INERIS

INSTITUT NATIONAL DE L'ENVIRONNEMENT INDUSTRIEL ET DES RISQUES

Analyse des risques et prévention des accidents majeurs (DRA-07)

Rapport intermédiaire d'opération d
Prise en compte de l'influence des barrières de sécurité dans l'évaluation des risques

Présentation des méthodes d'inspection
TRAM, NIVRIM et AVRIM2

S. BOUCHET

Unité Prévention
Direction des Risques Accidentels

Juin 2001

Analyse des risques et prévention des accidents majeurs (DRA-07)

Rapport intermédiaire d'opération d
Prise en compte de l'influence des barrières de sécurité dans l'évaluation des risques

Présentation des méthodes d'inspection TRAM, NIVRIM et AVRIM2

JUIN 2001

PERSONNES AYANT PARTICIPE A L'ETUDE

Ce document comporte 28 pages (hors couverture et annexes).

TABLE DES MATIERES

1. GLOSSAIRE

TRAM : Technical Risk Audit Methodology

LOD : Line Of Defence

SGS : Système de Gestion de la Sécurité

CEI : Commission Electrotechnique Internationale

Système E/E/PE : système électrique/électronique/électronique programmable

HSE : Health and Safety Executive

NIVRIM : méthode d'inspection pour les établissements ne devant pas réaliser de rapport de sécurité dans le cadre de la réglementation BRZO 1999

AVRIM2 : méthode d'inspection pour les établissements chimiques relevant de Seveso II seuil haut

2. INTRODUCTION

En application de la directive Seveso II, les exploitants d'installations à risques sont contraints de démontrer qu'ils maîtrisent les dangers que génère leur activité.

Aussi, l'INERIS a bâti un programme dénommé Analyse des Risques et Prévention des Accidents Majeurs (DRA-07) qui vise à faire évoluer la démarche d'évaluation des risques pratiquée en France pour tenir compte de cette nouvelle contrainte.

En effet, aujourd'hui, bien souvent seul le potentiel de danger des installations est évalué à travers l'évaluation des distances d'effets de scénarios d'accident majeur. Pour pouvoir faire la démonstration que les dangers de l'activité ont été recensés et qu'ils sont maîtrisés, il apparaît primordial de prendre en compte l'influence des mesures de réduction des risques mises en œuvre par les exploitants, qu'il s'agisse de mesures techniques ou organisationnelles.

Dans le cadre du programme mentionné ci-dessus, l'INERIS travaille sur la caractérisation de l'influence des mesures de réduction des risques pour en tenir compte dans l'évaluation du niveau de risque d'une installation. A ce titre, l'INERIS a recensé et examiné quelques méthodes développées par d'autres Etats Membres de l'Union Européenne pour évaluer et inspecter les mesures de sécurité mises en place sur les installations soumises à la directive SEVESO II. En général, ces méthodes sont utilisées, soit pour évaluer le contenu du rapport de sécurité, qui formalise la démonstration de l'identification et de la maîtrise des risques, soit pour inspecter les sites couverts par la directive.

Le présent document décrit trois méthodes :

- La méthode TRAM développée par le HSE britannique ;
- Les méthodes NIVRIM et AVRIM2 utilisées par les autorités néerlandaises.

Il convient de noter que les méthodes étudiées l'ont été au regard des références mentionnées au chapitre 8. Quelquefois, les articles ne donnent pas suffisamment de détail pour pouvoir mener une analyse plus fine. Cependant, l'INERIS a pu identifier les points forts et des particularités de ces différentes méthodes.

3. TECHNICAL RISK AUDIT METHOD

3.1 GENERALITES

La méthode TRAM a été développée par l'administration anglaise (Health and Safety Executive). C'est un outil d'audit des risques et d'inspection. Il permet l'évaluation des sites visés par les directives Seveso I et II. TRAM est basée sur le modèle d'arbres d'événements (Figure 1).

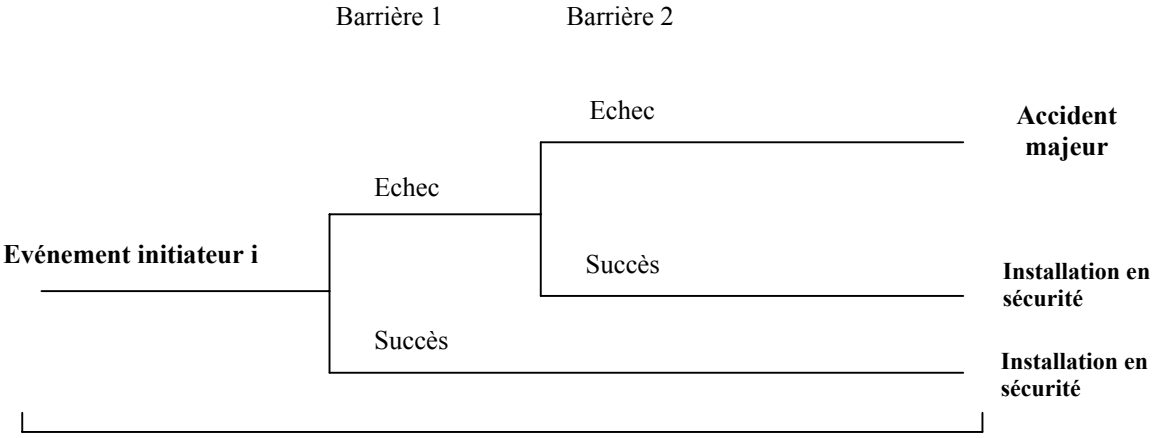

Figure 1 : Modèle d'arbre d'événement

C'est une technique qui permet l'évaluation approximative à la fois des risques et des mesures de réduction associées aux risques pour des processus donnés. Ces mesures de réduction du risque (ou barrières) sont appelées 'lignes de défense' (LOD : Line Of Defence). Ces LOD font l'objet d'un audit.

TRAM est définie comme une méthodologie conforme et cohérente avec les principes de la norme CEI 61508. Cette norme réalisée par la Commission Electrotechnique Internationale (C.E.I.) est relative à la sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables, relatifs à la sécurité.

3.2 METHODOLOGIE

3.2.1 Ligne de défense (Line Of Defence) ou barrière

Dans TRAM une LOD (Line Of Defence) est définie numériquement de la façon suivante:

$$LOD = -\log_{10}(PFD)$$

avec PFD : probabilité de défaillance sur demande. Si le taux de sollicitation de la barrière est continu, alors PFD est remplacée par la probabilité de défaillance par heure (PFU).

Les lignes de défense se répartissent en 4 groupes :

- active : barrière nécessitant une source d'énergie extérieure pour remplir à bien sa fonction et l'initiation de ses composants, comme une chaîne de détection,
- passive : barrière qui n'a pas besoin de source d'énergie extérieure pour fonctionner correctement, par exemple une cuvette de rétention, une soupape de sécurité mécanique,
- physique : barrière provenant d'un processus physique ou naturel, comme les conditions climatiques, la dissipation naturelle de la chaleur,
- procédure : barrière indiquant de façon très précise, les interventions humaines à effectuer pour supprimer ou réduire les conséquences d'un évènement initiateur.

3.2.2 Catégorie de conséquences

TRAM définit la catégorie de conséquences (C_i) des accidents issus de défaillances sur une échelle allant de 1 à 7. En pratique, considérant la sécurité des personnes et les conséquences environnementales, l'échelle utilisée est comprise entre 3 et 7. Mais cette échelle n'est pas fermée et C_i peut prendre des valeurs supérieures à 7.

C_i est déterminée par :

$$C_i = -\log_{10}(\frac{\alpha_N}{m})$$

C_i : catégorie de conséquences de la séquence de défaillances i

α_N : critère d'acceptabilité choisi pour un accident provoquant de N à 10N morts

m : nombre de séquence de défaillances provoquant de N à 10N morts

Par exemple, un accident provoquant de 1 à 10 morts est acceptable si sa fréquence d'occurrence est inférieure à 10^{-6} / an (soit $\alpha_N = 10^{-6}$). Il existe 10 séquences de défaillance amenant des accidents (qui peuvent être différents) provoquant de 1 à 10 morts. Dans ce cas, C=7 pour chacune des séquences de défaillances.

L'utilisation des données de l'usine est nécessaire pour déterminer les catégories de conséquences.

L'échelle est logarithmique, donc un accident classé dans 6 est considéré comme 10 fois plus grave qu'un accident classé dans 5 (voir Tableau 1).

Catégorie de conséquence	Descriptif
> 7	Accident catastrophique : atteintes hors du site, grand nombre de décès, grosse médiatisation, interrogation du public, impact sur le cadre réglementaire et législatif.
> 6	Accident important : dommages en dehors du site, nombreux morts et blessés, premier titre aux informations nationales, interrogation du public, poursuites judiciaires.
> 5	Accident significatif : quelques dommages en dehors du site, petit nombre de morts et / ou nombreux blessés, à la une des informations nationales, réclamation de dommages, d'enquête et d'action juridique.
> 4	Accident à petite échelle : perturbation à l'intérieur du site, morts limités aux travailleurs impliqués dans l'accidents, quelques blessés graves, parution dans les informations locales, demande de dédommagements et enquête.
> 3	Accident mineur : limité à une petite partie du site, quelques blessés légers, perte de temps, pas de mention dans la presse, uniquement une enquête de la compagnie.
=3	Accident limité à de faibles conséquences.

