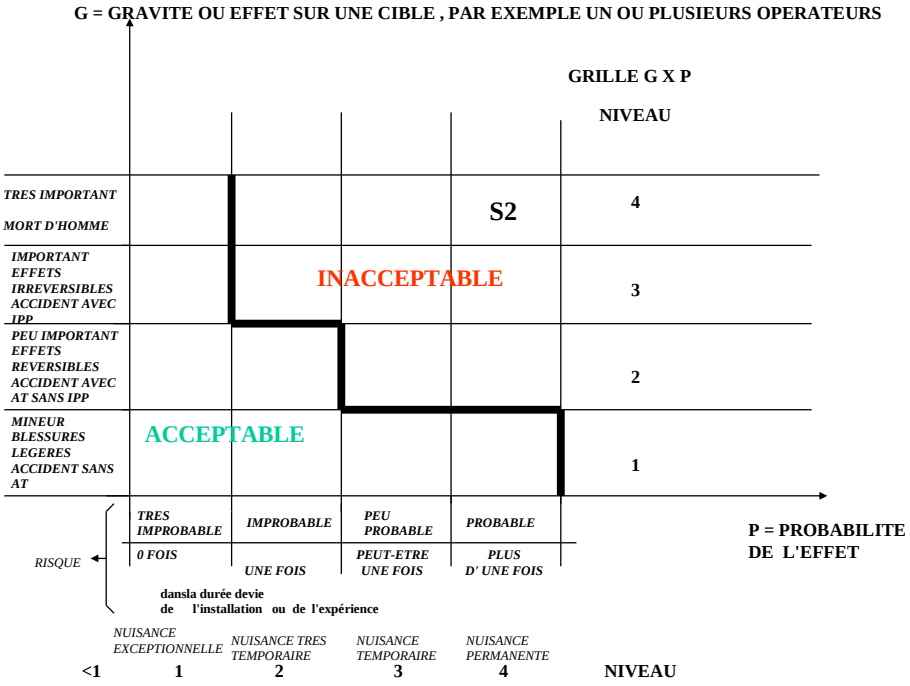


NEGOCIATION DE GRILLES GRAVITE-PROBABILITE ET SITUATION DES SCENARIOS DANS CES GRILLES

Pour l'installation d'argon, la grille ci-après est une grille possible pour situer les risques pour les opérateurs. Admettons bien sûr qu'elle ait été négociée par les acteurs concernés et notamment avec les opérateurs.

6.6.2 Situation des scénarios dans les grilles GxP et hiérarchisation de ces derniers

Il est alors possible d'y situer le scénario S2 qui est au niveau 4 en probabilité et au niveau 4 en gravité.



De la même manière on pourrait construire d'autres grilles GxP pour les autres cibles et y situer leurs scénarios.

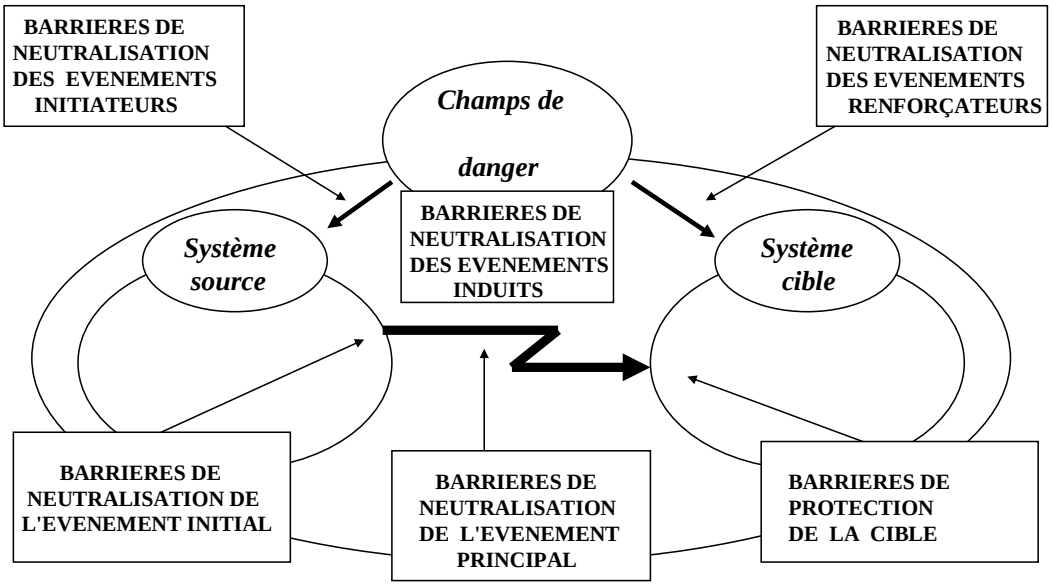
REMARQUE :

On peut aussi construire des grilles concernant le coût des accidents en prenant en compte par exemple le coût de la perte de production ou de la perte de l'outil de travail en fonction du temps ce qui permet de hiérarchiser les scénarios en fonction de cette perte.

