I. GÉNÉRALITÉS

L'approche par barrières consiste tout d'abord à vérifier, sur la base de certains critères, si la barrière de sécurité peut être retenue pour le scénario étudié. Il est ensuite attribué un niveau de confiance aux barrières de sécurité retenues.

La combinaison de la fréquence d'occurrence de l'événement initiateur et des niveaux de confiance des barrières de sécurité participant à la maîtrise d'un même scénario, permet d'estimer une classe de probabilité d'occurrence du scénario.

Cette démarche découle de travaux menés par l'INERIS dans le cadre de programmes de recherche financés par le Ministère chargé de l'environnement, à savoir le DRA 39 « *Évaluation des barrières de sécurité de prévention et de protection utilisées pour réduire les risques d'accidents majeurs* », le DRA-34 « *Analyse des risques et prévention des accidents majeurs* », ainsi que de diverses études réalisées par la Direction des Risques Accidentels.

La probabilité d'un évènement initiateur est issue de l'expérience et elle inclut des barrières de sécurité et leur efficacité. On considère notamment :

- la résistance des matériels mis en jeu,
- les procédures internes de sécurité mises en œuvre,
- les procédures de sécurité qui permettent d'éviter l'évènement initiateur (source d'ignition par exemple).

Cependant, la probabilité des événements initiateurs reste très souvent aléatoire, en l'absence de données bibliographiques suffisantes à l'heure actuelle.

En conséquence, dans la présente étude, la démarche suivante a été retenue :

1. Prise en compte de la probabilité de l'événement initiateur lorsque celle-ci existe et s'avère fiable.
2. Prise en compte des barrières organisationnelles et techniques (ainsi que des caractéristiques intrinsèques) mises en place au regard des événements courants pour déterminer la probabilité de l'événement initiateur, chaque événement courant ayant par défaut une probabilité initiale de 1 (évènement courant).
3. Comparaison, lorsque cela s'avère possible, de la probabilité de l'événement initiateur avec la probabilité du même événement initiateur déterminé pour une autre branche d'activité.

II. DÉFINITIONS

Afin de faciliter la compréhension de la démarche d'évaluation de la probabilité d'un évènement dangereux, on précisera ci-après quelques définitions sur les termes employés :

- **Barrière technique de sécurité (BTS)** : barrière qui permet d'assurer une fonction de sécurité. Elle est constituée d'un dispositif de sécurité ou d'un système instrumenté de sécurité qui s'oppose à l'enchaînement d'événements susceptibles d'aboutir à un accident.
- **Dispositif de sécurité** : c'est en général un élément unitaire, autonome, ayant pour objectif de remplir une fonction de sécurité, dans sa globalité. On distingue :
    - le dispositif passif, qui ne met en jeu aucun système mécanique (mur coupe-feu, rétention, etc.),
    - le dispositif actif, qui met en jeu un dispositif mécanique (ressort, levier, etc.).

- **Efficacité** : l'efficacité d'une BTS est évaluée au regard de son aptitude à remplir la fonction de sécurité pour laquelle elle a été choisie, dans son contexte d'utilisation et pendant une durée donnée de fonctionnement. Cette aptitude s'exprime en pourcentage d'accomplissement de la fonction définie, en considérant un fonctionnement normal (non dégradé). Ce pourcentage peut varier pendant la durée de sollicitation de la barrière technique de sécurité.
- **Système instrumenté de sécurité (SIS)** : combinaison de capteurs, d'unité de traitement et d'actionneurs (équipements de sécurité) ayant pour objectif de remplir une fonction ou sous fonction de sécurité.
- **Equipement de sécurité** : élément d'un SIS qui remplit une sous-fonction de sécurité.
- **Fonction de sécurité** : fonction ayant pour but la prévention et la protection d'événements redoutés. Les fonctions de sécurité identifiées peuvent être assurées à partir de barrières techniques de sécurité, de barrières organisationnelles (activités humaines), ou plus généralement par la combinaison des deux.

Une même fonction de sécurité peut être réalisée par différentes barrières de sécurité.