Tableau 1 : Catégories de conséquences dans le modèle TRAM

3.2.3 Classe de fréquence

Dans TRAM, la classe de fréquence (F_i) de la séquence de défaillances i est définie par :

$$F_i = -\log_{10}(f_i)$$

f_i : fréquence de l'évènement initiateur de la séquence de défaillances i.

3.2.4 Evaluation du risque

Le risque R_i, dû à la séquence de défaillances i, relie la conséquence et la fréquence d'occurrence de la façon suivante :

$$R_i = f_i C_i P_i$$

f_i : fréquence de l'évènement initiateur de la séquence de défaillances i

P_i : probabilité pour que cette séquence de défaillances i évolue vers un accident de catégorie de conséquence C_i

Si les barrières sont indépendantes les unes des autres, alors :

$$P_i = \prod_j P_{i,j}$$

$P_{i,j}$: probabilité de défaillance sur demande de la barrière j dans la séquence de défaillances i.

Pour être acceptable, chacune des séquences de défaillances i doit vérifier :

$$F_i + LOD_{exigées} \geq C_i$$

F_i : classe de fréquence de la séquence de défaillances i

avec $LOD_{exigées} = \sum_j LOD_i$ avec $LOD_i = -\log_{10}(P_{i,j})$

C_i : catégorie de conséquence de la séquence de défaillances i

$LOD_{exigées}$ donne l'acceptabilité du risque de laquelle découle l'acceptabilité du système de défense :

$$LOD_{excès} = LOD_{disponibles} - LOD_{exigées}$$

Pour que le système de défense soit acceptable, $LOD_{excès}$ doit être positif pour toutes les séquences de défaillances i. Si $LOD_{excès}$ est positif et inférieur à 1, une analyse plus poussée est nécessaire.

La quantification de $LOD_{disponibles}$ est le résultat d'audits.

3.2.5 Risque résiduel

Par conséquent, en fonction du critère d'acceptabilité α_N choisi au départ, le risque résiduel est donné par :

$$R_{résiduel} = 10^{-(C_i + LOD_{excès})} = 10^{-(F_i + LOD_{diponibles})}$$

3.3 CONCLUSION

Le modèle de risque TRAM comporte donc les éléments suivants :

- les classes de fréquence des évènements initiateurs , qui proviennent de données génériques et / ou d'usines (comme les taux de fuite, …),
- les types de scénarios qui rassemblent un certain nombre d'évènements initiateurs amenant à des conséquences semblables,
- les barrières (LOD), qui représentent les dispositifs de l'usine conçus pour empêcher l'évolution d'un évènement initiateur vers un accident important, ou pour atténuer les conséquences d'un accident important s'il se développe. Les LOD sont quantifiées en utilisant les informations collectées lors des audits,
- les catégories de conséquences, qui fournissent un moyen de classer les accidents importants en fonction de leurs conséquences possibles,
- les arbres d'évènement qui lient les composants ci-dessus et représentent les séquences de défaillances menant à un accident important à partir d'un évènement initiateur.

Le modèle de risques est basé sur un modèle classique d'escalade de risque (Figure 2).

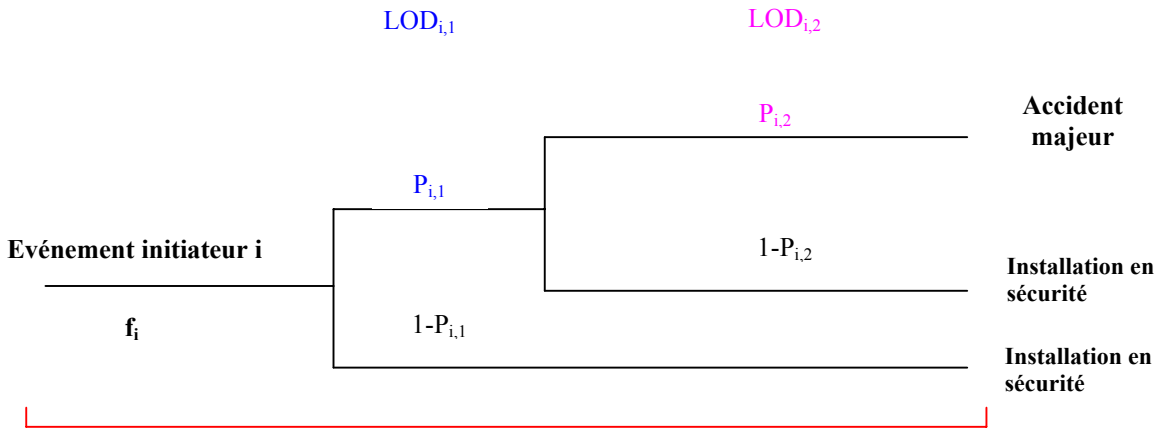

Figure 2 : Modèle de risques TRAM

A partir d'une analyse de risques, des scénarios sont établis et tous les évènements initiateurs de ces scénarios sont transposés dans un arbre d'évènements où figurent toutes les barrières. Ensuite, TRAM permet à la fois l'évaluation du risque et l'évaluation des barrières mises en place pour ce risque (après avoir choisi un critère d'acceptabilité pour chaque scénario redouté). Cette méthodologie prend en compte toutes les lignes de défense : actives, passives, physiques, procédures. C'est un atout très intéressant de la méthode.

Cependant, pour que l'évaluation soit menée à terme, TRAM nécessite une base de données conséquente sur les probabilités de défaillances des barrières qui sont installées sur les process et / ou équipements.

4. NIVRIM

4.1 GENERALITES

NIVRIM a été développée pour le Ministère des Affaires Sociales Néerlandais. C'est un outil d'inspection qui permet d'évaluer si le SGS d'une entreprise répond correctement aux exigences de la directive Seveso II pour les installations classées seuil bas.

L'inspection effectuée par cet outil comprend 6 étapes. La 6ème étape concerne la notification des résultats et ne sera pas développée dans le présent rapport.

NIVRIM est issue de la méthode AVRIM2, dédiée à l'inspection des installations concernées par le seuil haut de la directive Seveso II. En effet, la méthode AVRIM2 intègre l'outil d'inspection NIVRIM dans sa globalité.

4.2 METHODOLOGIE

4.2.1 1ère étape : préparation de l'inspection

Il s'agit d'avoir un aperçu de l'aspect technique des risques d'accidents majeurs, au travers des caractéristiques de l'établissement et du SGS, et de voir quels sont les textes applicables à cette activité. Les documents utilisés par l'équipe d'inspection sont les notifications, les autorisations et tous les documents disponibles de l'établissement (livre de sécurité, procédures, évaluation des risques, plan d'urgence interne…).

Les points particuliers examinés de près sont :

- diversité de produits dangereux de l'établissement,
- type d'activité : stockage, process en batch ou en continu, chargement/déchargement,
- classement par catégories : produits dangereux, process…,
- quantité de produit dangereux sur le site en comparaison au seuil bas et au rapport de sécurité,
- dimension de l'établissement pour identifier les accidents potentiels dus à des effets domino,
- le nombre de personnes exposées en dehors de l'établissement dans le cas d'un accident majeur,
- évaluation des conséquences potentielles,
- retour d'expérience et analyse des circonstances pouvant conduire à l'accident majeur, comme corrosion, érosion, erreurs humaines, facteurs externes,
- estimation des effets potentiels en cas de perte de confinement : feu, explosion, dispersion,
- âge du site,
- âge des installations.

4.2.2 2ème étape : inspection du document décrivant la politique de prévention des accidents majeurs

Le but de cette 2ème étape est de vérifier qu'un document existe, est disponible et d'évaluer s'il couvre l'ensemble des points suivants :

- si la politique a pour but de prévenir les accidents majeurs,
- les tâches, responsabilités et autorité pour effectuer des plans de prévention,
- les critères pour évaluer le risque d'accident majeur,
- les moyens disponibles,
- l'application des procédures au travers de procédures bien établies,
- l'application et évaluation des politiques de prévention,
- la structure de la communication.

La qualité du document décrivant la politique de prévention des accidents majeurs est estimé sur une échelle à 3 niveaux :

- **mauvais** : les objectifs sont écrits dans le document mais ils ne sont pas mesurables et le responsable de l'application des politiques de sécurité n'est pas clairement identifié.

- **acceptable** : Le document mentionne la plupart des sujets de la check-list de NIVRIM. Les objectifs de la politique de prévention sont clairs, les critères d'évaluation du risque majeur sont fournis, les responsabilités sont définies. Cependant, le document ne mentionne pas suffisamment les moyens disponibles, l'application et l'évaluation de la politique, et les façons par lesquelles les lignes directrices sont communiquées au personnel impliqué dans la politique de prévention.

