

RAPPORT D'ÉTUDE

21/09/2009

N° DRA-09-103041-06026B

**Démarche d'évaluation des Barrières Humaines
de Sécurité - Ω 20**

**Programme 181 - DRA 77 : Maîtrise des risques
accidentels par les dispositions technologiques
et organisationnelles**

INERIS

Programme 181 - DRA-77 : Maîtrise des risques accidentels par les dispositions technologiques et organisationnelles

Démarche d'évaluation des Barrières Humaines de Sécurité - Ω 20

Direction des Risques Accidentels

Client : **MINISTERE DE L'ÉCOLOGIE, DE L'ÉNERGIE, DU DEVELOPPEMENT DURABLE ET DE LA MER (MEEDDM)**

Liste des personnes ayant participé à l'étude : E. MICHE, R. PERINET

PREAMBULE

Le présent document a été établi :

- au vu des données scientifiques et techniques disponibles ayant fait l'objet d'une publication reconnue ou d'un consensus entre experts,
- au vu du cadre légal, réglementaire ou normatif applicable.

Il s'agit de données et informations en vigueur à la date de l'édition du document, mars 2009.

Le présent document comprend des propositions ou recommandations. Il n'a en aucun cas pour objectif de se substituer au pouvoir de décision du ou des gestionnaire(s) du risque ou d'une partie prenante.

PAGE DE VALIDATION			
Démarche d'évaluation des barrières humaines de sécurité			
Rédaction initiale			
Auteurs	Qualité	Date	Emargement
Elodie MICHE	Ingénieur à l'Unité Evaluation Quantitative des Risques		Signé
Romuald PERINET	Ingénieur à l'Unité Facteurs Humains et Gouvernance		Signé
Dans le cadre de la procédure générale qualité de l'INERIS et en respect du paragraphe 14.2 du manuel qualité, ce document a fait l'objet de relectures et d'un contrôle par des vérificateurs.			
Relecture	Qualité	Date	Emargement
Christophe BOLVIN	Responsable unité EQRI		Signé
Vérificateur final	Qualité	Date	Emargement
Marie-Astrid KORDEK	Délégué Appui à l'Administration		Signé
Sylvain CHAUMETTE	Responsable du Pôle AGIR Direction des Risques Accidentels		Signé
Approbateur	Qualité	Date	Emargement
Yann MACE	Directeur de la Direction des Risques Accidentels		Signé

REPERTOIRE DES MODIFICATIONS

Révision	Relecture	Application	Modifications
PROJET	Août 2006		Création du document
Version 1	Décembre 2006		Version 1 du document
Version 2	Mars 2009		<p>Modifications diverses de nature à améliorer l'appropriation de la méthode par les utilisateurs</p> <p>Explication du modèle utilisé par la méthode et de ses limites</p> <p>Précisions ou modifications mineures sur certaines étapes de la méthode et ses modalités d'application</p>

Avertissement au lecteur : Les modifications qui font l'objet de la présente version du document ne visent que très partiellement les tableaux présentés au paragraphe 4.3 qui permettent l'évaluation de la performance des barrières. Si ces tableaux ont légèrement évolué depuis la version 1 de la méthode, les modifications en question sont davantage à considérer comme des modifications de forme que de fond. Toutefois, ce document est appelé à évoluer dans le cadre d'un processus d'amélioration continue basé sur le retour d'expérience et les avancées de la recherche sur les facteurs humains.

Pour plus de détails sur le processus de développement de la méthode, voir le paragraphe 1.5.

TABLE DES MATIERES

1.	Introduction	7
1.1	Contexte général du présent document	7
1.2	Objectifs de la méthode $\Omega 20$	7
1.3	Enjeux de l'évaluation et de la démonstration de la performance des barrières humaines de sécurité	8
1.4	Cadre d'utilisation de la méthode $\Omega 20$	9
1.5	Processus de développement de la méthode	10
1.6	Plan du rapport.....	11
2.	Fondements théoriques et méthodologiques de la méthode oméga 20 ...	13
2.1	Qu'est-ce qu'une barrière humaine de sécurité ?.....	13
2.1.1	Barrières humaines de sécurité : Définition.....	13
2.1.2	Catégories de barrières humaines de sécurité retenues pour la maîtrise des risques.....	15
2.2	Quelles difficultés présente l'évaluation d'une barrière humaine de sécurité ?	16
2.3	Orientations méthodologiques retenues pour l'évaluation des barrières humaines de sécurité	16
2.3.1	Principes d'évaluation des tâches humaines de sécurité	17
2.3.2	Principes d'évaluation de l'environnement de travail.....	17
2.3.3	Principes de quantification des barrières humaines de sécurité.....	19
2.4	Limites de la méthode $\Omega 20$	20
2.4.1	Une vision simplifiée de l'homme et de son travail	21
2.4.2	Une prise en compte limitée de l'organisation.....	21
2.4.3	Des limites mais des possibilités d'articulation avec d'autres approches .	22
2.5	Bref résumé des principes fondateurs de la méthode Oméga 20	23
3.	Présentation succincte de la Méthode oméga 20.....	25
3.1	Etapes de l'évaluation $\Omega 20$	25
3.1.1	Analyse préalable : décomposition fonctionnelle et collecte des données utiles pour l'évaluation.....	25
3.1.2	Etape de sélection par critères minimaux.....	25
3.1.3	Etape d'évaluation de la performance : Niveau de confiance (NC)	26
3.2	Modalités de mise en œuvre de la démarche : recommandations	27
4.	Présentation détaillée des étapes de la Méthode Oméga 20	29
4.1	Analyse préalable : décomposition fonctionnelle et collecte des données utiles pour l'évaluation des barrières humaines de sécurité	29

4.2	Examen des critères sélectifs de performance des barrières humaines de sécurité.....	31
4.2.1	Principe d'indépendance	31
4.2.2	Efficacité (ou capacité de réalisation).....	32
4.2.3	Temps de réponse	33
4.3	Evaluation de la performance des barrières humaines de sécurité : Niveau de confiance (NC)	35
4.3.1	Première sous-fonction : obtention de l'information.....	35
4.3.2	Deuxième sous-fonction : diagnostic permettant le choix de l'action à réaliser	38
4.3.3	Troisième sous-fonction : action de sécurité à réaliser	39
4.3.4	Condition de décote complète de la barrière : Cas de la barrière humaine de sécurité faisant intervenir plusieurs acteurs	39
4.4	Application au cas des barrières mixtes à composantes techniques et humaines : les SAMS.....	40
5.	Agrégation des barrières humaines de sécurité	41
5.1	Examen de l'existence de mode commun de défaillance entre les BHS à agréger.....	41
5.2	Cas particulier de l'agrégation sur un scénario d'accident de barrières humaines de sécurité assurant la même fonction de sécurité.....	42
6.	Glossaire & définitions.....	43
7.	Références.....	47
8.	Liste des annexes	49

1. INTRODUCTION

1.1 CONTEXTE GENERAL DU PRESENT DOCUMENT

Depuis 2000, le Ministère chargé de l'Écologie et du Développement Durable finance un programme d'études et de recherches, intitulé « Formalisation du savoir et des outils dans le domaine des risques majeurs » (DRA-76).

L'objet du premier volet de ce programme est de réaliser un recueil global formalisant l'expertise de l'INERIS dans le domaine des risques accidentels. Ce recueil évolutif sera constitué de différents rapports consacrés aux thèmes suivants :

- les phénomènes physiques impliqués en situation accidentelle (incendie, explosion, BLEVE...),
- l'analyse et la maîtrise des risques,
- les aspects méthodologiques pour la réalisation de prestations réglementaires (étude de dangers, analyse critique...).

Chacun de ces documents reçoit un identifiant propre du type « Ω -X » afin de faciliter le suivi des différentes versions éventuelles du document.

In fine, ces documents décrivant les méthodes pour l'évaluation et la prévention des risques accidentels, constitueront un recueil des méthodes de travail de l'INERIS dans le domaine des risques accidentels.

Dans ce contexte, l'INERIS a développé une démarche d'évaluation des barrières techniques de sécurité, disponible dans le rapport Ω 10 [1]. L'objectif du présent document est de proposer une démarche s'inspirant de celle développée dans le rapport Ω 10 permettant de caractériser les barrières humaines de sécurité et d'évaluer leur performance. Les deux démarches présentent ainsi des similitudes utiles sur un plan pédagogique et leur application conjointe permet d'évaluer l'ensemble de l'architecture dédiée à la sécurité sur des installations industrielles.

Le présent rapport est la seconde version du document et a été rédigé sur la base du premier rapport Ω 20 daté de décembre 2006 [1].

1.2 OBJECTIFS DE LA METHODE Ω 20

Un objectif majeur de la Directive SEVESO II est la maîtrise des risques à la source ; pour ce faire, il est de la responsabilité de l'industriel de mettre en place des mesures de maîtrise des risques - appelées barrières de sécurité dans ce document - dont le but est d'assurer une prévention des risques d'accidents performante et, le cas échéant, de limiter les effets de ces accidents à l'extérieur de son site.

Les risques générés par son établissement - représentés par des scénarios accidentels - sont mis en évidence lors de la réalisation d'analyses de risques. Pour chacun des scénarios, des fonctions de sécurité sont déterminées. Ces fonctions sont remplies par des barrières de sécurité. La probabilité d'accident dans une installation classée dépend, entre autres, des performances de ces barrières de sécurité, c'est à dire de leur capacité à remplir efficacement la fonction de sécurité qui leur est dévolue.