Une fonction de sécurité peut se décomposer en sous-fonctions de sécurité liées.

- **Niveau de confiance (NC)** : c'est la classe de probabilité de défaillance à la sollicitation de la mesure de sécurité, dans son environnement d'utilisation, soit la probabilité qu'elle n'assure pas la fonction de sécurité pour laquelle elle a été choisie lorsqu'elle est sollicitée.
- **Principe de concept éprouvé** : un équipement simple est de conception éprouvée soit, lorsqu'il a subi des tests de « qualification » par l'utilisateur ou d'autres organismes, soit lorsqu'il est utilisé depuis plusieurs années sur des sites industriels et que le retour d'expérience sur son application est positif. Pour cela, on peut s'appuyer sur :
    - le retour d'expérience de l'utilisateur (exploitant, service maintenance, inspection, etc.), voire du fournisseur,
    - l'accidentologie (retour d'expérience des accidents et incidents),
    - les standards indiqués par des syndicats professionnels.
- **Redondance** : existence, dans une entité, de plus d'un moyen pour accomplir une fonction requise.
- **Temps de réponse** : il correspond à l'intervalle de temps entre le moment où une barrière de sécurité, dans un contexte d'utilisation, est sollicitée et le moment où la fonction de sécurité assurée par cette barrière de sécurité est réalisée dans son intégralité. Il s'exprime en secondes.

III. DÉTERMINATION DES FRÉQUENCES D'OCCURRENCE DES ÉVÈNEMENTS INITIATEURS

Dans la réalisation des nœuds papillons, les évènements initiateurs interviennent uniquement dans l'arbre des causes. Pour chaque branche de cet arbre, on affecte une fréquence d'occurrence aux évènements issue de banques de données tels que Reference manual BEVI Risk Assessment, le Handbook for failure frequencies, etc.

Le retour d'expériences issu de l'accidentologie interne ou externe peut aussi être utilisé directement ou pour ajuster ou confirmer la fréquence d'occurrence retenue.

Ainsi, les évènements initiateurs des phénomènes dangereux sont combinés à des fréquences d'occurrence.

Bases de données disponibles :

Les bases de données gouvernementales telles que :

- le Reference manual BEVI risk assessment ,
- le Handbook for failure frequencies,
- le FRED 2.

D'autres données sont également accessibles :

- les bases de données issues d'un retour d'expérience des sociétés spécialisées (DOROTE, CHARAD, etc.),
- des banques de données issues de guide telles que :
    - ARAMIS,
    - DRA 34 – ope J – Intégration de la dimension probabiliste dans les analyses de risques – Partie 2 données quantitatives,
    - COVO,
    - OREDA,
    - EIREDA,
    - Guideline PERD 1989,
    - Last Fire,
    - LOPA,
    - Base de données de DNV.

IV. CRITÈRES DE PRISE EN COMPTE DES BARRIÈRES

Les performances des mesures de maîtrise des risques doivent être évaluées et justifiées. Plus généralement, pour être prises en compte dans l'évaluation de la probabilité, les mesures de sécurité indépendantes doivent répondre à quatre critères :

- Efficacité,
- Cinétique,
- Maintenabilité,
- Testabilité.

L'INERIS a par exemple proposé deux méthodes d'évaluation de la performance des mesures de maîtrise des risques[1] : l'une adaptée aux mesures techniques et la seconde méthode concernant les mesures organisationnelles, à travers des critères d'efficacité, d'indépendance, de temps de réponse et enfin, par l'attribution d'un niveau de confiance :

- **Indépendance** : il faut s'assurer que la mesure de sécurité est bien indépendante du procédé, des autres dispositifs et de l'exploitation.
- **Efficacité ou capacité de réalisation** (cf. définitions ci-dessus) : elle est liée au dimensionnement du dispositif. L'évaluation en termes de capacité de réalisation passe par l'étude de trois critères :
    - Concept éprouvé.