- **bon** : le document contient tous les éléments mentionnés dans la check-list de l'étape 2 de NIVRIM.

4.2.3 3ème étape : entretien avec une personne (responsable) du management de l'établissement

L'engagement de l'équipe de management de l'établissement doit être sans ambiguïté (pour la politique de prévention des accidents majeurs et son application). Afin d'éviter de trop impliquer l'équipe de management dans la vérification de l'engagement, l'équipe d'inspection s'entretient avec le(s) directeur(s) du management seulement. Le but de cette 3ème étape est d'obtenir une image globale de la politique de prévention des accidents majeurs et de la qualité du SGS. Le dialogue doit suffisamment montrer si le management prend en compte les risques majeurs et s'il met en œuvre les moyens adéquats pour les maîtriser.

4.2.4 4ème étape : inspection du SGS

Cette étape est primordiale car elle permet de vérifier le fonctionnement du SGS avec plus de détails. Dans cette étape, l'équipe d'inspection vérifie l'existence du SGS, son degré de couverture, sa connaissance et son application dans les ateliers. L'équipe d'inspection s'entretient avec plusieurs membres d'équipe de même que les managers de la production responsables pour leur part du SGS, et vérifie leur dire en discutant avec les opérateurs.

Dans cette étape, le SGS est divisé suivant les 7 thèmes de l'annexe 3 de la directive Seveso II. Pour chaque thème, une check-list est disponible avec des questions cotées sur une échelle à 4 niveaux :

- absent : pas d'approche systématique (--),

- faible : approche systématique faiblement développée (-),

- raisonnable : approche systématique disponible et plus ou moins complète, son exécution pourrait être améliorée (-/+),

- présent : l'approche systématique est présente, complète et connue par le personnel ouvrier (+).

La check-list peut être présentée sous forme de tableau :

	Présence	Degré de couverture	Appropriation
Est ce que la communication et les supports d'information sur le risque majeur sont organisés ?	+	-	-
Le travail journalier est-il conforme avec l'organisation de la sécurité ?	-/+	-/+	--
Les opérateurs connaissent ils les exigences associées à leur poste de travail pour le contrôle de accidents majeurs	--	--	--

Tableau 2 : Exemple de check-list pour chacun des 7 thèmes de l'annexe 3 de la directive

Les 2 premières colonnes (présence et degré de couverture) sont remplies en discutant avec le directeur et l'équipe de management, tandis que l'évaluation de la dernière (appropriation) est obtenue à partir des discussions avec les opérateurs.

4.2.5 5ème étape : évaluation du résultat de "l'enquête"

Toutes les informations obtenues lors des précédentes étapes sont rassemblées afin d'obtenir une photographie sur la qualité de fonctionnement du SGS.

Une boucle de contrôle a été développée pour les sociétés obligées de produire un rapport de sécurité, connue sous le nom de "boucle AVRIM2". Bien que le nombre de questions contenues dans les check-list de NIVRIM est bien inférieur à celui de AVRIM2, cette boucle peut être utilisée pour vérifier l'adéquation des SGS pour les établissements classés seuil bas.

Elle est constituée de 15 éléments et relations. Elle est décomposée en 3 principaux compartiments, NIVRIM n'utilise que le 2ème compartiment (qui est le compartiment intermédiaire), appelé management de l'installation.

Ce compartiment intermédiaire est composé de 3 niveaux :

- fiabilité humaine,

- communication, contrôle et retour d'information,

- organisation et normes.

4.2.5.1 Boucle de contrôle AVRIM2

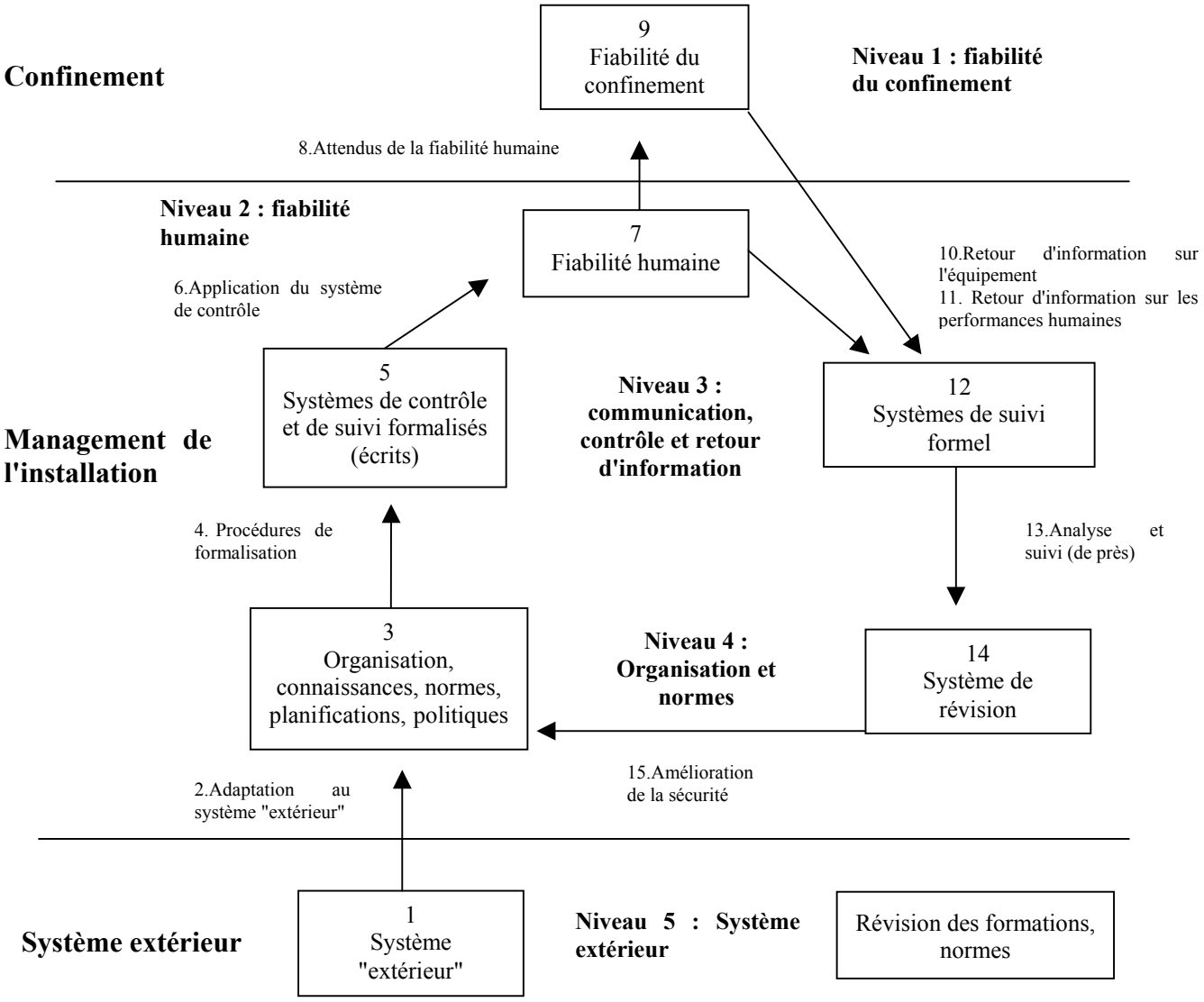

Figure 3 : Boucle de contrôle et de management AVRIM2

Une matrice croise les différentes questions des 7 check-list de l'étape 4 avec les 15 éléments et relations de la boucle de contrôle et de management, soit :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	5	10	26	17	6	1	1	8	4	15	10	8	6

Tableau 3 : Nombres de questions relatives aux éléments de la boucle NIVRIM

Par exemple, il n'y a pas de question pour la relation 1, il y en a 10 pour la relation 4, et 15 pour l'élément 12, etc…

4.2.5.2 Détails des différents éléments de la boucle

Les paragraphes ci-dessous reprennent et explicitent les différents éléments de la boucle, à l'exception de la partie "système extérieur".

3 : organisation, connaissances, normes, planifications, politiques.

La société doit établir une organisation du management qui déterminera et appliquera la politique de sécurité. Cette organisation doit avoir des connaissances sur la sécurité, lui permettant d'établir des normes de sécurité sur lesquelles la sécurité des opérations sera évaluée et ajustée. La société s'engage à appliquer des politiques et des plans, et à désigner du personnel avec des rôles spécifiques pour veiller à l'application et à la coordination de la politique et des plans.

4 : procédures de formalisation.

Les politiques, les standards et les plans sont formalisés par des procédures qui détermineront ce qui doit être écrit et l'organisation de l'information. Les procédures de formalisation doivent reprendre ce qui est important pour le SGS, et permettre l'organisation de l'information pour qu'elle soit accessible et compréhensible par tous.

5 : Systèmes de contrôle et de suivi formalisés (écrits).