6.7 Définition des moyens de prévention et de protection et qualification de ces moyens

6.7.1 Identification des barrières de prévention et de protection

Ces barrières vont permettre, comme nous l'avons vu plus haut, de neutraliser les scénarios identifiés.



APPROCHE DETERMINISTE OU DE DIMENSIONNEMENT

Le schéma ci-dessus montre bien les différentes barrières nécessaires pour neutraliser l'enchaînement des événements et donc des scénarios.

L'arbre logique montre, lui, qu'en principe il suffit de neutraliser les événements primaires (ceux qui apparaissent les premiers) pour que le scénario correspondant n'ait pas lieu. Pour renforcer la prévention on recherche aussi les barrières possibles tout le long du scénario aussi bien sur les événements que sur leurs enchaînements. Par exemple un équipement protégeant le conteneur d'azote liquide contre le renversement, pour éviter les nappes d'azote liquide au sol.

6.7.2 Types de barrières

On distinguera deux types de barrières :

a) LES BARRIERES TECHNOLOGIQUES (BT)

Elément ou ensemble technologique faisant partie intégrante de l'installation, qui s'oppose automatiquement à l'apparition d'un événement préjudiciable à la sécurité et qui ne nécessite pas d'intervention humaine.

Elle peut être statique (exemples : écran fixe, capot de protection, enceinte de confinement) ou dynamique (exemples : soupape de sécurité à ouverture automatique, éléments de contrôle commande.

b) LES BARRIERES OPERATOIRES OU D'UTILISATION (BU)

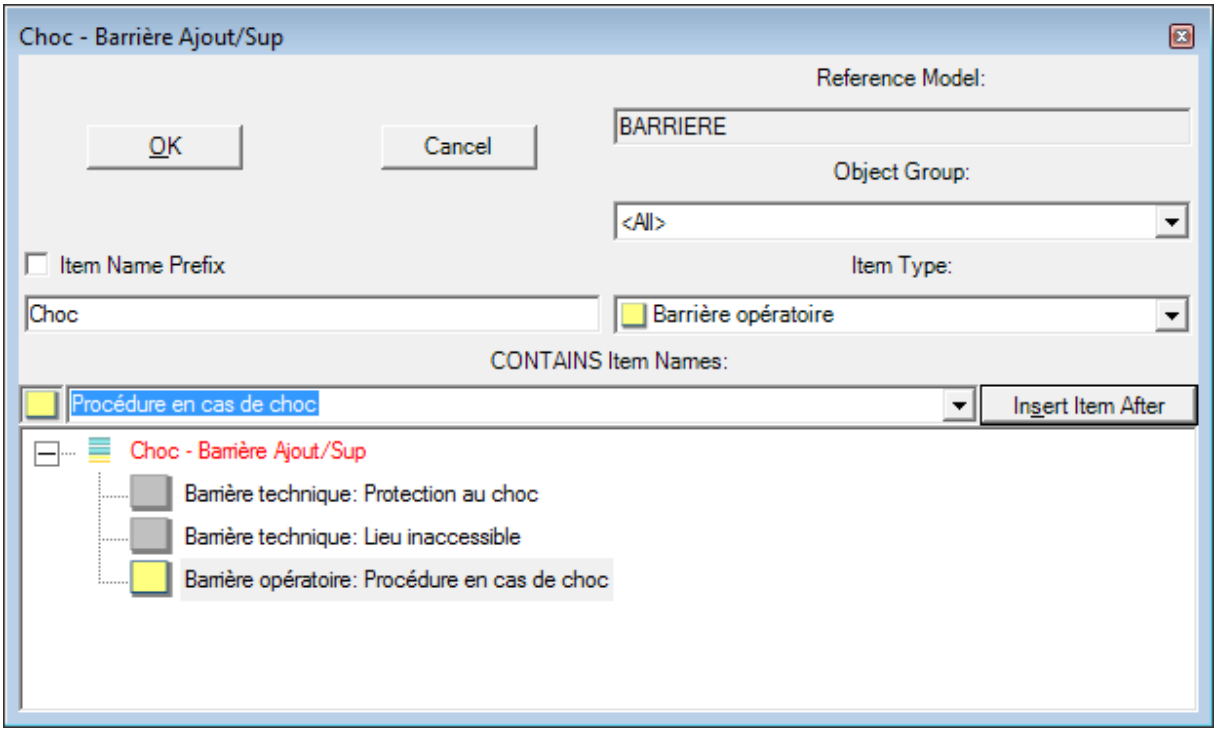
Action nécessitant une intervention humaine, reposant sur une consigne précise, activée ou non par un élément ou un ensemble technologique. (Exemples : procédure, mode opératoire, application de règles, vanne à ouverture manuelle, protections individuelle).