[1] OMEGA 10 – Evaluation des dispositifs de prévention et de protection utilisés pour réduire les risques d'accidents majeurs et OMEGA 20 – Démarche d'évaluation des barrières humaines de sécurité (date de publication : 10/10/06).

    - Dimensionnement adapté.
    - Résistance aux contraintes spécifiques.
- **Temps de réponse (cf. définitions ci-dessus)** : le temps de réponse est à comparer à la cinétique du phénomène.
- **Niveau de confiance (ou intégrité de sécurité)** : La probabilité est calculée pour une capacité de réalisation et un temps de réponse donnés. Elle est liée aux paramètres suivants :
    - Type d'architecture,
    - Principe de sécurité positive,
    - Tolérance à la première défaillance,
    - Comportement sur défaut (mise hors service, blocage ou dérive possible),
    - Maintien dans le temps de la qualité de la mesure (existence de procédures de tests réguliers, de maintenance préventive, de procédures d'installation ou d'inspection/audits internes).

Ainsi, ces mesures doivent tout d'abord répondre au même critère d'indépendance et sont regroupées en deux catégories : **les mesures de pré-dérive** (ex : contrôle d'une température avant la mise en œuvre du process) et les **mesures de rattrapage de dérive** (ex : extinction d'un incendie par un opérateur).

Pour évaluer la performance de ces mesures, des pré-requis sont indispensables : la formation et l'habilitation des opérateurs, la coordination et la communication opérationnelle des acteurs (notamment dans le cas d'un travail d'équipe), l'entraînement et les exercices, l'encadrement du recours à la sous-traitance, ainsi que le critère de disponibilité des opérateurs. Ces critères sont impératifs pour considérer qu'une mesure de ce type est efficace.

V. DÉTERMINATION DU NIVEAU DE CONFIANCE (NC) DES BARRIÈRES

Le niveau de confiance des barrières de sécurité est déterminé selon la méthode définie par l'INERIS. Le niveau de confiance ne se substitue pas aux normes NF-EN 61508 et CEI 61511 relatives à la sécurité fonctionnelle. La démarche proposée est une méthode d'évaluation qualitative « simple » en vue d'évaluer la performance des barrières techniques et humaines de sécurité.

Les niveaux de confiance des barrières de sécurité sont basés sur :

- la fiche N°7 de la circulaire du 10 mai 2010,
- le guide OMEGA 10 de l'INERIS portant sur l'évaluation des barrières techniques de sécurité,
- le guide OMEGA 20 de l'INERIS portant sur l'évaluation des barrières humaines de sécurité.

- **Cas des barrières techniques de sécurité**

Avant de déterminer ce niveau de confiance pour les barrières techniques de sécurité (BTS), il est important de vérifier que cette BTS est de concept éprouvé, qu'elle est indépendante du procédé et qu'elle est indépendante d'une autre BTS. Le niveau de confiance est ensuite déterminé par :

- une proportion de défaillance en sécurité (ou Safe Failure Fraction – SFF) qui correspond au rapport du taux de défaillances détectées sur la somme des taux de défaillances du système. Cette valeur est généralement inférieure à 60% mais qui selon les cas (bon retour d'expérience, essais, niveau SIL selon la norme NF-EN 61511, etc.) peut augmenter vers des niveaux (SFF) de l'ordre de 99%.
- une tolérance aux anomalies matérielles qui est l'équivalent d'une redondance.

On obtient alors un niveau de confiance défini selon les grilles données dans le rapport Oméga 10 de l'INERIS pour les systèmes techniques dits « simples » (vannes, relais, interrupteurs…) ou « complexes » (système capable de traiter une information).