Tous les supports de documentation jouent un rôle dans le suivi et le contrôle des personnes et des équipements. Sont inclus les politiques, les plans, les procédures, les schémas, les ordres de mission, les données de sécurité des matériels, les revues de sécurité, le manuel de sécurité…

Le système de documentation devra reprendre la connaissance de la société sur le travail en sécurité, démontrer qu'il a été soumis à la revue de sécurité et accepté par les responsables. Il doit être disponible et compréhensible par tous les utilisateurs.

6 : Application du système de contrôle.

Ce n'est pas suffisant de mettre le SGS sur papier. La politique et les procédures doivent être appliquées au moyen de la structure de management, par tout le personnel, des dirigeants aux opérateurs, en utilisant la communication, la formation et tous les moyens à disposition (personne, équipement, outils, contrôles et affichages).

7 : Fiabilité humaine.

C'est la fonction qui affecte finalement la fiabilité de confinement au travers de la conception, la construction, la maintenance et l'exploitation. La fiabilité humaine dépendra de l'information, des formations, de l'interface homme machine, de la définition des tâches et des charges de travail, de l'environnement de travail. Elle dépendra également de l'efficacité avec laquelle est contrôlée la sécurité au travers de l'application de normes et procédures.

8 : Attendus de la fiabilité humaine.

Les processus de prise de décision qui déterminent les actions, telles que la résolution des conflits entre les besoins et pressions de la production, et la sécurité déterminent les attendus. La discipline la compagnie pour l'exécution des règles, telles qu'effectuer des revues de dangers, suivre les procédures correctement, assurer une maintenance appropriée sans danger, etc., influencera le comportement des personnes sur la sécurité de l'usine. Les non conformités, incidents et presque incidents seront un indicateur de performance.

9 : Fiabilité du confinement.

Le confinement est réalisé par des réservoirs, des conduites de transfert, des petites canalisations qui contiennent les produits dangereux, et tous les systèmes associés dans la conception de l'usine et du process chimique qui agissent en prévention et en protection contre le dépassement de la limite de contenance. Les actions et décisions humaines qui sont prises en différents points du cycle de vie de l'installation affecteront l'intégrité des systèmes de confinement.

10, 11 : Retour d'information.

L'application de la sécurité est suivie par des mesures, l'observation, des audits, des réunions revue de sécurité, et par la remontée des informations des opérateurs vers leur hiérarchie. Finalement, les informations du suivi de la sécurité retournent au plus haut niveau du management par l'intermédiaire de rapports réguliers de performance de la sécurité.

12 : Systèmes de suivi formel.

La prise des informations pour le suivi de la sécurité est hautement dépendante des exigences formelles du suivi de la sécurité, et l'existence de personnel avec des rôles spécifiques pour le suivi de la sécurité, telle qu'une équipe interne d'audit, entraînée à la réalisation d'audit et l'utilisation de système d'audit formalisé. Le système de suivi formel se rapporte aux normes qui ont été élaborées et appliquées sur la partie "contrôle" de la boucle. Il inclut la récupération des données sur les incidents et presque incidents.

13 : Analyse et suivi.

Les données récupérées à propos de la performance du SGS nécessiteront une analyse, afin de fournir des informations significatives, pour pouvoir en tirer les enseignements. Il est important de ne pas se limiter à l'analyse des statistiques des événements suivis, mais aussi d'analyser les raisons sous jacentes, par exemples : pourquoi une norme correspondante à l'application de la sécurité n'a pas été respectée, quel contrôle était défaillant ou n'était pas en place ?

14 : Système de révision.

Le procédé d'analyse permet d'identifier les défaillances de contrôle ou les pertes de contrôle. Il est alors nécessaire de réviser ou de renforcer le procédé de contrôle par lequel la sécurité est appliquée. De cette façon, le système entier est auto ajusté.

15 : Amélioration de la sécurité.

Le suivi pour identifier les besoins de réviser le SGS est appliqué pour la sécurité, au moins pour obtenir le niveau fixé dans les normes, ou pour l'améliorer quand les normes sont toujours satisfaites. Quand la boucle est entière, l'amélioration continue de la sécurité est accomplie, ce qui est mis en évidence par la formalisation de plans d'amélioration de la sécurité.

4.3 CONCLUSION

NIVRIM est un outil d'inspection très élaboré qui permet l'évaluation du SGS des installations couvertes par le seuil bas de Seveso II aux Pays Bas.

AVRIM2 englobe la méthode NIVRIM, dont elle est issue. La connaissance préalable de NIVRIM permet une meilleure compréhension d'AVRIM2.

5. AVRIM2

5.1 GENERALITES

AVRIM2, de même que NIVRIM a été développée pour le Ministère des Affaires Sociales Néerlandais.

AVRIM2 est une méthode holistique, basée sur le concept de scénarios et de lignes de défense (concept similaire à TRAM). Cette méthode permet d'évaluer "la solidité" du Système de Gestion de la Sécurité d'une entreprise, en ce qui concerne la maîtrise des risques de perte de confinement de substances dangereuses, dans le cadre des sites soumis à la directive Seveso II et classés seuil haut. L'évaluation est effectuée à travers l'examen du rapport de sécurité (équivalent de l'étude des dangers) et une inspection du site.

Cette méthode et son logiciel d'application SAVRIM (la version anglaise n'est pas disponible à la date de rédaction de ce rapport) permettent d'assister l'évaluation du rapport de sécurité et d'effectuer l'inspection des risques majeurs d'un site industriel, avec au départ, une limitation aux effets susceptibles de se produire sur le site (on-site).

AVRIM2 repose sur le concept suivant : le SGS doit être adapté au système technique et aux risques associés. Ce concept dérive de l'expérience et de l'observation des législateurs et Inspecteurs du travail du Ministère des Affaires Sociales Néerlandais. Ce concept exige que :

- les Inspecteurs doivent en premier évaluer le système technique avant d'examiner le SGS,
- l'Industriel doit montrer par quels moyens le SGS gère la prévention des accidents majeurs du système technique.

5.2 METHODOLOGIE

5.2.1 Matrice des risques

La matrice des risques permet l'évaluation de l'occurrence des scénarios. L'application de la directive SEVESO II aux Pays Bas exige une évaluation quantifiée des risques pour les scénarios avec des conséquences hors du site.

Les données de défaillance pour cette évaluation quantitative proviennent de données historiques génériques et d'expertises. Ces données ont pour but de se concentrer sur la fiabilité des systèmes de LOD (Line Of Defence) et les possibles conséquences en cas de défaillances, permettant ainsi à l'Inspecteur de mener à bien une vérification de la qualité des LOD.

Dans cette perspective, une approche semi quantitative est recommandée ; le calcul des probabilités de défaillances et les conséquences qui en découleraient peuvent être classés dans des catégories, dont les critères sont proposés par l'exploitant.

La matrice des risques résulte de la composition de ces catégories. Plus les conséquences des scénarios d'accident sont graves, plus la fiabilité des LOD devra être importante.

Probabilité de perte de confinement	Conséquence				
	5 Très grave	4 Majeure	3 Sérieuse	2 Mineur	1 Négligeable
5 Très importante	X	X	X	X	O
4 Importante	X	X	X	O	O
3 Moyenne	X	X	O	O	=
2 Faible	X	O	O	=	=
1 Très faible	O	O	=	=	=

Tableau 4 : Matrice des risques AVRIM2

X : risque élevé inacceptable. La Société doit le réduire par des mesures de prévention et / ou des moyens de protection.

O : risque élevé. La Société doit adresser aux inspecteurs des analyses coûts bénéfices des réductions de risque supplémentaires à mettre en place. Les inspecteurs doivent vérifier ces analyses coûts bénéfices et les contrôles déjà en place.

= : acceptable. Aucune action n'est requise.

Echelle de probabilité	Echelle des conséquences
1 très faible jamais vu dans ce secteur industriel presque impossible dans l'établissement $<10^{-4}$ par an	1 négligeable impact mineur sur le personnel, pas d'arrêt de production coût < 4540 €
2 faible déjà rencontrer dans ce secteur industriel possible dans l'établissement $<10^{-3}$ par an	2 mineur soins médicaux pour le personnel, dommage mineur, petite perte de production coût < 45400 €
3 moyenne déjà rencontrer dans la société occasionnelle mais peut arriver quelque fois dans l'établissement $<10^{-2}$ par an	3 sérieuse personnel sérieusement blessé (arrêt de travail), dommages limités, arrêt partiel de la production coût < 227000 €
4 importante arrive quelque fois par an dans toute la société possibilité d'incidents isolés dans l'établissement $<10^{-1}$ par an	4 majeure blessure handicapante à vie, dommages importants, arrêt de la production coût < 454000 €
5 très importante arrive plusieurs fois par an dans toute la société incidents répétés dans l'établissement $>10^{-1}$ par an	5 très grave un ou plusieurs morts, dommages très étendus, long arrêt de la production coût > 4540000 €

Tableau 5 : Classe de fréquences AVRIM2

5.2.2 Scénarios et lignes de défense ou barrières (LOD)

La description des étapes par lesquelles les accidents peuvent se réaliser est basée sur l'identification de scénarios, avec unicité ou combinaison de défaillances du système technique, donc des équipements et procédures relatifs à la maîtrise du confinement des substances dangereuses. Ces scénarios sont retranscrits à l'aide d'arbres de défaillances et d'arbres d'événements, joints, constituant une figure en forme de "nœud papillon".