Les barrières de sécurité peuvent être composées exclusivement d'éléments techniques : on les nomme barrières techniques de sécurité. Elles peuvent également avoir une composante humaine, c'est à dire être constituées en tout ou partie d'opérations réalisées par l'homme visant à s'opposer à l'enchaînement d'évènements susceptibles d'aboutir à un accident : on les nomme barrières humaines de sécurité.

Le développement de la démarche présentée dans ce document a été guidé par la nécessité de disposer d'outils permettant d'évaluer et de démontrer la performance des barrières humaines de sécurité. Dans les pratiques actuelles, l'évaluation et la gestion des risques sont réalisées par des « techniciens » (notamment des ingénieurs). Ces derniers n'ont généralement pas toutes les connaissances nécessaires pour prendre en compte la dimension du facteur humain pourtant primordiale dans la maîtrise des risques.

L'objectif de la démarche décrite dans ce rapport est avant tout de fournir à des "techniciens du risque" non-spécialistes des facteurs humains une méthode d'évaluation pour caractériser et évaluer la performance des barrières humaines de sécurité.

1.3 ENJEUX DE L'ÉVALUATION ET DE LA DÉMONSTRATION DE LA PERFORMANCE DES BARRIÈRES HUMAINES DE SÉCURITÉ

Il s'agit d'abord d'un enjeu de sécurité. Les industries à risques attribuent aux agents assurant leur exploitation au plus près du terrain un rôle essentiel dans la gestion de ces risques (surveillance des paramètres, détection des anomalies,...). Des dispositions doivent être mises en place par les industriels pour permettre à ces agents de remplir efficacement leur mission de sécurité (ex : élaboration de procédures, mise à disposition d'équipements, formation des agents...). Ces dispositions doivent être évaluées afin de s'assurer de leur adéquation vis-à-vis des performances de sécurité recherchées et du niveau de risque accepté. La méthode Oméga 20 a été conçue pour répondre à cet enjeu.

Il s'agit également d'un enjeu réglementaire. En France, la politique de prévention des risques technologiques repose principalement sur la réglementation des Installations Classées s'appuyant sur le code de l'environnement, modifié par la loi du 30 juillet 2003 relative à la prévention des risques technologiques et naturels et à la réparation des dommages (JO du 31 juillet 2003).

Cette nouvelle loi introduit au niveau réglementaire¹ le principe d'une étude de dangers basée sur une analyse de risque qui doit caractériser non seulement la gravité potentielle, mais aussi la probabilité d'occurrence des accidents en prenant en compte la performance des barrières de sécurité techniques et humaines, nommées sous le terme générique de « mesures de maîtrise des risques » dans les textes réglementaires. En complément, l'article 4 de l'arrêté du 29 septembre 2005 précise que "pour être prises en compte dans l'évaluation de la probabilité, des mesures de maîtrise des risques doivent être efficaces, avoir une cinétique de mise en œuvre en adéquation avec celle des événements à maîtriser, être testées, maintenues de façon à garantir la pérennité du positionnement précité".

C'est dans ce contexte que nous avons souhaité développer une méthode d'évaluation de la performance des barrières humaines de sécurité (BHS) dont les résultats seraient compatibles avec une démarche semi-quantifiée (en classe de probabilité) d'évaluation des risques.

1.4 CADRE D'UTILISATION DE LA METHODE Ω 20

Le cadre principal d'utilisation est celui de **l'évaluation des risques avec pour objectif la démonstration de la maîtrise des risques** évoqué ci-avant. Les caractéristiques de la méthode Ω 20 – sa finalité, ses choix méthodologiques, son ambition de profondeur d'analyse, ses modalités d'application et les moyens associés – ont été développées pour répondre à cet objectif et sont donc spécifiques de ce cadre d'utilisation précis.

Ainsi, l'utilisateur principal de cette méthode est l'analyste ou évaluateur de risque (ou de sûreté), qu'il soit industriel ou consultant externe pour l'industriel.

Autres cadres d'utilisation possibles :

Nous considérons que la méthode – dans son intégralité ou a minima dans ses principes – peut être utilisée avec bénéfice dans d'autres cadres et dans la perspective d'autres finalités comme par exemple :

- Dans le cadre d'une démarche d'amélioration des dispositions de sécurité mises en place : par exemple, lors de revues périodiques de ces dispositions ou d'étapes de re-conception des installations. Dans cet objectif, la méthode sera appliquée avec le souci de mettre en évidence des points d'améliorations (par exemple : amélioration de l'ergonomie du poste de travail ou des interfaces, ou des moyens d'actions, amélioration ou simplification des procédures, mise en place de vérifications supplémentaires ou de barrières supplémentaires, ...).

¹ Arrêté ministériel du 29 septembre 2005 relatif à l'évaluation et la prise en compte de la probabilité, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les installations soumises à autorisation.

- Dans le cadre de l’instruction des études de dangers présentées par l’exploitant des installations par les services de contrôle ou dans le cadre de leur analyse critique : la méthode propose des éléments d’appréciation de l’évaluation de la performance des barrières humaines de sécurité complémentaires de ceux de la « Fiche n°7 : Mesures de maîtrise des risques fondées sur une intervention humaine »² mise à disposition des inspecteurs de Installations Classées par le Ministère chargé de l’Écologie et du Développement Durable (fiche annexée au guide d’élaboration et de lecture des études de dangers pour les établissements AS du 28/12/2006).
- Dans le cadre de l’analyse d’incident : la méthode propose un modèle de la barrière et des critères descriptifs des situations de travail qui peuvent servir de grille d’analyse pour l’identification des causes d’incidents ou d’accidents.

L’utilisateur de la méthode peut alors également être auditeur interne, inspecteur des Installations Classées, acteur chargé de l’analyse d’événements ou encore toute personne chargée de sécurité.

1.5 PROCESSUS DE DEVELOPPEMENT DE LA METHODE

La méthode Oméga 20 a fait l’objet d’un développement initial et de tests d’application sur des cas industriels réels. A ce titre, nous tenons à remercier la société RHODIA qui a contribué à l’amélioration de la méthode à travers l’exploitation de tests d’application de la méthode sur plusieurs installations chimiques et par des échanges quant aux avantages et inconvénients de la méthode.

Dans le cadre d’un processus d’amélioration continue, l’Oméga 20 continue de faire l’objet de développements méthodologiques et sera ainsi amené à évoluer de manière :

- d’une part à améliorer la pertinence de la méthode de l’évaluation des barrières humaines de sécurité,
- d’autre part à répondre au mieux aux besoins des principaux utilisateurs que sont les analystes ou évaluateurs de risque.

Nous appelons les utilisateurs de la méthode à nous contacter (voir site internet www.ineris.fr) pour nous faire partager leur retour d’expérience dans une démarche doublement bénéfique d’accompagnement des utilisateurs de la méthode et d’intégration de leurs besoins et remarques dans la future version de la méthode.

²Cette fiche fournit des éléments d’appréciation sur la prise en compte des barrières humaines de sécurité dans le cadre des études de dangers. La méthode Oméga 20 s’en distingue notamment au sujet des niveaux de confiance pouvant leur être attribués.

En effet, cette fiche indique notamment que, sauf justification particulière, les mesures de maîtrise des risques fondées sur une intervention humaine de la part de l’opérateur chargé du process par ailleurs ont un niveau de confiance maximal de 1, et que les mesures de maîtrise des risques fondées sur une intervention humaine de la part d’un tiers par rapport à l’opérateur chargé du process (dans le cas d’une vérification) ont un niveau de confiance maximal de 2.

La méthode présentée ici apporte quant à elle des éléments de justification permettant d’attribuer, sous certaines conditions, un niveau de confiance de 2, y compris pour les barrières de sécurité ne faisant pas intervenir de tierce personne.

1.6 PLAN DU RAPPORT

Outre cette introduction (chapitre 1), ce document est organisé en 4 principaux chapitres.

Dans un premier temps (chapitre 2), le présent document fournit au lecteur les principaux fondements théoriques et méthodologiques devant lui permettre de se familiariser avec les termes relatifs à la performance d'une barrière humaine de sécurité. Ce chapitre permet également d'aborder les difficultés que pose l'objectif d'évaluer la fiabilité humaine. Il permettra enfin d'évoquer les choix méthodologiques effectués dans le cadre de la démarche développée dans le présent rapport et de présenter les limites associées à une telle démarche.

Ensuite (chapitre 3), l'INERIS présente de manière succincte la démarche développée pour permettre d'évaluer les barrières humaines pouvant être retenues pour la maîtrise des risques technologiques. Le lecteur pourra ainsi avoir une vision d'ensemble de la méthodologie avant de s'intéresser dans le détail aux différentes étapes nécessaires pour l'évaluation des barrières humaines de sécurité (chapitre 4). Le court chapitre qui suit (chapitre 5) présente la manière dont on peut agréger les performances évaluées d'un ensemble de barrières humaines de sécurité agissant sur un scénario dans un objectif de démonstration de la maîtrise de risques.

Enfin, le lecteur trouvera en annexe quatre exemples d'évaluation de barrières humaines de sécurité issus pour la plupart du domaine de la chimie ayant permis d'appliquer l'ensemble de la démarche proposée dans ce document.