Proportion de défaillances en sécurité	**Tolérances aux anomalies matérielles** (selon le nombre d'équipements de sécurité)		
	0	**1**	**2**
<60%	NC1	NC2	NC3
60 – 90 %	NC2	NC3	NC4
90 – 99 %	NC3	NC4	NC4
> 99 %	NC3	NC4	NC4

Tableau 1 : Niveaux de confiance pour des systèmes techniques simples de sécurité (Extrait et adapté de la norme CEI-EN 61508 /Tab.1 de l'Omega 10)

Proportion de défaillances en sécurité	**Tolérances aux anomalies matérielles** (selon le nombre d'équipements de sécurité)		
	0	**1**	**2**
<60%	NC0	NC1	NC2
60 – 90 %	NC1	NC2	NC3
90 – 99 %	NC2	NC3	NC4

> 99 %	NC3	NC4	NC4

Tableau 2 : Niveaux de confiance pour des systèmes techniques complexes de sécurité (Extrait et adapté de la norme CEI-EN 61508 / Tab.2 de l'Omega 10)

- **Cas des dispositifs passifs de sécurité**

Pour déterminer le niveau de confiance d'un dispositif passif de sécurité (cuvette de rétention, mur coupe-feu, etc.), il faut déterminer sa probabilité moyenne de défaillance (ou taux de défaillance à la sollicitation/PFD).

Une fois celle-ci estimée, le tableau ci-après, qui est inspiré de la norme NF EN 61508, permet de faire le lien avec le niveau de confiance.

Probabilité moyenne de défaillance	Sens d'évolution de la probabilité de défaillance	Niveau de confiance
$10^{-5} \leq PFD < 10^{-4}$	↓	NC4
$10^{-4} \leq PFD < 10^{-3}$		NC3
$10^{-3} \leq PFD < 10^{-2}$		NC2
$10^{-2} \leq PFD < 10^{-1}$		NC1

Tableau 3 : Evaluation d'un niveau de confiance en fonction de sa probabilité moyenne de défaillance (Tab.5 de l'Omega 10)

L'exploitation des bases de données montre que le NC pour les murs coupe-feu et les cuvettes de rétention serait de 2.

Le niveau de confiance pourra être maintenu ou décoté en fonction des procédures et des moyens (maintenance, inspection, etc.) mis en œuvre par l'industriel pour maintenir dans le temps le niveau de confiance du dispositif.

Note : en l'absence d'études spécifiques ou d'un retour d'expérience suffisant permettant d'apprécier la probabilité de défaillance d'un système, le niveau de confiance retenu par défaut sera NC1.

- **Cas des barrières humaines de sécurité**

Les barrières humaines de sécurité sont constituées d'une activité humaine (une ou plusieurs opérations) qui s'opposent à l'enchainement d'évènements susceptibles d'aboutir à un accident.

Le niveau de confiance d'une barrière humaine est déterminé selon la méthode INERIS (document Omega 20) proposant de décomposer les barrières humaines de sécurité en trois principales sous-tâches : détection, diagnostic et action.

Le niveau de confiance initial à retenir est déterminé selon les critères suivants :

- le niveau de confiance maximal d'une barrière humaine de sécurité est de 2,
- le niveau de confiance retenu correspond à la différence entre le niveau de confiance optimal (2) et la somme des décotes définies pour chacune des sous-fonctions (détection, diagnostic et action),
- selon le niveau de décote associé à la barrière analysée, le niveau de confiance final pourra être de 2, 1 ou 0.

Le niveau de confiance pourra être maintenu ou décoté, en fonction :

- de la simplicité de détection de l'évènement anormal,

- de la simplicité du diagnostic, quant aux choix de l'opération à mener pour empêcher le scénario redouté de se produire,
- de la simplicité de l'action de sécurité à conduire pour éviter ou en réduire les effets,
- de la pression temporelle à laquelle sont soumis les intervenants, si le temps d'intervention doit être bref ou si la cinétique des événements menant à l'accident est rapide.

Dans le cas d'une mesure de pré-dérive, cette mesure sera cotée NC2 si elle est réalisée par une personne dédiée spécifiquement à cette action (spécialiste) et NC1 si elle est réalisée par l'opérateur chargé du process.

- **Formations et consignes**

Les formations et consignes de sécurité sont des éléments qui participent à la fiabilité et au maintien du niveau de confiance d'autres barrières de sécurité ou à la probabilité de l'événement initiateur. De ce fait, aucun niveau de confiance ne leur est appliqué de manière spécifique et elles ne sont pas prises en compte dans la détermination de la probabilité.