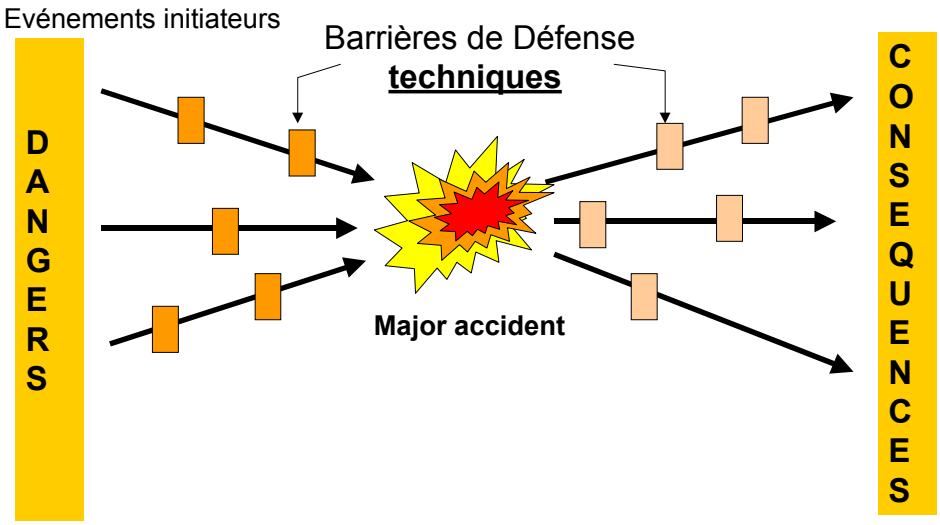

Figure 4 : modèle du « nœud papillon »

AVRIM2 est composé de 11 arbres génériques auxquelles sont associés 139 événements de base, représentant un total de 125 scénarios de perte de confinement.

Sur les arbres génériques sont placées les lignes de défense qui agissent soit en prévention, soit en protection. 4 types de LOD sont définies dans AVRIM2 :

- LOD physiques : elles sont intrinsèques au matériel, comme l'épaisseur du métal d'un réservoir…

- LOD "contrôle et instrumentation" : elles préviennent une défaillance de mesure et/ou de contrôle du process. Par exemple, une boucle de contrôle, un filtre, une pompe, etc, font partie de cette catégorie,

- LOD passives : protection contre les chocs, soupapes…

- LOD pour prévenir l'erreur humaine : procédures, informations, formations….

Ces LOD permettent le lien entre le SGS et le système technique : en effet, le SMS est lié aux LOD, qui préviennent ou protègent contre l'occurrence des scénarios, et ces LOD font partie du système technique.

5.2.3 Liens entre SGS et système technique

A chaque événement de base (obtenu à partir des arbres génériques) correspond un ensemble de lien qualifié de "check-list LOD".

Une "check-list LOD" comprend :

- un événement de base,
- un ou plusieurs types de LOD associés au scénario issu de l'événement de base,
- des cycles de vie par LOD,
- des thèmes de management par cycle.

Les cycles de vie sont :

- la conception et les modifications,
- la construction,
- l'exploitation,
- la maintenance, l'inspection et les tests.

5.2.4 Les thèmes de management

Les thèmes de management réalisent l'interconnexion du système technique au système de management. Pour chaque cycle de vie existe un modèle de management, une boucle de suivi et de contrôle. Cette boucle possède un nombre de composants de contrôle et de suivi liés, comme par exemple un système de contrôle d'auto amélioration et d'auto régulation.

Pour chacun des 15 composants de la boucle du système, il existe des thèmes communs. Les points importants pour l'audit du système sont groupés sous 9 thèmes, qui rappellent chacun des 15 composants de la boucle (voir NIVRIM). La sélection d'un nombre limité de thèmes (9) rend possible un audit restreint de la boucle de contrôle et de suivi.

Ces 9 thèmes de management qui interviennent dans tous les cycles de vie sont :

- connaissance des dangers / risques,
- utilisation de normes,
- maîtrise des conflits sécurité - production,
- études de sécurité obligatoires,
- procédures de sécurité,
- aptitude, compétence et entraînement,
- les facteurs humains dans le management,
- supervision et vérification,
- retour d'expérience.

Le concept permet de passer du système technique au SGS mais également du SGS au système technique selon le modèle présenté dans la figure ci-dessous. La Figure 5 montre l'imbrication des différentes "couches" successives depuis les dangers et leur identification jusqu'au cycle de vie, en passant par les LOD et le SGS.

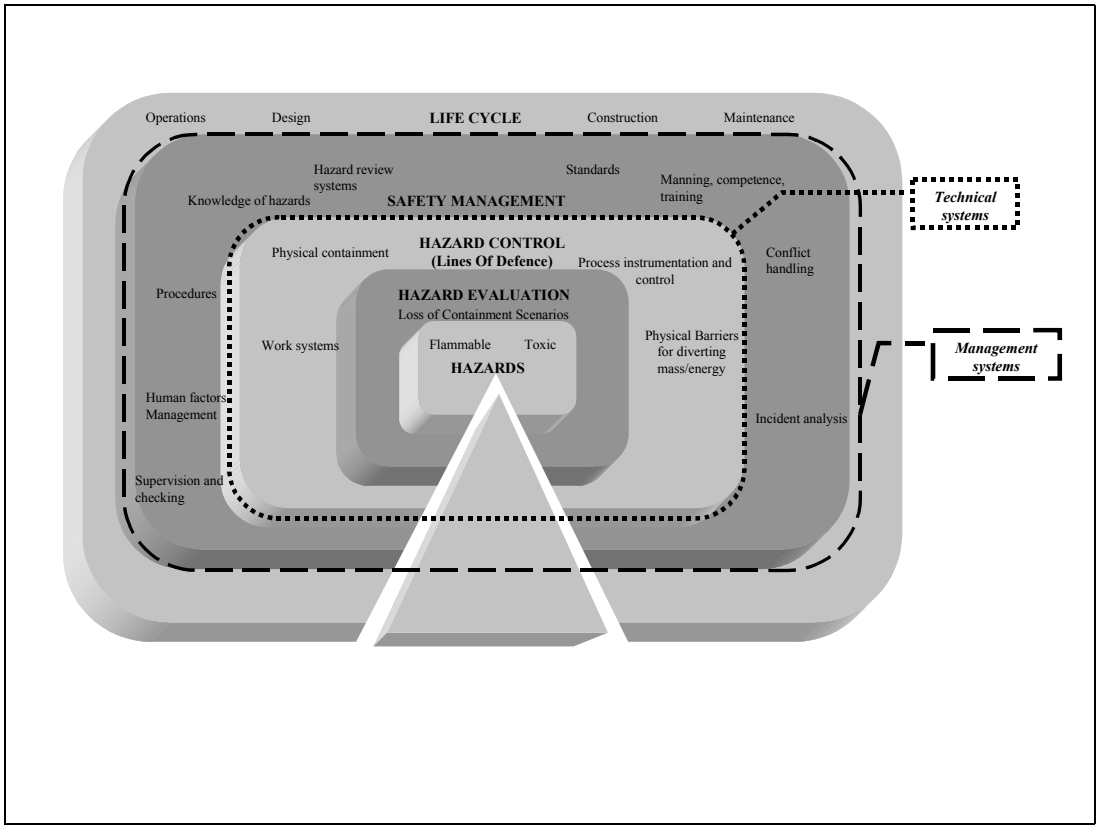

Figure 5 : Présentation des dangers en relation avec les systèmes technique et de management

5.3 CONCLUSION

Pour l'instant, cette méthode est uniquement appliquée aux usines chimiques.

Cette méthode est avant tout basée sur des scénarios qui amènent à une perte de confinement, retranscrits par des arbres de défaillances et d'événements, d'où l'importance de l'analyse des risques.

AVRIM2 reprend des concepts développés dans TRAM (notamment les LOD et le passage du quantitatif au semi quantitatif…). La quantification des défaillances reste difficile et s'obtient par un retour d'expérience ou le recours aux experts. La difficulté est amoindrie en raisonnant sur du semi quantitatif, donc sur des classes de probabilité et catégories de conséquence.

C'est une procédure uniforme qui permet l'évaluation des sites classés seuil haut dans la directive Seveso II. La méthode met en évidence des liens entre le système technique et le SGS, et elle en tient compte pour l'évaluation du SGS.

L'évaluation du SGS est principalement basée, aux Pays bas, sur la partie gauche de la figure en papillon, soit l'arbre des défaillances, de par l'approche probabiliste prônée. De plus, ces évaluations sont menées par des Inspecteurs du travail Néerlandais qui se focalisent plus sur les aspects de prévention que sur les aspects de protection.