2. FONDEMENTS THEORIQUES ET METHODOLOGIQUES DE LA METHODE OMEGA 20

L'objectif de ce chapitre est d'introduire la définition de la barrière humaine de sécurité qui est utilisée pour l'application de la méthode développée dans ce document et son rôle dans la maîtrise des risques. D'autre part, nous évoquerons de façon la plus didactique possible certains fondements théoriques et méthodologiques nécessaires pour expliciter les principes sur lesquels la méthode a été construite. Nous avons retenu de développer en particulier deux notions importantes : celle de tâche humaine de sécurité et celle d'environnement de travail. Nous espérons également ici éveiller l'intérêt du lecteur sur l'ambition et la difficulté de l'objectif que l'on se donne ici à savoir, l'évaluation, avec un objectif de quantification, de la performance de l'activité complexe que peut être une tâche humaine de sécurité. Enfin, nous attirerons l'attention sur les limites qui résultent des modèles utilisés sur l'évaluation réalisée à travers la méthode développée dans ce document.

2.1 QU'EST-CE QU'UNE BARRIERE HUMAINE DE SECURITE ?

Le concept de barrière est apparu avec celui de défense en profondeur³. Ce concept vise à la sécurisation d'un système par la mise en place d'un ensemble de mesures successives et indépendantes les unes des autres – ou encore niveaux de défense⁴ - permettant de prévenir ou de maîtriser les incidents possibles et d'en limiter les conséquences. La désignation « barrière de sécurité » utilisée dans les méthodes Oméga 10 et Oméga 20 se restreint aux systèmes actifs ou passifs, techniques ou humains, assurant une fonction de sécurité.

2.1.1 Barrières humaines de sécurité : Définition

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

Comme les barrières techniques de sécurité, les barrières humaines de sécurité se définissent par la fonction de sécurité⁵ qu'elles assurent vis-à-vis d'un scénario d'accident majeur.

³ Ce concept a été utilisé aux Etats-Unis par l'AIEA (Agence internationale de l'énergie atomique) dans les années 1960 pour concevoir la sécurité des premiers réacteurs nucléaires.

⁴ Parmi ces niveaux de défense, on trouve les dispositions adoptées en matière de conception, construction et modalités d'exploitation incluant la maintenance et les mesures d'urgence internes et externes.

⁵ Fonction ayant pour but la prévention et la protection d'évènements redoutés

Elles se définissent également par les éléments qui la composent : les barrières humaines de sécurité ont **une composante humaine, le plus souvent associée à une composante technique** (l'opérateur est *a minima* en interaction avec les éléments techniques du système qu'il surveille ou sur lesquels il agit). Lorsque la barrière est composée d'éléments techniques de sécurité entrant dans une chaîne de sécurité, on parle de **Système à Action Manuelle de Sécurité (SAMS)**.

La *Figure 1* présente une typologie des barrières de sécurité qui illustre les différents types de barrières.

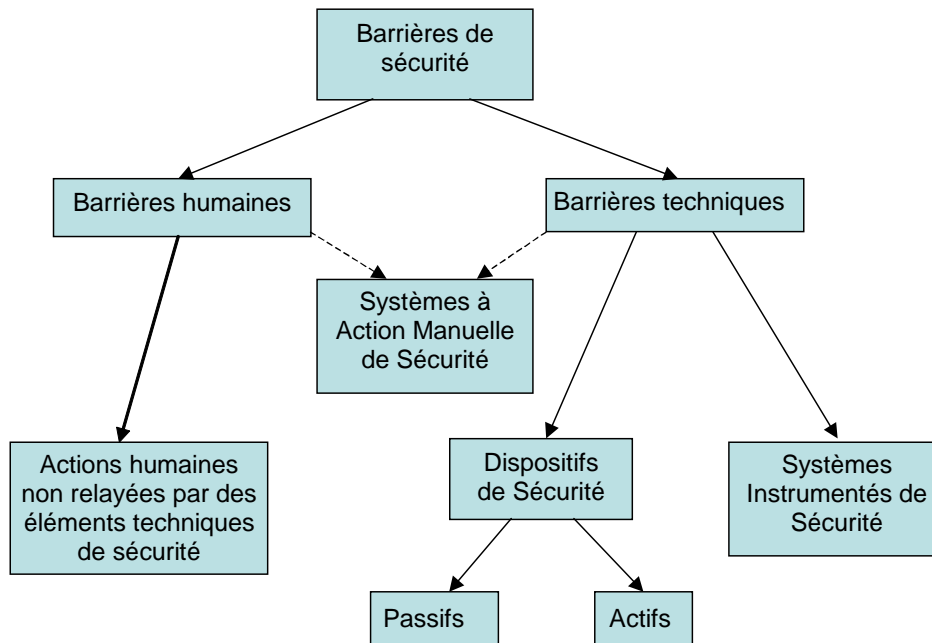


Figure 1 : Typologie des barrières de sécurité (complément de la typologie présentée dans le rapport Ω 10 [1].

Exemples de barrières humaines de sécurité :

- Opération de contrôle de l'étanchéité d'un circuit conditionnant la mise en service du circuit.
- Action de fermeture manuelle d'une vanne suite à la détection visuelle d'une augmentation anormale de la pression d'un réacteur.

Exemple de SAMS :

- Action de mise en sécurité de l'installation par actionnement d'un bouton d'arrêt d'urgence suite à une détection de fuite de gaz au cours d'une ronde de surveillance.

Remarque importante :

L'objet de ce document est de proposer une démarche permettant d'aider à l'évaluation de ces deux types de barrières de sécurité. **Pour les Systèmes à Action Manuelle de Sécurité, la démarche d'évaluation présentée dans ce document s'applique exclusivement à la composante humaine de la chaîne de sécurité. Pour disposer d'une évaluation complète, le lecteur pourra faire le lien avec la démarche présentée dans le rapport Ω 10 [1].**

2.1.2 Catégories de barrières humaines de sécurité retenues pour la maîtrise des risques

Le parti pris pour l'identification des barrières humaines est de considérer l'homme, dans un système industriel, dans sa fonction de prévenir ou de rattraper les dérives d'un procédé ou d'une activité à risques. Les activités humaines qui concourent au fonctionnement normal d'exploitation du système ne sont donc pas prises en compte. Par exemple, le chargement de réactif dans un réacteur n'est pas considéré comme une barrière de sécurité.

L'application de ce principe conduit à identifier deux types d'actions susceptibles d'être considérées comme indépendantes :

- Celles qui interviennent en amont d'une activité ou du démarrage du procédé susceptible de présenter des risques d'accident majeur et consistent en la préparation de cette activité, sous l'angle de la sécurité : la fonction de sécurité sera de vérifier que les conditions d'occurrence d'un scénario d'accident sont maîtrisées préalablement à une activité à risques. **Ces barrières seront appelées "barrières de vérification".**
- Celles qui prennent place au cours (ou en aval) de l'activité ou du procédé susceptible de présenter des risques d'accident majeur et dont la fonction de sécurité sera de détecter une dérive prévue et d'agir en vue de limiter ses conséquences. L'action de ces barrières s'inscrit dans la cinétique de la séquence incidentelle ou accidentelle. **Ces barrières seront appelées "barrières de rattrapage".**

La détection de la dérive peut être réalisée à différents stades de l'activité dangereuse : par exemple très en amont de l'évènement redouté comme certaines rondes de surveillance et campagnes d'inspection des équipements ou encore en aval de l'évènement redouté comme les rattrapages de dérive de procédé (intervention sur montée en température anormale d'un réacteur) ou même en aval du phénomène dangereux (intervention sur un cas de feu).

2.2 QUELLES DIFFICULTES PRESENTE L'EVALUATION D'UNE BARRIERE HUMAINE DE SECURITE ?

L'évaluation des barrières humaines de sécurité ne peut pas se résumer à la simple évaluation des compétences humaines. Leur fiabilité ne dépend pas uniquement des hommes chargés de leur mise en œuvre, elle découle également des situations conçues, aménagées ou organisées pour leur permettre de remplir leur mission. Contrairement à ce que peut laisser entendre l'expression « fiabilité humaine », la fiabilité humaine n'est pas réductible à la seule fiabilité du seul composant humain. La fiabilité humaine est en réalité celle de l'homme pris dans son environnement, par nature complexe (matériel, procédural, organisationnel, culturel...). La fiabilité humaine dépend de ces différents facteurs humains et environnementaux, de leur complémentarité et de leurs influences sur les différents processus en jeu dans le travail des hommes (cognitif, affectif, sociologique, physique,...).

Pour une situation donnée, il s'agit d'identifier **les facteurs les plus déterminants vis-à-vis de la réussite de la tâche de sécurité humaine considérée** et de les caractériser en fonction de l'aide qu'ils apportent à l'homme pour remplir sa mission (**facteurs d'aide**), ou des menaces qu'ils font peser sur le succès de celle-ci (**facteurs perturbateurs**).

L'évaluation des barrières humaines de sécurité ne peut pas non plus se résumer à la simple évaluation des règles de sécurité telles que présentées dans les procédures. En effet, le travail de l'homme se différencie de la simple application des règles prescrites : il consiste en des ajustements permanents, plus ou moins importants, et plus ou moins conscients, par rapport à ces règles pouvant conduire selon les cas à des actions inappropriées ou bien à des actions favorables à la sécurité. L'application mécanique par l'homme des règles de sécurité n'est pas possible : en effet, ces règles font irrémédiablement l'objet d'une interprétation de la part de l'homme, en fonction notamment de son expérience et du contexte de la situation. En outre, les situations de travail sont par nature singulières, compte tenu de leur variabilité notamment en termes d'exigences d'exploitation, de contraintes organisationnelles ou de ressources techniques. Cette variabilité, en excluant la possibilité de prévoir dans leur exhaustivité toutes les situations de travail, confirme l'impossibilité d'une application mécanique par l'homme des règles de sécurité.