VI. DÉTERMINATION DE LA PROBABILITÉ

Pour rappel, il existe cinq classes de probabilités définies dans l'arrêté du 29/09/2005. Elles sont indiquées ci-dessous :

Classe	E	D	C	B	A
Probabilité	10^{-5}		10^{-4}	10^{-3}	10^{-2}

Tableau 4 : Classes de probabilités définies par l'arrêté du 29 septembre 2005

Cette probabilité d'occurrence du phénomène dangereux est amalgamée à sa fréquence d'occurrence future estimée sur l'installation par an.

La probabilité d'occurrence du phénomène dangereux est déterminée à partir des arbres des causes et des conséquences. L'ensemble étant retranscrit dans un logigramme.

- **Formation de l'arbre des causes**

L'arbre des causes permet de déterminer la probabilité d'occurrence d'un évènement redouté central. Les évènements initiateurs ainsi que les barrières permettant d'en limiter leur fréquence d'occurrence sont rassemblés par le biais de portes logiques afin d'atteindre un unique évènement commun qui est l'ERC.

Le logigramme suivant permet d'illustrer ces arrangements d'évènements de barrières conduisant à un ERC :

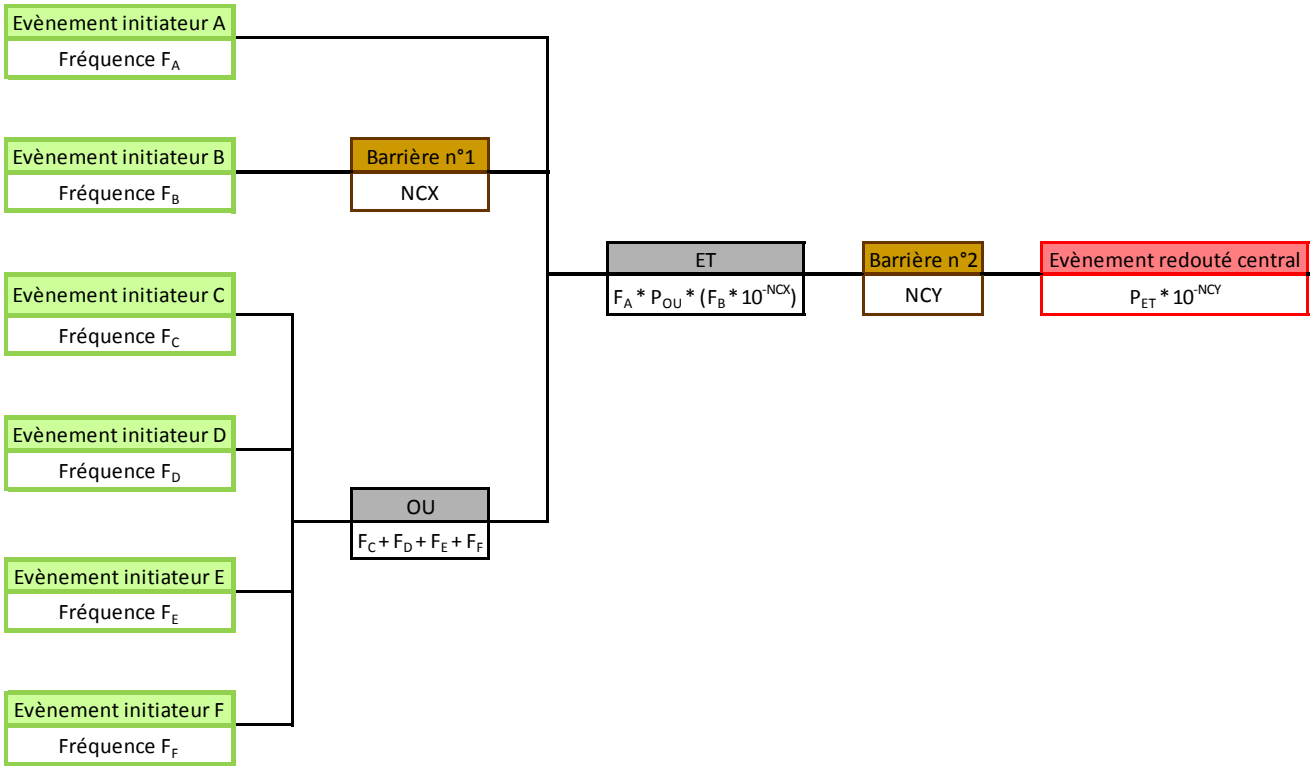

Figure 1 : Illustration d'un arbre des causes

Deux types de portes peuvent être observés sur ce logigramme :