Les BU sont souvent considérées comme étant plus faibles que les BT.

Elles sont en fait très sensibles à la formation, et notamment à la formation sécurité, des opérateurs.

L'identification des barrières peut se faire classiquement à l'aide d'un tableau. Dans notre cas, l'outil utilisé permet de réaliser cette opération directement depuis les diagrammes des processus de danger, en cliquant sur un événement du diagramme. Dans ce cas, le tableau sera généré à la demande et automatiquement par l'outil.

Ci-dessous – Boite de dialogue permettant d'ajouter (associer) des barrières à un événement d'un processus de danger



6.7.3 Analyse de risques : Tableau B

(Tableau partiel, généré automatiquement par l'outil)

Source de danger	Phase de vie	Evénements				
2 - Le container d'azote liquide	Exploitation	Nom	Barrières			
		Percement	Nom	Coût	Taux	Etat
			Double coque	40	20	A définir
		Nom	Barrières			
		Nappe d'azote liquide au sol	Nom	Coût	Taux	Etat
			Détecteur de liquide	1000	80	A définir
		Nom	Barrières			
		Choc	Nom	Coût	Taux	Etat
			Protection au choc	30	30	Ex - existant
			Nom	Coût	Taux	Etat
			Lieu inaccessible	102	50	In - à installer
			Nom	Coût	Taux	Etat
			Procédure en cas de choc	20	40	A définir
		Nom	Barrières			
		Corrosion	Nom	Coût	Taux	Etat
			Traitement périodique anti corrosion	50	80	A définir
		Nom	Barrières			
		Usure	Nom	Coût	Taux	Etat
			Replacement container	2500	100	A définir

REMARQUES SUR LES BARRIERES

- Les premières barrières recherchées sont les barrières de conception. En effet on commence toujours par travailler la prévention et la protection collectives, la protection individuelle n'intervenant que si la protection collective est insuffisante car elle introduit des nuisances. Ces barrières sont des BT.
- La ventilation est une barrière importante qui fait partie des barrières de conception. On l'identifie à part. Elle intervient sur l'événement principal ou flux (c'est un absorbeur de flux).
- L'habilitation est une procédure écrite (avec cosignature de l'habiliteur et de l'habilité) qui consiste à confier à un exécutant un travail décrit pour lequel l'habiliteur s'est assuré que l'habilité a la connaissance des risques, les moyens et l'autorité d'assurer ce travail.

- L'identification des facteurs d'ambiance ne conduit pas forcément à une définition de barrières mais il peut la faciliter. Il est une introduction à l'approche ergonomique.
- Les consignations sont des procédures qui consistent à mettre en sécurité une installation ou une partie d'installation de manière à ce que même si quelqu'un veut la remettre en fonctionnement, il ne puisse pas le faire. Elles font l'objet de verrouillages avec clef unique possédée par le consignateur seul.
- L'implantation consiste à définir quelle est la meilleure implantation possible compte tenu des risques identifiés et de l'environnement.
- L'influence sur l'environnement permet de définir quelle est l'influence du scénario sur l'environnement passif et de rechercher les barrières adéquates.

Notez que dans ce tableau, des champs paramétrables et spécifiques à l'outil employé ont été ajoutés pour permettre une analyse de la valeur des barrières. En effet les budgets « sûreté-sécurité » sont très souvent limités et une optimisation coûts/résultats est recherchée.

6.7.4 Qualification des barrières de prévention et de protection

Une fois les barrières définies, il faut s'assurer qu'elles ne présentent ou ne génèrent pas de risques, et il faut les qualifier dans le temps c'est à dire s'assurer de leur pérennité.

Pour cela on constate que si l'on introduit chaque barrière dans le tableau B (baptisé alors tableau C), un certain nombre de rubriques de ce tableau permettent de répondre aux deux contraintes définies ci-dessus. Illustrons ceci avec l'installation argon.