L'évaluation des barrières humaines de sécurité implique donc un travail d'analyse qualitative des modalités réelles de leur mise en œuvre, compte tenu notamment des connaissances des agents concernés et de leurs conditions de travail. Cette démarche s'inscrit donc d'abord dans une approche ergonomique des situations de travail.

2.3 ORIENTATIONS METHODOLOGIQUES RETENUES POUR L'EVALUATION DES BARRIERES HUMAINES DE SECURITE

Nous allons développer dans le paragraphe suivant les principes avec lesquels nous avons utilisé l'approche ergonomique des situations de travail pour élaborer notre méthode d'évaluation des barrières humaines de sécurité.

2.3.1 Principes d'évaluation des tâches humaines de sécurité

La méthode Oméga 20 a été conçue pour le plus grand nombre de barrières. Pour des raisons pédagogiques, elle a été élaborée à partir d'une vision du travail de l'homme proche du fonctionnement des systèmes instrumentés de sécurité. En effet, l'Oméga 20 considère que l'homme est composé de trois systèmes : un système sensoriel, un système cognitif et un système moteur. A l'image des systèmes instrumentés, nous supposons que ces systèmes interviennent successivement dans l'acquisition et le traitement d'information, la prise de décision et la production d'un comportement de sécurité.

Ce modèle de tâche, très simplificateur, est proche des modèles généraux développés en psychologie ergonomique pour rendre compte en première analyse des activités humaines. L'une des grilles d'analyse des tâches humaines les plus utilisées, inspirée de Rasmussen [3], considère trois principales sous-tâches : détection, traitement de l'information et action.

La méthode Oméga 20 propose donc de décomposer les barrières humaines de sécurité en trois principales sous-tâches : détection, diagnostic et action.

- **Détection (ou obtention de l'information)** : il s'agit d'obtenir une ou plusieurs informations permettant d'identifier ou de détecter une défaillance ou une dérive pouvant mener à un accident majeur ou le phénomène en lui-même. L'opérateur peut avoir un rôle plus ou moins actif dans l'obtention de cette/ces information(s).
- **Diagnostic permettant le choix de l'action de sécurité** : il s'agit de produire un diagnostic à partir de la ou des informations obtenues à l'issue de la phase précédente et de faire le choix de l'action de sécurité qui devra être réalisée.
- **Action** : il s'agit d'une action (ou d'un enchaînement d'actions) manuelle ou relayée par un système technique qui, sous condition de son efficacité, s'oppose au scénario d'accident majeur prévu (actions sur un élément de sécurité ou un élément agresseur de l'installation).

La méthode Oméga 20 propose d'évaluer l'influence de l'environnement sur les performances de chacune de ces sous-tâches.

2.3.2 Principes d'évaluation de l'environnement de travail

La méthode Oméga 20 considère l'homme comme un utilisateur des ressources et moyens (en temps, compétences, informations...) mis à sa disposition pour lui permettre de remplir ses missions. Elle propose une démarche visant à évaluer l'adéquation ou la suffisance de ces moyens vis-à-vis des objectifs à atteindre. L'Oméga 20 propose de procéder à cette évaluation à partir d'un ensemble de facteurs généraux déterminant la fiabilité humaine, caractéristiques ou descriptifs des conditions et de l'environnement du travail des opérateurs, et choisis pour leur pertinence vis-à-vis du plus grand nombre d'interventions ou tâches de sécurité.

Ces « facteurs déterminants » concernent pour l'essentiel les rapports entre un signal ou une information, les hommes et les actions de sécurité à réaliser :

- présentation et accès des informations,
- disponibilité de l'opérateur,

- qualité des informations utiles au diagnostic,
- niveau de guidage pour le choix de l'action,
- niveau de stress dans le contexte de l'action,
- niveau d'exigence et de complexité de l'action.

Il existe plusieurs classifications des facteurs déterminants la fiabilité humaine. L'une des plus utilisées est la classification proposée par Hollnagel [4], illustrée par la Figure 2. Selon ce modèle, la performance de l'action humaine peut être considérée comme le résultat des interactions entre trois principales catégories de facteurs : Homme, Technologie et Organisation.

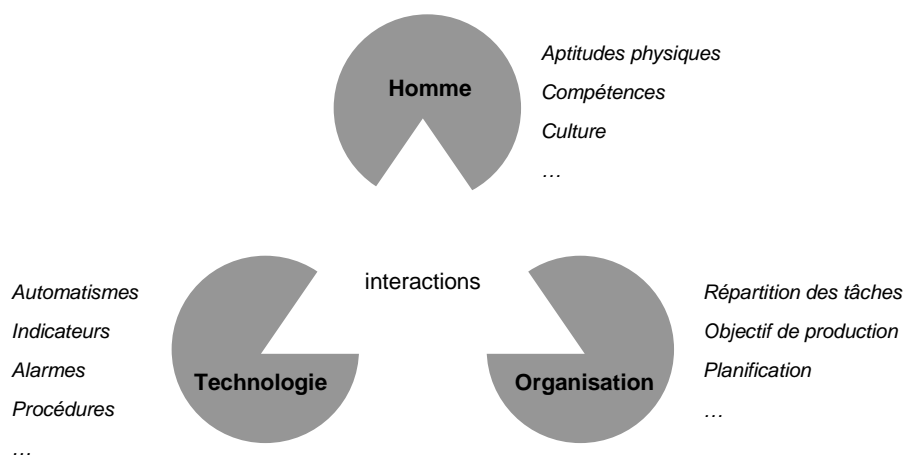


Figure 2 : Modèle des causes et manifestations de l'erreur humaine (d'après Hollnagel, 1998)

Nous considérons que ce type de classification peut aider à l'identification des facteurs déterminants. Toutefois, nous considérons également qu'un inventaire complet de ces facteurs n'aurait de sens que s'il était possible de prétendre à cette exhaustivité, ce qui n'est pas le cas. Pour la méthode $\Omega 20$, nous avons fait le choix d'encourager les utilisateurs à rechercher les facteurs les plus pertinents vis-à-vis des situations. De plus, l'expérience montre que l'enjeu de cette identification tient moins à l'exhaustivité de l'inventaire réalisé qu'à la pertinence des facteurs identifiés vis-à-vis des spécificités des situations.

L'identification de ces facteurs (ou facteurs déterminants) est un exercice qui demande de bien connaître les situations de travail concernées, tant du point de vue de ce qu'il est requis en terme de sécurité (ex : fermeture d'une vanne) que du point de vue du travail des opérateurs impliqués, tel qu'ils l'effectuent habituellement, y compris dans certaines situations dégradées. **C'est par le jeu de la comparaison entre les situations de travail telles qu'elles sont prévues et les situations de travail telles qu'elles sont réellement gérées qu'il est possible de mettre en évidence les facteurs facilitant ou perturbant la réalisation des missions de sécurité confiées aux hommes.**

L'identification de ces facteurs déterminants est importante vis-à-vis de la qualité de l'évaluation de la barrière. Elle s'effectue par la comparaison entre :

- Des données théoriques, formelles, et prescriptives sur la tâche et les conditions prévues de sa réalisation, telles que les définissent les concepteurs et managers des installations. Ces données sont le plus souvent formalisées dans des modes opératoires, des procédures ou notes d'organisation.
- Des données plus informelles et plus subjectives sur le contexte et les pratiques réelles de travail. Ces données correspondent par exemple à certaines situations perturbées ou non prévues par l'organisation dans le cadre desquelles les hommes ont développé différentes stratégies ou formes d'adaptation, conscientes ou non, leur permettant d'atteindre les objectifs fixés moyennant certains compromis (ex : compte tenu de l'urgence d'une situation, un opérateur confie l'une de ses tâches à un autre opérateur).

L'analyse du caractère facilitant ou perturbateur des facteurs ainsi identifiés sera la première étape devant permettre d'apprécier qualitativement dans un premier temps le risque d'échec de chacune des sous-tâches dans le cadre de la méthode $\Omega 20$. Il s'agira ensuite pour répondre à l'objectif de quantification de la performance de la barrière de « traduire », à l'aide des outils proposés par la méthode, le risque d'échec de chacune des sous-tâches constituant la barrière de sécurité en taux d'échec global de la mission confiée à l'opérateur, exprimé quantitativement.

2.3.3 Principes de quantification des barrières humaines de sécurité

Le taux de défaillance ou d'échec d'une mission confiée à un opérateur peut être rapproché d'une notion équivalente habituellement utilisée pour un dispositif technique : la probabilité de défaillance à la demande (PFD). On peut étendre cette notion à l'action humaine pour évaluer la probabilité de défaillance à la demande de l'opérateur en charge d'une action de sécurité.

On peut trouver dans la bibliographie [5] des ordres de grandeur de taux de défaillance des actions humaines. Voici, par exemple, des valeurs que l'on trouve dans l'annexe F de la norme NF-EN 61511-3 [6] pour estimer la probabilité de défaillance à la demande (PFD).

Action d'un homme entraîné et sans stress	: $1,0 \times 10^{-2}$ à $1,0 \times 10^{-4}$,
Réponse d'un opérateur à une alarme	: $1,0 \times 10^{-1}$,
Action d'un homme stressé	: 0,5 à 1.