En France, de par notre approche déterministe, l'évaluation du SGS recherchée se porte plus sur la partie droite de la figure en papillon (arbre des événements), sur les barrières qualifiées de protection voire d'intervention.

En résumé, AVRIM2 sert à la fois pour l'évaluation des scénarios et LOD retenus dans le rapport de sécurité, et pour l'évaluation du SGS par l'intermédiaire de NIVRIM, module issu de la méthode AVRIM2.

6. ANALYSE DES METHODES

Ce chapitre présente une synthèse des points forts et des particularités des méthodes étudiées dans les chapitres précédents.

Il convient de souligner que ces approches sont toutes basées sur le concept de « barrières de sécurité » (Line Of Defence) avec raisonnement en semi quantitatif pour l'évaluation de leurs qualités. L'INERIS a pu tester cette approche et la trouve appropriée pour l'analyse des risques et l'identification des mesures de réduction de risques.

A partir de l'étude de ces méthodes, l'INERIS a identifié les étapes particulièrement importantes pour proposer une démarche d'évaluation de la qualité des mesures de réduction des risques, qu'elles soient d'ordre technique ou organisationnel.

Par ailleurs, il convient d'insister en préambule à ce chapitre que toutes les méthodes étudiées n'ont de sens et d'intérêt que si une analyse des risques pertinente est menée, en particulier, dans le sens de l'identification des dangers. A ce titre, il convient d'insister sur l'importance de mener l'analyse des risques en groupe de travail avec une méthode structurée de type HAZOP, AMDEC, APR ou Arbre des Défaillances. La combinaison des méthodes inductives et déductives est l'idéal, mais la lourdeur de ces deux étapes est généralement rédhibitoire. Il convient donc de retenir que l'analyse des risques constitue le fondement et le préalable à ces approches d'évaluation des barrières de sécurité techniques et organisationnelles

6.1 TRAM

Domaine d'application

- Méthode d'évaluation du rapport de sécurité et audit de sécurité par l'inspection.

Points forts

- Evaluation à la fois des risques et des barrières associées,
- Evaluation possible de toutes les barrières (active, passive, procédure, physique),
- Compatibilité avec les normes CEI 61508 et CEI 61511,
- Approche semi-quantitative avec critères d'acceptabilité du nombre de barrières à installer face à une séquence accidentelle,
- Introduction de la notion d'équivalence des barrières de sécurité,
- Proposition d'une approche d'audit pour vérifier que la réalité est conforme à l'approche théorique menée à partir du rapport de sécurité.

Données d'entrée, besoins, contraintes

- Nécessité d'une base de données sur les probabilités de défaillances des barrières, mais aussi sur les fréquences d'occurrence des événements initiateurs. Ce genre d'information est difficile à obtenir pour un process particulier. Forcément, faute de retour d'expérience suffisant sur l'installation étudiée, des incertitudes seront introduites en utilisant les informations de bases de données génériques.
- Besoin de définir des critères d'acceptabilité pour le nombre et la qualité des barrières. Dans cette méthode, les critères d'acceptabilité sont fixés sur la base du nombre de victimes susceptibles d'être impliquées en cas d'accident.

6.2 NIVRIM

Domaine d'application

- Méthode d'inspection plus orientée sur les mesures organisationnelles, utilisée pour l'inspection des établissements seuil bas selon Seveso II.

Points forts

- Cohérence avec une approche sociologique de l'évaluation des organisations,
- Prise en compte à la fois la formalisation d'un système de gestion de la sécurité et le fonctionnement de ce système,
- Vérification de l'impact du SGS à tous les niveaux hiérarchiques (du directeur à l'opérateur),
- Présence d'une grille d'audit permettant l'inspection du SGS.

Données d'entrée, besoins, contraintes

- Nécessité de mener des entretiens, d'avoir des rencontres avec le personnel des installations inspectées : la durée de l'inspection s'étend sur plusieurs jours,
- Nécessité d'une sensibilisation aux concepts de gestion, aux facteurs humains et aux organisations.

6.3 AVRIM2

Domaine d'application

- Méthode d'inspection et d'analyse du rapport de sécurité, utilisée pour l'inspection des établissements seuil haut selon Seveso II.

Points forts

- Lien entre les mesures techniques de maîtrise des risques et les mesures organisationnelles,
- Démarche systématique et générique : rassurant pour l'inspection, mais quelquefois pas suffisamment détaillé sur des points précis du process,
- Idem NIVRIM quant à l'évaluation du SGS.

Données d'entrée, besoins, contraintes

- Nécessité de mener des entretiens, d'avoir des rencontres avec le personnel des installations inspectées : la durée de l'inspection s'étend sur plusieurs jours,
- Nécessité d'une sensibilisation aux concepts de gestion, aux facteurs humains et aux organisations.

De manière générale et valable pour les trois méthodes étudiées, l'approche est lourde et nécessite un investissement important pour la personne qui mène l'analyse. Cependant des logiciels permettent, aussi bien pour TRAM que pour AVRIM2, de faciliter le traitement des données.

7. INTERET DES METHODES ETUDIEES POUR L'ANALYSE DE LA QUALITE DES BARRIERES TECHNIQUES

TRAM et AVRIM2 (et NIVRIM) sont des méthodes utilisées respectivement en Angleterre et aux Pays Bas pour mener à bien l'inspection des établissements soumis à la directive Seveso II.
Bien que TRAM soit plus axée sur les dispositifs techniques, elle permet aussi la prise en compte des barrières de type organisationnel.
AVRIM2 et NIVRIM, quant à elles, sont plus orientées sur l'inspection du SGS.

Le champ d'application de ces méthodes se cantonne pour l'instant aux établissements chimiques.

L'analyse de ces méthodes a été utile à deux niveaux :

- Premièrement, pour structurer une approche pour vérifier l'efficacité des barrières de sécurité.
- Deuxièmement, pour trouver une cohérence entre la maîtrise technique et organisationnelle des risques.

7.1 STRUCTURATION D'UNE APPROCHE POUR L'ANALYSE DES BARRIERES TECHNIQUES

En ce qui concerne la structuration d'une approche pour vérifier l'efficacité des barrières de sécurité mises en place par les exploitants, les concepts de la méthode TRAM nous semblent très intéressants et utiles pour proposer une approche adaptée au contexte français.

En particulier, l'approche semi-quantitative proposée dans TRAM qui vise à proportionner la qualité des barrières au niveau de conséquences des séquences potentielles d'accident est appropriée et pourra être adaptée. Le raisonnement est plus facile à mener sur la qualité des barrières que sur la quantification de la probabilité d'occurrence des événements accidentels. Toutefois, pour mener l'analyse, il est nécessaire de connaître les probabilités de défaillances des barrières de sécurité et des chaînes de sécurité. Ce type de données est toujours difficile à obtenir. Aussi, l'INERIS continuera de travailler sur ce thème, notamment en se rapprochant d'industriels, utilisateurs d'équipements de sécurité. Dans cette optique, des contacts ont été pris avec l'EXERA.

Autre point fort de la méthode TRAM, l'approche est cohérente avec l'application des normes CEI 61508 et CEI 61511. L'application de ces normes, dédiées à la sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables (cf. annexe A) permet de déterminer, entre autre, le niveau d'intégrité et de sécurité des barrières, qui est en relation directe avec leurs probabilités de défaillances.

Au total, la combinaison de l'approche semi-quantitative de TRAM et la méthode d'évaluation des normes CEI permettrait de construire un système d'analyse cohérent et opérationnel qui pourrait être utile pour mener l'analyse des barrières dans le cadre de l'étude des dangers. Il reste à le vérifier sur le terrain industriel que l'analyse complète peut être menée. Des tests de l'approche devraient être lancés prochainement.

7.2 COHERENCE ENTRE MAITRISE TECHNIQUE ET ORGANISATIONNELLE DES RISQUES

Les méthodes NIVRIM et AVRIM2 se focalisent plus sur l'analyse du système de management. L'approche qui est développée dans ces 2 méthodes est basée sur le fait que le système organisationnel (SGS) est lié au système technique par l'intermédiaire des barrières (LOD), ce qui donne une cohérence entre la maîtrise technique et organisationnelle des risques.

L'INERIS a décidé de développer ce concept pour formaliser une méthode d'analyse des risques qui combine les aspects techniques et organisationnels. Cette méthode a été baptisée ATOS (Analyse Technique et Organisationnelle de la Sécurité). Elle s'articule de la manière suivante :

- Dans un premier temps, une analyse des risques techniques des activités de l'entreprise est réalisée. Cette analyse repose sur la mise en œuvre de méthodes classiques d'analyses telles que l'Analyse Préliminaire des Risques, Analyse des Modes de Défaillances et leurs Effets, Hazop, … Cette analyse est effectuée en vue d'identifier les activités ayant un impact sur la sécurité et donc potentiellement sur l'environnement et de mettre en lumière les barrières techniques de sécurité présentes sur le site.
- Dans un second temps, un audit des pratiques organisationnelles est réalisé pour toutes les activités identifiées à l'étape précédente. Cet audit porte sur :
    - Les aspects formels de l'organisation : évaluation des procédures mises en place par l'industriel en vue de gérer la sécurité relative au risque majeur (analyse et évaluation des risques, gestion des modifications, gestion du retour d'expérience…),
    - Les aspects informels de l'organisation (communication, prise de décision, coopération, compétences…).