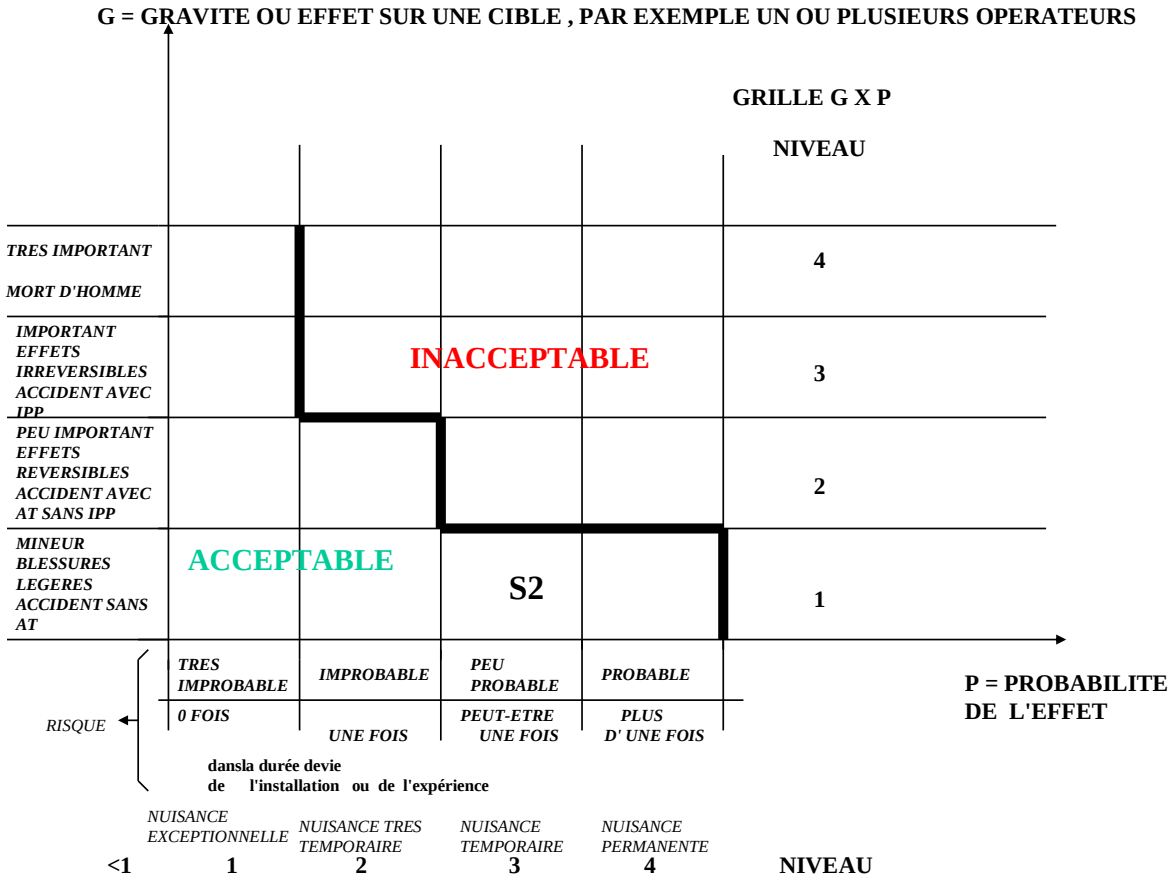
6.7.5 Tableau des barrières (Tableau partiel)

TABLEAU C					
BARRIERES DE: 1-1 Conception	Scénario	Type	Eléments de conception de ces barrières	Contrôles et vérifications techniques	Maintenance
Bloc de protection	1	BT	A2 Note de calcul de résistance A3 Bon équilibrage A4 Manutention facile A9 Montage anti-vibratoire C1 Double coque	Déjà pris en compte	Déjà pris en compte

Le tableau montre que la colonne conception, introduit un nouveau système « Bloc de protection » dans l'analyse. Il convient de vérifier maintenant que ce nouvel élément n'engendre par l'arrivée de nouveau ENS. Si doute, nous devons alors faire un nouveau processus de danger pour cet élément.