Ces valeurs sont des grandeurs qui ne rendent pas compte de divers paramètres d'influence tels que la nature de la tâche qui était demandée ou encore le contexte environnant l'opérateur. Il existe néanmoins plusieurs méthodes d'évaluation de la fiabilité (THERP, SHERPA, ...) qui utilisent ce type de données quantifiées, en les corrigeant par des facteurs d'influence.

La méthode THERP par exemple prend en compte plusieurs dizaines de facteurs d'influence sur les actions humaines tels que le nombre d'heures de travail, la température, la complexité, la pression temporelle ... etc.

En 1985, une étude a été menée par le JRC⁶ afin de procéder à une évaluation croisée de la probabilité de la défaillance humaine sur une séquence « incidentelle » identifiée sur un site nucléaire [7]. Quinze équipes de spécialistes de 11 pays différents ont procédé à cette évaluation. Les résultats mettent en lumière des difficultés d'application - lourdeur de mise en œuvre et sensibilité au jugement d'expert - et une insuffisante prise en compte des interactions de l'homme avec l'organisation et la culture d'entreprise.

Bien que d'autres méthodes plus récemment développées permettent de répondre à certaines des critiques adressées habituellement aux méthodes d'EPFH (Evaluation Probabiliste de la Fiabilité Humaine), des difficultés demeurent : incertitudes attachées aux évaluations, sensibilité au jugement d'expert, ... etc. Les spécialistes des facteurs humains s'accordent à dire que les connaissances sur les mécanismes de l'erreur humaine sont aujourd'hui suffisamment importantes pour mieux concevoir les interfaces, mais qu'elles ne sont encore que des modèles simplifiés d'une activité mentale, et de réalités complexes. Elles ne permettent pas de prédiction précise, au sens de celles qui sont développées dans les sciences pour l'ingénieur (comportement des produits, comportements des équipements de sécurité).

Aussi, compte-tenu de ces limites, nous avons fait le choix d'adopter une quantification par classe de probabilité et une démarche *a priori* conservative, en considérant une probabilité nominale de défaillance humaine de 10^{-2} ; cette probabilité de défaillance devant être revue à la hausse en cas d'identification de facteurs perturbateurs de la fiabilité humaine lors de l'analyse de la situation de travail mais ne pouvant jamais être inférieure.

La méthode Oméga 20 se distingue de ce point de vue des pratiques plus forfaitaires basées sur la seule utilisation de base de données, référant le plus souvent à des données trop générales n'intégrant pas les spécificités de l'environnement des barrières évaluées.

2.4 LIMITES DE LA METHODE Ω 20

Les orientations évoquées ci-avant ainsi que les choix méthodologiques présentés aux paragraphes précédents sont justifiés par l'objectif et le cadre d'utilisation prévu de la méthode. En effet, rappelons que l'approche développée dans ce document est dictée par une finalité pragmatique de transfert pour des non-experts des disciplines des facteurs humains, mais experts dans le domaine des risques industriels. Ces choix impliquent deux limites majeures dont le lecteur doit être averti. Elles sont évoquées dans les paragraphes suivants.

⁶ Le JRC (Joint Research Center) ou Centre Commun de Recherche est l'organisme scientifique de la Commission européenne.

2.4.1 Une vision simplifiée de l'homme et de son travail

La vision simplifiée de la tâche humaine (détection, diagnostic et action) présente l'avantage d'être facile à s'approprier pour le plus grand nombre d'utilisateurs. En revanche, elle ne prend pas en compte un certain nombre d'autres caractéristiques de l'homme et de son comportement : ses capacités d'anticipation des aléas et de récupération de ses propres erreurs, l'influence de sa culture de sécurité, son rapport au risque, sa confiance dans les procédures, sa personnalité, sa rigueur, ses valeurs, ses croyances, ses rapports à ses collègues, sa résistance au stress...

Selon les cas, ces dimensions affectives, sociales et culturelles peuvent avoir une influence sur la performance des BHS parfois plus importante que les dimensions cognitives et physiologiques prises en compte dans l'Oméga 20. Par exemple, ces dimensions sont prédominantes dans la performance des barrières symboliques reposant sur le respect de certaines interdictions (interdiction de fumer, interdiction de pénétrer dans un local, ...etc.). La prise en compte de ces dimensions nécessite des démarches d'analyse complémentaires qui exigent des connaissances en psychologie du travail, en ergonomie ou en sociologie et une profondeur d'analyse plus importante. Ces disciplines permettent également de mieux prendre en compte les aspects collectifs et relatifs à la coopération entre acteurs pour la mise en œuvre des barrières humaines de sécurité.

En conséquence, la méthode ne permet pas d'appréhender l'ensemble des modes d'échec comme des modes de bon fonctionnement de ces barrières, ce qui est inhérent à toute démarche d'analyse de ce type. En d'autres termes, nous considérons que la vision du travail de l'homme sur laquelle repose la méthode et les critères d'évaluation associés permet d'appréhender une partie essentielle - et à la portée des non-spécialistes - des dimensions du fonctionnement des barrières humaines.

2.4.2 Une prise en compte limitée de l'organisation

Nous considérons que les barrières humaines de sécurité sont des systèmes socio-techniques conçus, maintenus et contrôlés par un ensemble de processus accompagnant leur évolution ou cycle de vie : mise à jour de consignes, maintenance des systèmes de supervision, formation et maintien des compétences, contrôle hiérarchique et audit, ...etc. Ces processus concourent à garantir aux hommes les moyens d'action ou ressources dont ils ont besoin pour agir et faire face à d'éventuelles perturbations permettant ainsi de maintenir dans le temps un niveau de fiabilité satisfaisant des tâches de sécurité. **Ainsi, nous considérons que la performance de chacune des barrières humaines de sécurité est sous la dépendance de celle d'un ensemble de processus organisationnels.**

Autrement dit, nous pouvons considérer que **le maintien des performances des barrières humaines devra être assuré par des moyens organisationnels mis en place par l'entreprise**. Ces moyens, normalement gérés par les processus de gestion de la sécurité (décrits par le système de Gestion de la Sécurité ou SGS), sont les suivants :

- les moyens de maintien dans le temps de la compétence : formation, entraînement, exercices,
- les moyens de gestion des dérives et migrations des pratiques et de maintien dans le temps des ressources : gestion des modifications et maîtrise d'exploitation,
- les moyens de contrôle de la performance des barrières : exercices, contrôles,
- les moyens de surveillance du système, de détection des dérives et d'amélioration des pratiques : audits et système de retour d'expérience.

Toutefois, la méthode Oméga 20 n'a pas pour objectif et ne permet pas d'évaluer ces processus organisationnels. L'évaluation de ces processus organisationnels fait appel à d'autres types de démarches (audit, diagnostic organisationnel) qui seront alors complémentaires à la démarche proposée dans l'Oméga 20.

Nota :

Dans le cadre de la méthodologie développée dans ce document, on ne peut pas évaluer *a priori* la performance d'une procédure, d'un ensemble de moyens organisationnels (PPR, POI) ou d'un processus de gestion (comme la maintenance et la formation). Seules les dispositions opérationnelles qui sont prévues dans le cadre de l'application de ces procédures, moyens organisationnels ou processus de gestion, peuvent être évaluées par la méthode Ω 20.

2.4.3 Des limites mais des possibilités d'articulation avec d'autres approches

Comme déjà indiqué à l'issue du paragraphe 2.2, la méthode Oméga 20 s'inscrit dans une approche ergonomique de l'évaluation des situations de travail. Toutefois, si les enjeux de la méthode Oméga 20 convergent avec ceux de la méthodologie d'analyse ergonomique, la méthode Oméga 20 s'en distingue au moins selon deux points de vue, parmi lesquels celui des hypothèses volontairement simplificatrices sur lesquelles repose l'Oméga 20 et celui de la complexité et du coût volontairement limités de sa mise en œuvre.

Nécessairement simplificatrice, cette méthode propose une première approche qui, selon le contexte et les enjeux, pourra être complétée par la mise en œuvre par des spécialistes des «facteurs humains et organisationnels» de méthodes d'analyse plus représentatives de la complexité des systèmes de travail.

2.5 BREF RESUME DES PRINCIPES FONDATEURS DE LA METHODE OMEGA 20

La méthode Oméga 20 est une méthode qui propose une première approche des facteurs humains accessible aux gestionnaires de risques pour évaluer la performance des barrières humaines de sécurité.

Elle se base sur une analyse qualitative de la situation de travail correspondant à la mise en œuvre de la barrière humaine de sécurité. La situation de travail est analysée pour mettre en évidence des facteurs aidant ou perturbant la réalisation des missions de sécurité confiées aux hommes. Cette analyse fait appel au jugement et à l'expertise d'un groupe de travail, dans le but de comparer les situations de travail telles qu'elles sont prévues et les situations de travail telles qu'elles sont réellement gérées.

Pour répondre au besoin d'évaluation quantitative des performances des barrières de sécurité, la méthode propose un système de cotation permettant, à partir de l'analyse qualitative, de déterminer une classe de probabilité de défaillance de la barrière de sécurité.

3. PRESENTATION SUCCINCTE DE LA METHODE OMEGA 20

Nous rappelons que préalablement à l'application de notre démarche, l'ensemble des situations dangereuses ainsi que les fonctions de sécurité permettant de prévenir ou limiter les conséquences de ces situations dangereuses auront été identifiées au cours d'une analyse des risques.