  Cet audit met en œuvre des techniques spécifiques pour l'analyse des facteurs organisationnels.

Cette approche complète sera testée prochainement sur le terrain. A ce titre, l'INERIS recherche des partenaires industriels, en particulier des PMI de la chimie.

8. REFERENCES

Linda J. BELLAMY, Williët G. J. BROUWER.
AVRIM2, a Dutch major hazard assessment and inspection tool.
Journal of hazardous materials, n°65 (1999), p 191-210.

A. R. HALE, F. GULDENMUND, K. SMITH, L. BELLAMY.
Modification of technical risk assessment with management weighting factors
ESREL 1998

A. R. HALE, M. A. F. COSTA, L. H. J. GOOSSENS, K. SMIT.
Relative importance of maintenance management influences on equipment failure and availability in relation to major hazards.
ESREL 1999.

Linda J. BELLAMY, Ir. JAAP van der SCHAAF.
Major hazard management : technical-management links and the AVRIM2 method
Seveso 2000, Athène (1999).

Joy I. H. OH, Linda J. BELLAMY.
AVRIM2 : a holistic assessment tool for use within the context of EU Seveso II directive.
Seveso 2000, Bordeaux.

A. ZANDVOORT.
Implementation of the seveso-2 guideline at a large chemical site in the Netherlands.
The conference forum Aldgate East, London, 6-8 november 2000.

Joy I. H. OH, Linda J. BELLAMY.
Use of the inspection tool AVRIM2 to inspect the demonstrating aspects.
The conference forum Aldgate East, London, 6-8 november 2000.

Dr Tom. MADISON, Dr P. KIRK, Richard STANSFIELD.
Technical Risk Audit Method (TRAM). Development and application to the auditing of major hazard sites.

Patrick J. NAYLOR, Dr Tom MADISON, Richard STANSFIELD.
TRAM : Technical Risk Audit Methodology for comah sites.

CEI 61508.
Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité.
1998.

CEI 61511.
Functional safety : safety instrumented systems for the process industry sector.
1999.

Eric FAE, Jean-Luc DURKA.
Conception et évaluation de la sécurité fonctionnelle des systèmes instrumentés de process industriels. Rapport INERIS. 2001

9. LISTE DES ANNEXES

Repère	Désignation précise	Nombre de pages
A	Cycle de vie et niveau d'intégrité de sécurité dans les normes CEI 61511 et CEI 61508	6

ANNEXE A

CYCLE DE VIE ET NIVEAU D'INTEGRITE DE SECURITE DANS LES NORMES CEI 61511 ET CEI 61508

CYCLE DE VIE ET NIVEAU D'INTEGRITE DE SECURITE DANS LES NORMES CEI 61511 ET CEI 61508

Les normes CEI 61508 et 61511 ont été réalisées par des groupes de travail internationaux, sous la direction de la Commission Electrotechnique Internationale.

La norme CEI 61508 traite de la sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité. La CEI 61511 est une déclinaison de la 61508 appliquée aux processus industriels.

L'approche de ces normes est basée sur deux concepts qui sont le cycle de vie et le niveau d'intégrité de sécurité.

Le cycle de vie

Afin de traiter de façon systématique toutes les activités nécessaires pour assurer le niveau d'intégrité de sécurité prescrit pour les systèmes E/E/PE relatifs à la sécurité, les normes 61508 et 61511 ont choisi un cycle de vie de sécurité global comme cadre technique, qui englobe les trois mesures suivantes de réduction des risques :

- systèmes de sécurité E/E/PE,
- systèmes de sécurité basés sur d'autres technologies,
- dispositifs externes de réduction de risque.

Le cycle de vie de sécurité globale est représenté Figure 6. Les activités relatives à la vérification, à la gestion et à l'évaluation de la sécurité fonctionnelle ne sont pas représentées mais concernent toutes les phases globales du cycle de vie de sécurité des systèmes E/E/PE.

La portion du cycle de vie de sécurité global qui concerne les systèmes de sécurité E/E/PE est appelée "cycle de vie de sécurité du système E/E/PE" (cf. Figure 7). Chaque système de sécurité E/E/PE possède un cycle de vie.

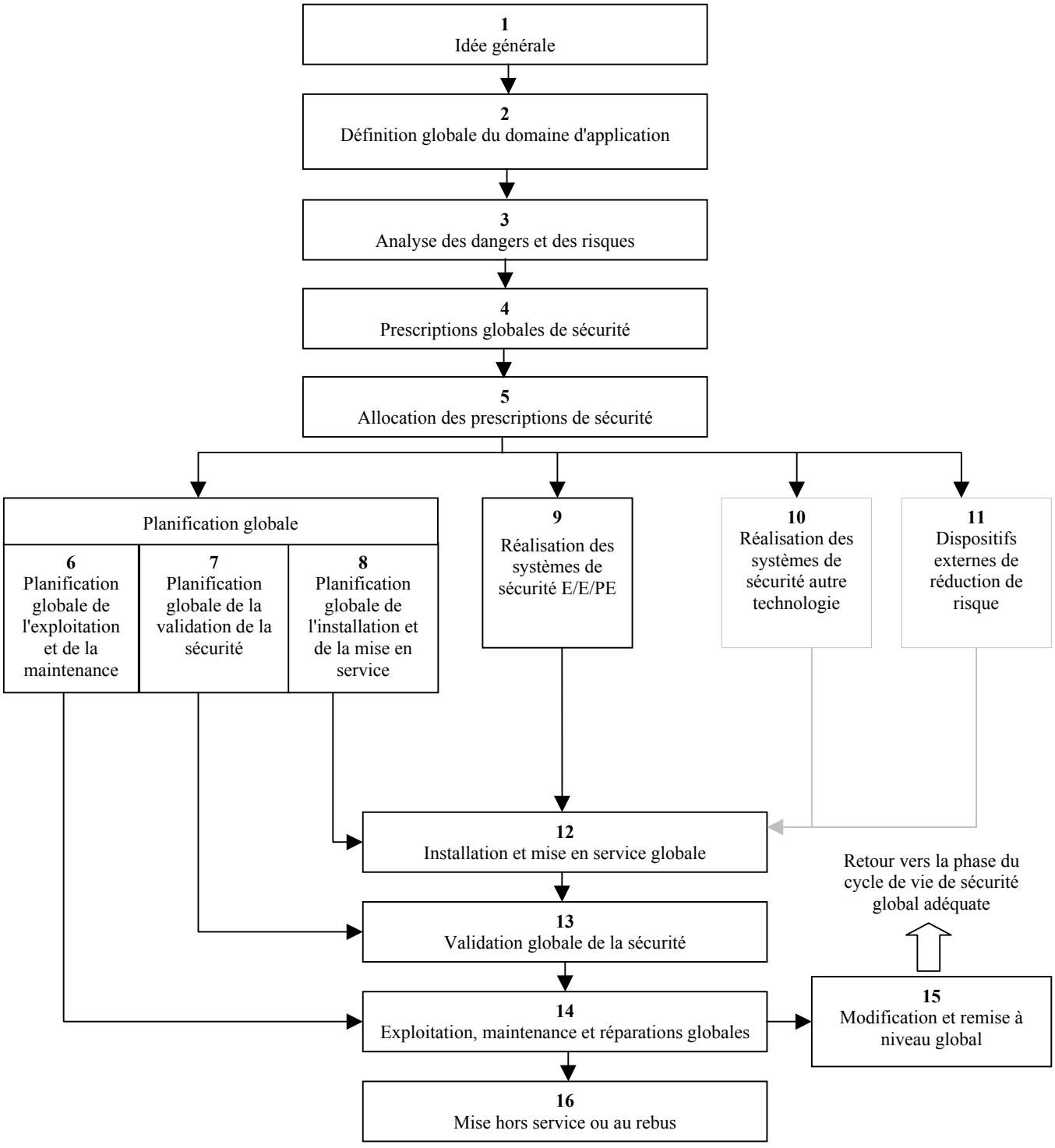

Figure 6 : Cycle de vie de sécurité globale (issue de la figure IEC 1647/98)