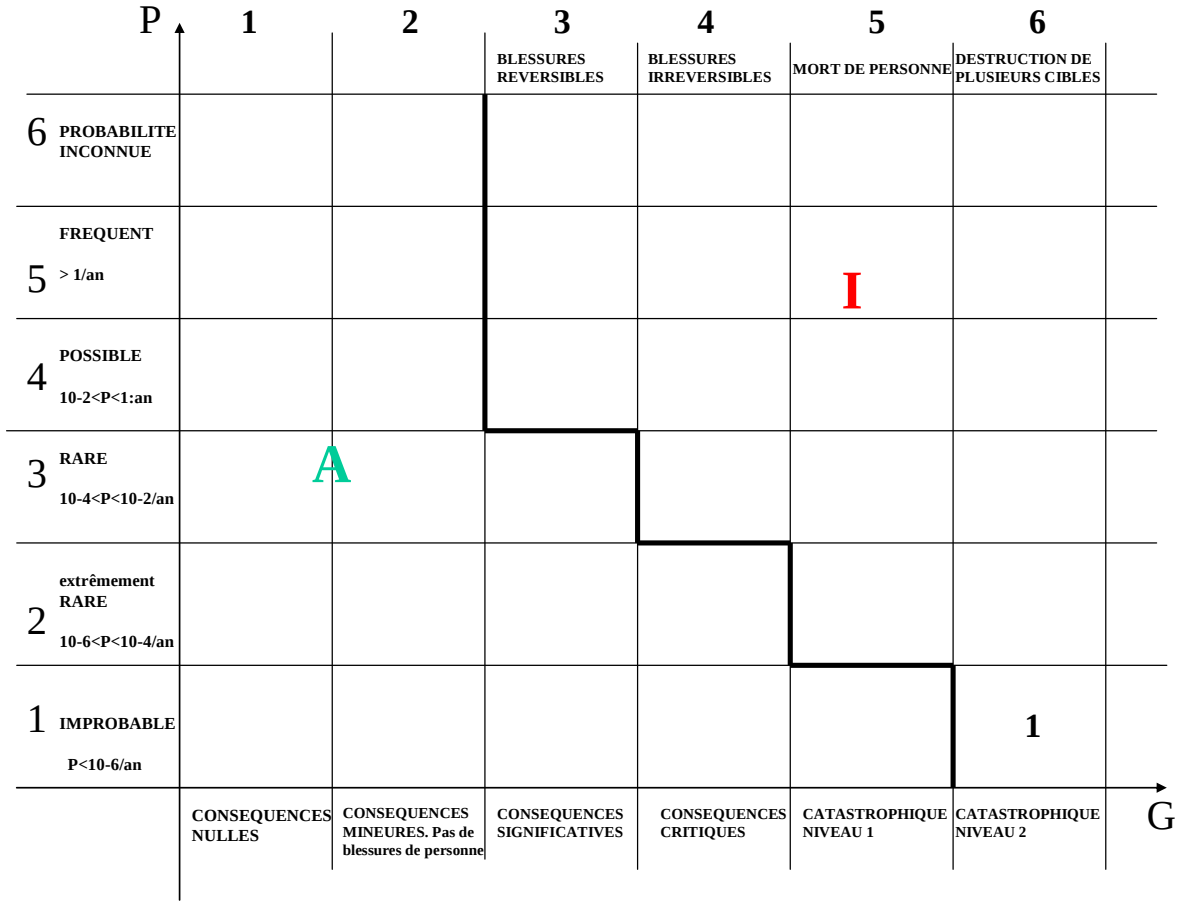
6.7.6 Nouvelle situation des scénarios dans les grilles GxP

Il est possible de vérifier comment les barrières font évoluer les scénarios dans leur position dans les grilles G x P. Commençons par le scénario S2 :



On peut admettre, compte tenu des barrières envisagées, que gravité et probabilité seront diminués et que cet ENS sera peu probable et avec des conséquences mineures. Cette décision sera prise par le groupe de travail après discussion d'évaluation.

Pour ce qui concerne maintenant l'anoxie :



Les scénarios 1 à 6, après mise en place des barrières, gardent le même niveau de gravité car, s'ils arrivent, aucune barrière ne peut en diminuer les effets mais leur probabilité est fortement diminuée et ils deviennent improbables.

Il s'agit alors du **RISQUE RESIDUEL**.

Le MODULE A de la méthode MOSAR est terminé. C'est en fait la partie la plus originale.

Nous avons fait une analyse principale de sécurité de l'installation ou une analyse des risques principaux de l'installation.

Dans la plupart des cas cette analyse est suffisante. Mais il peut être nécessaire d'aller plus loin soit parce qu'on le décide pour parachever l'analyse et aller jusqu'à la mise en place d'une culture de sécurité, soit parce qu'une réglementation l'impose (installations classées par exemple). On entrera alors dans le module B de la méthode. Mais ceci est une autre histoire…

Les diagrammes colorés illustrant ce document ont été réalisés avec le logiciel d'analyse de risques ***Envision Risks Mosar©.***
Pour en savoir plus : www.case-france.com/envisionrisks2.htm

***

*

Table des matières