3.1 ETAPES DE L'EVALUATION Ω 20

La démarche comprend d'abord une **analyse qualitative** menée en groupe de travail nécessitant un effort de collecte de données sur la situation de travail étudiée.

Les données collectées permettent dans un premier temps de « sélectionner » la barrière en s'assurant qu'elle satisfait aux trois critères minimaux suivants :

- **L'indépendance,**
- **L'efficacité (ou capacité de réalisation),**
- **Le temps de réponse,**

Une fois « sélectionnée », la barrière est évaluée pour sa contribution à la réduction des risques d'accident. Cette **évaluation** se fait à travers le critère du **niveau de confiance**.

3.1.1 Analyse préalable : décomposition fonctionnelle et collecte des données utiles pour l'évaluation

Pour pouvoir répondre aux critères de sélection et de performance des barrières humaines de sécurité, une étape préalable est nécessaire : elle vise à permettre la décomposition fonctionnelle de la barrière humaine de sécurité selon le découpage (détection, diagnostic, action), ce qui implique également d'identifier les éléments qui décrivent chacune de ces sous-actions. Il s'agit aussi de collecter un ensemble suffisant d'informations pertinentes pour renseigner les différents critères d'évaluation proposés par la méthode. Ces critères concernent pour l'essentiel le niveau d'exigences de la tâche et sa faisabilité par les hommes impliqués compte tenu de l'adéquation des dispositifs techniques prévus.

3.1.2 Etape de sélection par critères minimaux

1 – Vérification du principe d'indépendance :

La barrière humaine de sécurité doit être **indépendante** de l'événement initiateur pouvant conduire à sa sollicitation pour pouvoir être retenue en tant que barrière agissant sur le scénario induit par l'événement initiateur. **Ses performances ne doivent pas être dégradées par l'occurrence de l'évènement initiateur.**

2- Evaluation de l'efficacité :

L'efficacité est l'aptitude de la barrière de sécurité à remplir la fonction de sécurité pour laquelle elle a été choisie, dans son **contexte d'utilisation** et **pendant une durée donnée de fonctionnement**.

L'évaluation de l'efficacité repose sur les principes de **dimensionnement adapté** et de **résistance aux contraintes spécifiques**.

3- Evaluation du temps de réponse :

Le temps de réponse 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.

Rappelons que **pour qu'une barrière soit retenue selon ce critère, le temps de réponse de la barrière doit être en adéquation avec la cinétique du phénomène qu'elle doit maîtriser, c'est-à-dire qu'il doit être significativement inférieur à la cinétique**.

3.1.3 Etape d'évaluation de la performance : Niveau de confiance (NC)

Le NC permet de déterminer un facteur de réduction de risques induit par les barrières selon la correspondance suivante : pour une barrière de niveau de confiance NC la **réduction de risques est de manière conservative 10^{NC}** : Le tableau qui suit présente les équivalences entre niveau de confiance, probabilité de défaillance à la demande et facteur de réduction du risque.

PFD	NC	Facteur de réduction du risque
$10^{-3} \leq \text{PFD} < 10^{-2}$	2	100
$10^{-2} \leq \text{PFD} < 10^{-1}$	1	10
$\text{PFD} \geq 10^{-1}$	0	1

Tableau 1 : correspondance entre niveau de confiance, probabilité de défaillance et facteur de réduction du risque

L'évaluation du NC s'effectue en 3 étapes, correspondant aux trois sous-fonctions par lesquelles on décompose la barrière humaine de sécurité (détection, diagnostic et action). Pour chacune des sous-fonctions, un tableau permet d'associer une décote en fonction des caractéristiques de la situation de travail à analyser.

Dans le cas de barrière de sécurité faisant intervenir plusieurs acteurs, des critères qualitatifs associés à la dimension collective de la barrière devront être vérifiés. La prise en compte de cette dimension nécessite comme le reste de la démarche une réflexion adaptée au contexte.

La méthode proposée dans le présent document postule que le niveau de confiance maximal d'une barrière humaine de sécurité est de 2 ($10^{-2} \geq \text{PFD} \geq 10^{-3}$). Selon le niveau de décote associé à la barrière analysée, le niveau de confiance final pourra être de 2, 1 ou 0.

3.2 MODALITES DE MISE EN ŒUVRE DE LA DEMARCHE : RECOMMANDATIONS

La qualité de l'évaluation dépendra du niveau de compréhension de la dimension réelle de la situation de travail et de la capacité des utilisateurs à intégrer ces éléments de connaissance dans l'appréciation des critères génériques de la méthode.

Deux points de vue complémentaires doivent être pris en compte :

- Les points de vue de l'expert technique du procédé ou de l'activité opérationnelle en jeu, du « concepteur » de la barrière de sécurité et des personnes chargées d'en contrôler l'application : quelles sont les actions efficaces et prescrites, dans quel but et avec quels résultats attendus vis-à-vis du procédé ou de l'activité à maîtriser, quel contexte et quelles conditions associés ont été imaginés, ... ?
- Le point de vue de/des opérateur(s) en charge des actions constitutives de la barrière de sécurité : comment l'opérateur répond-t-il habituellement aux consignes et prescriptions (est-ce bien en adéquation avec l'objectif poursuivi dans le cadre de la barrière de sécurité ?), quelles limites ou difficultés pour la réalisation de l'action son expérience lui fait-il connaître ou envisager, ... ?

Pour ces raisons, l'évaluation doit impérativement se faire dans le cadre d'un groupe de travail, animé par un garant de la méthode, résulter d'un travail collectif et d'interactions entre les différents membres du groupe de travail de manière à faire émerger les éléments d'appréciation des différents critères de la méthode sur la base d'une vision la plus proche possible de la situation réelle de travail.

Certaines précautions doivent donc être prises et le garant de la méthode attachera un soin particulier à favoriser l'expression du/des opérateur(s) d'éléments de connaissance de la situation de travail issus de son propre retour d'expérience ou de celui de ses collègues en charge de la même barrière de sécurité.

En préalable à la tenue du groupe de travail, il est indispensable de faire une visite sur le terrain des installations et des postes de travail concernés pour se rendre compte par exemple :

- de l'environnement physique - distances, luminosité, accessibilité, etc -
- de la clarté des informations à traiter par l'opérateur,
- de l'accessibilité des modes opératoires, moyens d'aide ou d'actions,
- etc.

Une visite de terrain et la constitution d'un groupe de travail, animé par un garant de la méthode et comprenant des représentants des différentes fonctions concernées par la tâche de sécurité et ses enjeux, sont requises.

4. PRESENTATION DETAILLEE DES ETAPES DE LA METHODE OMEGA 20

Dans ce chapitre, le terme « barrière humaine de sécurité » est également utilisé pour désigner la composante humaine d'une barrière de sécurité, au sens donné dans la définition du SAMS.

4.1 ANALYSE PREALABLE : DECOMPOSITION FONCTIONNELLE ET COLLECTE DES DONNEES UTILES POUR L'EVALUATION DES BARRIERES HUMAINES DE SECURITE

Nous désignons par « situation de travail » le système formé par la tâche de sécurité, de l'ensemble des moyens conçus pour permettre aux opérateurs de satisfaire les exigences de la tâche et des autres facteurs susceptibles d'en perturber la réalisation. En corollaire, nous considérons que la performance des tâches de sécurité dépend de la suffisance et de l'adéquation des moyens conçus compte tenu des exigences de la tâche mais aussi des effets prévisibles d'un certain nombre de facteurs perturbateurs ou menaces.

Il s'agit donc de :

- analyser les exigences de la tâche à partir d'une décomposition fonctionnelle de la barrière de sécurité en trois sous-fonctions,
- collecter les données relatives à la situation de travail afin de mettre en évidence les facteurs facilitant ou perturbant la réalisation des missions de sécurité confiées aux hommes.

Le premier résultat de cette étape correspond à la décomposition de la barrière de sécurité suivant les trois sous-fonctions qui la composent.

Le tableau suivant donne un exemple de décomposition fonctionnelle de la barrière humaine de sécurité « Opération de contrôle de l'étanchéité d'un circuit conditionnant la mise en service du circuit ».

Obtention de l'information	Diagnostic / choix de l'action de sécurité	Réalisation de l'action de sécurité
Information obtenue par application d'un produit moussant et circulation d'air sous pression à l'intérieur du circuit	Interprétation du bullage en surface du circuit comme défaut d'étanchéité	Suspendre la mise en service du circuit

Tableau 2 Exemple de décomposition fonctionnelle de la barrière humaine de sécurité

Nota : Attention à la définition de l'action de sécurité :

L'action de sécurité incluse dans la BHS est réduite aux tâches permettant de s'opposer au scénario d'accident prévu. C'est à dire qu'elle n'englobe notamment pas les activités de remise en état des installations faisant suite à une détection d'anomalie.

Par exemple, suite à la possibilité d'occurrence d'un scénario de fuite par corrosion, une barrière humaine de sécurité a été mise en place : elle consiste à réaliser un contrôle périodique d'épaisseur des canalisations. Lorsque ce contrôle aboutit à l'identification d'un défaut (phases de détection et de diagnostic), il est prévu un remplacement du tube incriminé. L'action de sécurité de la barrière n'est pas le remplacement du tube mais l'arrêt de l'installation (ou le by-pass de la portion de canalisation) avant l'occurrence du scénario.