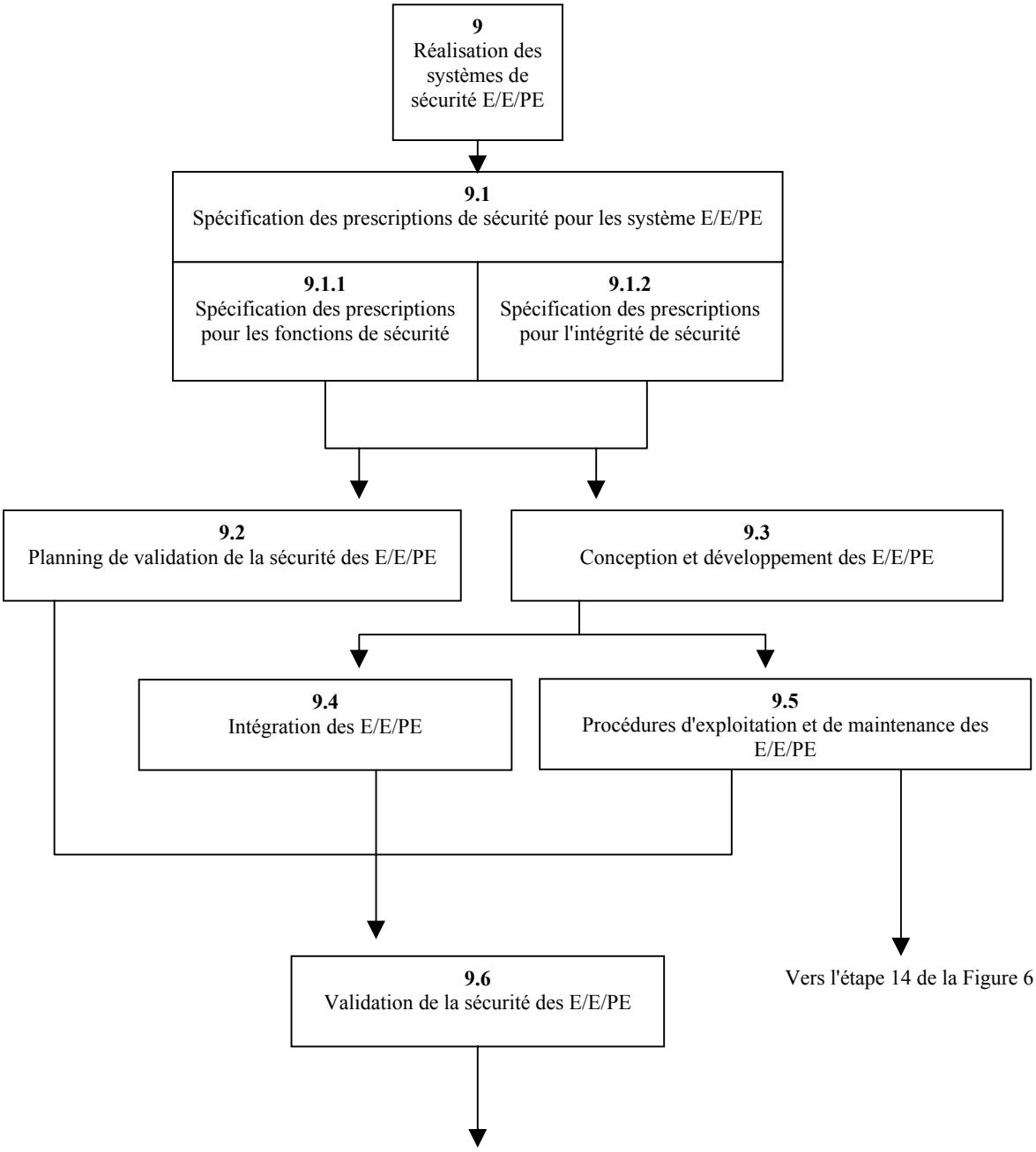

Figure 7 : Cycle de vie de sécurité du système E/E/PE (issue de IEC 1 647/98)

Le niveau d'intégrité de sécurité ou Safety Integrity Level (S.I.L.)

La détermination du besoin d'un système E/E/PE pour un équipement donné, en plus d'autres dispositifs externes de sécurité, est effectué au préalable par une analyse de risques. Cette analyse des risques est suivie de l'utilisation d'un modèle de réduction du risque pour estimer le S.I.L. associé au système E/E/PE. Cette démarche est illustrée Figure 8.

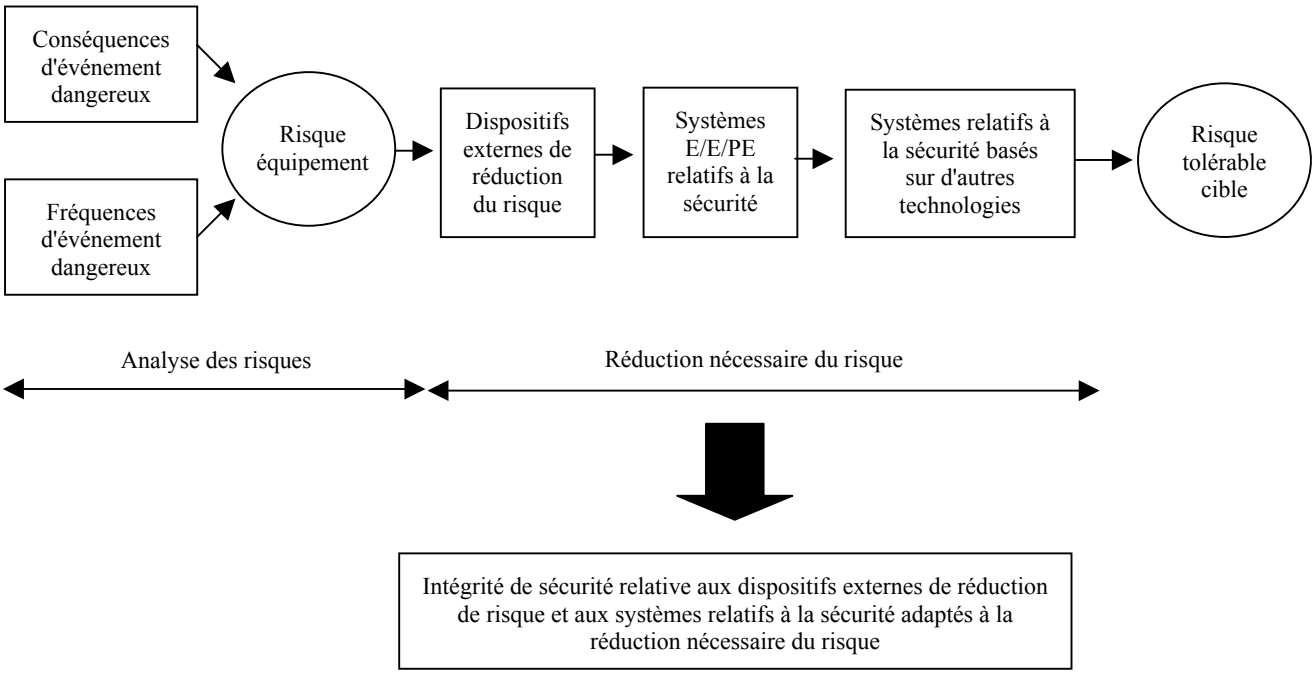

Figure 8 : Concepts de risque et d'intégrité de sécurité

La norme 61508 spécifie 4 niveaux d'intégrité de sécurité, le niveau 4 étant le plus élevé et le niveau 1 le plus faible. Les objectifs en matière de sécurité pour les 4 niveaux d'intégrité de sécurité sont spécifiés dans le Tableau 6 et le Tableau 7. Deux paramètres sont spécifiés, un pour les systèmes relatifs à la sécurité fonctionnant en mode demande basse et un pour les systèmes relatifs à la sécurité fonctionnant en mode demande continue ou élevée.

Niveau d'intégrité de sécurité	Mode de fonctionnement à faible sollicitation (Probabilité moyenne de défaillance à exécuter, lors d'une sollicitation, la fonction pour laquelle il a été conçu)
4	$\Sigma\ 10^{-5}$ à $< 10^{-4}$
3	$\Sigma\ 10^{-4}$ à $< 10^{-3}$
2	$\Sigma\ 10^{-3}$ à $< 10^{-2}$
1	$\Sigma\ 10^{-2}$ à $< 10^{-1}$

Tableau 6 : Correspondance entre niveaux d'intégrité de sécurité et probabilité de défaillance pour un système de sécurité E/E/PE fonctionnant en mode faible sollicitation

Niveau d'intégrité de sécurité	Mode de fonctionnement continu ou à forte sollicitation (Probabilité d'une défaillance dangereuse par heure)
4	entre 10^{-9} et 10^{-8}
3	entre 10^{-8} et 10^{-7}
2	entre 10^{-7} et 10^{-6}
1	entre 10^{-6} et 10^{-5}

Tableau 7 : Correspondance entre niveaux d'intégrité de sécurité et probabilité de défaillance pour un système de sécurité E/E/PE fonctionnant en mode continu ou de forte sollicitation

L'application des normes CEI 61508 et 61511 permet donc d'apprécier si un système de sécurité E/E/PE est nécessaire et de déterminer son niveau d'intégrité de sécurité associé pour réduire le risque (analyse de risques et réduction du risque).

L'application d'un cycle de vie défini par les normes permet la vérification du niveau d'intégrité de sécurité prescrit a chaque stade de sa vie, de la conception à la mise hors service en passant par les modifications.