- les portes « ET » : l'évènement intermédiaire se produit lorsque deux évènements initiateurs indépendants ont lieu simultanément,
- les portes « OU » : plusieurs évènements initiateurs peuvent aboutir au même évènement intermédiaire.

Lors de passage de portes « ET », les règles de détermination de probabilités est réalisée par la multiplication des fréquences des évènements initiateurs :

$$f_{Ei} = f_{EIA} \times f_{EIB}$$

Lors de passage de portes « OU », la règle de détermination de probabilités est réalisée par l'addition des fréquences des évènements initiateurs :

$$f_{Ei} = f_{EIA} + f_{EIB} + f_{EIC}$$

- **Formation de l'arbre des conséquences**

L'arbre des causes permet de déterminer la probabilité d'occurrence des phénomènes dangereux (PhD) découlant de l'évènement redouté central. Ce dernier peut se décomposer en évènements redoutés secondaires (ERS) menant à leur tour à d'autres ERS ou PhD. Ces décompositions ont lieu lors du fonctionnement ou dysfonctionnement d'une barrière et lors d'une inflammation ou non-inflammation. La figure suivante permet d'illustrer un arbre de défaillance annoté :

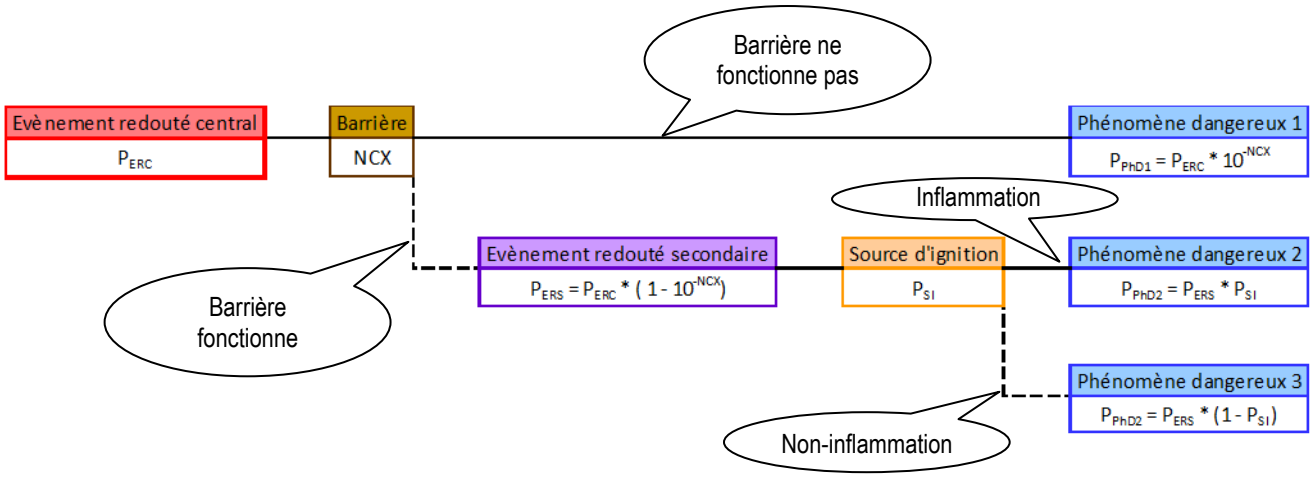

Figure 2 : Illustration annotée d'un arbre des conséquences