Le second résultat de cette étape d'analyse et de collecte de données consiste à identifier les éléments relatifs :

- **aux moyens prévus pour la réalisation de la tâche de sécurité** : personnes en charge des actions, délai disponible, ressources utilisées (procédures, outils, documentation, ..., etc), dispositifs de signalisation utilisés et éléments de commande actionnés,
- **aux éléments de contexte** liés à l'environnement, aux conditions de travail, à l'activité générale en cours, ...

Comme expliqué dans le chapitre précédent, **les modalités de collecte de ces données sont celles du groupe de travail**. Celui-ci pourra s'appuyer sur des méthodes d'analyse et de questionnement de type QQQCCP⁷ ou 5M⁸. Il pourra également être utile d'exploiter les données issues d'observations in situ, d'exercices, du retour d'expérience sur la mise en œuvre des barrières, et sur les situations incidentelles/accidentelles rencontrées.

Notons qu'il est intéressant de tracer ces éléments à des fins diverses : justification de la démonstration de l'évaluation, prise en compte d'éléments fins de contexte, capitalisation de l'expérience du groupe de travail, ...etc.

⁷ QQQCCP : Quoi – Qui – Où – Quand – Comment – Combien – Pourquoi ?

⁸ 5M : Milieu, Méthode de travail, Matière (produits), Matériel, Main d'œuvre

4.2 EXAMEN DES CRITERES SELECTIFS DE PERFORMANCE DES BARRIERES HUMAINES DE SECURITE

4.2.1 Principe d'indépendance

Pour pouvoir retenir une barrière humaine de sécurité vis-à-vis d'un scénario d'accident, il est nécessaire qu'elle soit **indépendante de la cause du scénario ou du scénario lui-même**. La BHS doit être **indépendante** de l'événement initiateur pouvant conduire à sa sollicitation pour pouvoir être retenue en tant que barrière agissant sur le scénario induit par l'événement initiateur, c'est à dire que l'opérateur en charge de la barrière et les éléments techniques dont il se sert doivent être indépendants de la cause du scénario ou du scénario lui-même.

Ce premier principe d'indépendance est un critère de sélection dans le cadre de la démarche barrière. **Si ce critère n'est pas vérifié, la démarche s'arrête à ce stade : la barrière ne peut pas être retenue.**

Traduit d'une autre manière, la vérification de l'indépendance de la barrière revient à « vérifier l'indépendance entre la tâche de sécurité et la tâche d'exploitation ». Cette vérification consiste à s'interroger sur les dépendances entre les causes d'échec de la barrière sur le scénario et la cause même du scénario (par exemple, une défaillance technique ou une erreur opératoire).

Pour le cas des barrières de rattrapage, le mode de dépendance éventuel est souvent aisé à identifier. Par exemple, si un débordement est causé par un malaise d'un opérateur, on ne peut pas considérer l'action de ce même opérateur en rattrapage du débordement : la barrière est sous la dépendance de la cause du scénario.

Pour les barrières de vérification, cela peut être plus délicat, les fonctions de sécurité et d'exploitation étant structurellement moins séparées que dans le domaine technique (Par exemple, les bonnes pratiques industrielles se traduisent fréquemment par une redondance d'une vanne d'exploitation avec une vanne de sécurité.)

En ce qui concerne les opérations de vérification, l'indépendance de la barrière de sécurité pourra être assurée de deux manières :

- La tâche de sécurité est réalisée par une personne différente de celle qui a réalisé l'action d'exploitation : cela correspond à une forme d'indépendance "organisationnelle".
- La tâche de sécurité s'inscrit dans une séquence de travail différente de l'action d'exploitation⁹ : cela correspond à une forme d'indépendance "temporelle".

⁹ A noter que la capacité de l'opérateur à se contrôler en cours de réalisation de l'action et à rattraper la situation en cas de détection d'une erreur est un processus inhérent à l'être humain et ne peut donc pas être considérée comme une action indépendante.

4.2.2 Efficacité (ou capacité de réalisation)

C'est l'aptitude d'une barrière de sécurité à remplir la fonction de sécurité pour laquelle elle a été choisie, dans son contexte d'utilisation, pendant une durée donnée de fonctionnement.

L'efficacité est à considérer par rapport à tous les éléments composant la BHS.

Par analogie avec les BTS, l'évaluation de l'efficacité repose sur l'adaptation des principes de :

- dimensionnement adapté,
- résistance aux contraintes spécifiques.

4.2.2.1 Principe de dimensionnement adapté

La composante humaine des BHS répond au principe de dimensionnement adapté :

- **si la tâche de sécurité, telle qu'elle est prévue, permet de remplir l'objectif de sécurité visé dans le contexte du scénario,**
- **si les besoins en connaissances de l'opérateur liés à la réalisation de la tâche de sécurité ont été identifiés et pourvus (connaissance des enjeux de sécurité relatifs à la tâche à effectuer et aux conditions de sa réalisation, formation, compagnonnage, ...),**
- **si les besoins matériels de l'opérateur liés à la réalisation de la tâche de sécurité ont été identifiés et pourvus (outils d'aide, documentation, procédures, ... etc.) de sorte que la tâche de sécurité permette de remplir l'objectif de sécurité visé dans le contexte du scénario.**

Le recueil d'informations à partir des réponses aux questions suivantes (liste non exhaustive) permet de justifier des moyens prévus et d'évaluer le dimensionnement adapté de la barrière vis-à-vis de la fonction de sécurité à assurer :

- L'opérateur a-t-il suffisamment conscience des enjeux de sécurité liés à la tâche à réaliser ? A-t-il conscience des phénomènes dangereux susceptibles d'être générés et des dangers encourus pour sa personne ?
- Les compétences nécessaires pour effectuer la tâche ont-elles été identifiées ? Quels sont les moyens de formation mis en œuvre pour répondre à ces besoins : formation initiale, compagnonnage, entraînements, ...etc.
Selon la nature des tâches à effectuer ainsi que leur fréquence d'exécution, il peut être nécessaire d'avoir des entraînements ou des recyclages réguliers. L'entraînement doit être réalisé dans les conditions les plus proches des conditions réelles.

- Est-ce qu'une documentation (procédure, check-list, logigramme, abaque, ...etc) est nécessaire pour aider l'opérateur dans sa tâche ? Si oui, est-elle prévue ? Est-elle mise à jour suffisamment régulièrement ? Est-elle à disposition de l'opérateur ?
- Les outils nécessaires pour effectuer la tâche sont-ils prévus ? Sont-ils à disposition de l'opérateur ?
- Existe-t-il un retour d'expérience de mise en œuvre de la barrière, en situation réelle ou dans des conditions proches des conditions réelles ?
L'exploitation du retour d'expérience (confrontation des expériences de divers opérateurs, exercices, audits, ...) peut permettre de justifier dans une certaine mesure de la bonne conception et du bon dimensionnement de la tâche.

4.2.2.2 Principe de résistance aux contraintes spécifiques

La composante humaine des BHS répond au **principe de la résistance aux contraintes spécifiques si les contraintes liées au contexte d'utilisation de la barrière (contraintes liées à l'environnement, à l'exploitation, aux produits mis en œuvre, ...) ne remettent pas en question le fonctionnement des éléments constitutifs de la barrière.**

L'objectif est de vérifier que les contraintes liées au contexte d'utilisation de la barrière ne remettent pas en cause la capacité de l'opérateur à assurer sa tâche de sécurité. Il s'agit en particulier de s'assurer que les acteurs devant réaliser les actions de sécurité seront protégés du contexte accidentel du scénario.

Liste (non exhaustive) de questions pour répondre au principe de résistance aux contraintes spécifiques :

- Les équipements de protection individuels sont-ils adaptés pour protéger l'opérateur devant intervenir ?
- Les moyens d'intervention sont-ils conçus et positionnés de manière à ne pas exposer l'opérateur qui devra les actionner ?

4.2.3 Temps de réponse

C'est l'intervalle de temps entre le moment où une barrière de sécurité, dans un contexte d'utilisation, est sollicitée ou activée et le moment où la fonction de sécurité assurée par cette barrière de sécurité est réalisée dans son intégralité.

Cette définition implique que le temps de réponse intègre :

- le temps nécessaire à la détection de l'incident ou de l'information recherchée (comprenant le cas échéant le temps nécessaire à cette recherche),
- le temps nécessaire au diagnostic permettant le choix de l'action de sécurité assurant la fonction de sécurité,
- le temps nécessaire à la réalisation de l'action de sécurité.

Pour qu'une barrière humaine de sécurité soit retenue, son temps de réponse doit être en adéquation avec la cinétique du phénomène qu'elle doit maîtriser.

Ce critère peut également être sans objet dans le cas de certains types de barrières : notamment les tâches consistant à vérifier que les conditions prévues pour opérer l'installation en sécurité sont réunies. Dans ce cas, la seule exigence temporelle sur l'action de vérification est qu'elle ait bien lieu avant d'opérer l'installation.

Le temps de réponse est obtenu en prenant en compte l'ensemble des étapes élémentaires nécessaires à la réalisation de la tâche de sécurité.

Par exemple, le temps de réponse intègre :

- Dans le cas de rondes : le laps de temps maximal entre le démarrage potentiel du feu et le moment où le rondier pourra détecter ce feu. Si la ronde est effectuée toutes les deux heures, le temps maximal de détection pourra donc être de deux heures, temps à ajouter au temps nécessaire pour, par exemple, se déplacer jusqu'au poste de commande et déclencher l'alerte et le démarrage des moyens incendie, ainsi que le temps de montée en puissance des moyens de protection incendie.
- Dans le cas où l'opérateur doit se protéger pour intervenir : le temps nécessaire pour revêtir les équipements individuels de protection (combinaison, appareil de respiration individuel, ...).

Il est à noter que le temps de réponse défini précédemment n'intègre pas le temps nécessaire pour que le flux de danger (par exemple un incendie) atteigne le moyen (technique ou humain) de détection. Par exemple, si la détection est olfactive, le temps entre le début de la fuite et le moment où l'odeur parvient à l'opérateur n'est pas inclus.

On notera que l'évaluation du temps de réponse doit être conservatrice de manière à prendre en compte un certain nombre de facteurs aggravants comme le stress, la disponibilité non optimale des ressources,...etc. Elle doit également être conservatrice afin de prendre en compte les marges de manœuvres nécessaires aux opérateurs pour faire face à ces aléas et sources de stress.

La réalisation d'exercices (cas d'intervention incendie par exemple) et l'exploitation du retour d'expérience sur ces mises en situation accidentelle (observation, chronométrage, analyse des aléas, ...) sont ainsi vivement recommandées.

4.3 EVALUATION DE LA PERFORMANCE DES BARRIERES HUMAINES DE SECURITE : NIVEAU DE CONFIANCE (NC)

La méthode proposée postule que le niveau de confiance optimal d'une barrière est de 2 ($10^{-2} \geq \text{PFD} \geq 10^{-3}$) et que ce niveau décroît du moment que les exigences liées aux trois sous-fonctions (obtention de l'information, traitement permettant le choix de l'action et réalisation de l'action) composant la fonction de sécurité assurée par la barrière sont partiellement ou non satisfaites.

La méthode requiert **l'examen de trois tableaux** (un tableau par sous-fonction) puis **l'examen de conditions minimales de prise en compte de la BHS lorsqu'elle fait intervenir plusieurs acteurs.**

Le niveau de confiance retenu pour la barrière humaine de sécurité correspond à la différence entre le niveau de confiance optimal (2) et la somme des décotes sur les trois tableaux correspondant à chacune des sous-fonctions. Il sera nul si les conditions minimales à prendre en compte ne sont pas respectées.

Les paragraphes qui suivent présentent des tableaux indicatifs pour évaluer le niveau de décote adéquat. Pour chaque sous-fonction, les tableaux indiquent deux types d'exigences à remplir pour assurer un niveau de performance optimal. De manière pratique, l'application de ces tableaux se fait de la façon suivante :

- On obtient une décote nulle à condition que chacune des deux exigences pour le succès de la tâche soient satisfaites.
- On obtient une décote intermédiaire (-1) lorsqu'au moins une des deux exigences pour le succès de la tâche n'est que moyennement satisfaite.
- On obtient une décote maximale (-2) dès lors qu'une des deux exigences pour le succès de la tâche n'est pas satisfaite

Nous rappelons que le choix d'une décote est réalisé sur la base d'un **jugement qualitatif construit par les personnes du groupe de travail** participant à l'évaluation de la performance de la barrière. Le choix de la décote s'appuie en particulier **sur l'identification qui aura été faite des facteurs d'aide ou des facteurs perturbateurs déterminants vis-à-vis de la réussite de la tâche de sécurité évaluée.**

4.3.1 Première sous-fonction : obtention de l'information

Dans le cadre de cette première sous-fonction, l'activité de l'opérateur peut être de nature différente. Deux cas se présentent :

- L'opérateur a un rôle « passif » : l'opérateur est alerté ou sollicité par l'arrivée d'une information fortuite (alarme prévue, phénomène physique, ...); l'arrivée de l'information peut venir interrompre l'activité en cours.

- L'opérateur a un rôle « actif » : il doit s'engager dans une activité planifiée (par exemple une phase de surveillance, une ronde, ...) de prévention des risques dont la finalité est l'obtention d'une ou plusieurs informations lui permettant de détecter des anomalies ou une dérive du procédé. Le terme "information" a une connotation assez large, il englobe notamment la valeur d'un paramètre de fonctionnement, une mesure physique, la caractérisation d'un état (étanche ou non étanche, vanne fermée ou non, tenue ou non en pression...), ...etc.

4.3.1.1 "Détection passive"

Décote	Caractéristiques de la situation de travail
0	<p><u>Information clairement perceptible et identifiable :</u> Information disponible de façon hiérarchisée (par exemple : alarme dédiée visuelle et sonore clairement distincte des autres types d'alarmes) donnant l'état du système, quelles que soient les conditions environnementales (nuit, brouillard, ...) qui seraient susceptibles d'empêcher ou de gêner la perception de ces informations.</p> <p><u>ET</u> <u>Totale disponibilité de l'opérateur :</u> L'opérateur est présent à l'endroit où l'information est disponible et il peut interrompre toute autre activité en cours. Les conditions de travail sont favorables au maintien d'un bon niveau de vigilance.</p>
- 1	<p><u>Information perceptible et identifiable avec une difficulté modérée :</u> Information disponible de façon non hiérarchisée au milieu d'un nombre limité d'autres informations,</p> <p><u>ET/OU</u> <u>Disponibilité de l'opérateur :</u> L'opérateur est présent à l'endroit où l'information est disponible et il peut être amené à gérer un nombre acceptable d'autres tâches en même temps sans remise en cause de ses capacités de perception.</p>
- 2	<p><u>Information difficilement perceptible et identifiable :</u> Information noyée parmi d'autres informations, ou information difficilement détectable (localisation des informations non adaptée à l'activité de l'opérateur, perception pouvant s'avérer difficile, notamment dans certaines conditions environnementales ou dans le cadre du déroulement du scénario).</p> <p><u>OU</u> <u>Faible disponibilité de l'opérateur :</u> L'opérateur est rarement présent à l'endroit où l'information est disponible ou il est présent de façon aléatoire non prévisible ou il peut être amené à gérer un nombre important de tâches en même temps.</p>

Tableau 3 : Estimation du niveau de confiance sur la sous-fonction d'obtention de l'information (cas de "détection passive")

4.3.1.2 "Détection active"

Décote	Caractéristiques de la situation de travail
0	<p><u>Facilité d'obtention de la/des information(s) recherchée(s) :</u> Identification ou obtention de l'information simple (information clairement identifiable, pas de confusion possible, ...) par rapport au niveau de compétence attendu de l'opérateur et conditions de travail jugées non contraignantes (conditions environnementales favorables, bonne accessibilité à l'information...).</p> <p><u>ET</u> <u>Totale disponibilité et engagement de l'opérateur :</u> Cette tâche est une activité planifiée, bien dimensionnée dans le plan de charge de l'opérateur, et perçue comme prioritaire¹⁰ par l'opérateur. Celui-ci dispose d'une marge de manœuvre suffisante pour faire face à d'éventuels aléas sans compromettre la réalisation de la tâche dans les conditions requises.</p>
- 1	<p><u>Conditions d'obtention de la/des information(s) recherchée(s) moyennement aisées :</u> Identification ou obtention de l'information réalisée avec un effort (intellectuel et/ou physique) acceptable par rapport au niveau de compétence attendu de l'opérateur et aux conditions d'accès à l'information.</p> <p><u>ET/OU</u> <u>Disponibilité et engagement de l'opérateur :</u> Cette tâche est une activité planifiée et dimensionnée dans le plan de charge de l'opérateur, et perçue comme importante par l'opérateur. Celui-ci dispose d'une marge de manœuvre plus réduite pour faire face à d'éventuels aléas.</p>
- 2	<p><u>Impossibilité ou difficulté d'obtention de la/des information(s) recherchée(s) :</u> Identification ou obtention de l'information difficilement réalisable ou réalisée avec un effort (intellectuel et/ou physique) important ou conditions de travail jugées fortement contraignantes (accessibilité à l'information très difficile, forte pénibilité de l'activité, ...).</p> <p><u>OU</u> <u>Faible disponibilité et engagement de l'opérateur :</u> Cette tâche n'est pas prévue ou n'est pas correctement dimensionnée dans le plan de charge de l'opérateur ou cette tâche peut être perçue comme moins prioritaire vis-à-vis d'autres contraintes d'exploitation.</p>

Tableau 4: Estimation du niveau de confiance sur la sous-fonction d'obtention de l'information (cas de "détection active")

¹⁰ La priorité que l'opérateur peut donner à la tâche de sécurité doit s'évaluer dans le contexte plus général de l'activité globale de l'opérateur. Les ressources disponibles n'étant pas infinies et la tâche de sécurité n'étant qu'une partie du travail de l'opérateur, celui-ci peut être amené, en fonction des aléas ou imprévus, à réviser, ponctuellement ou plus durablement, la planification ou la priorité de certaines de ses tâches. Dès lors, le non-accomplissement de la tâche de sécurité tel que prévu peut avoir de multiples explications. On pourra porter attention en particulier :

- Aux conditions de travail de l'opérateur (tâches routinières, mauvaises conditions environnementales, isolement, travail très physique ou difficultés d'accès au poste de travail, ...etc) : l'intégration de l'ergonomie lors de la conception et de la modification des postes ou conditions de travail permet à l'opérateur d'optimiser l'utilisation de ses ressources et limite le risque de reports successifs de certaines tâches voire leur négligence progressive.
- Au sens que peut donner l'opérateur à cette tâche de sécurité : par exemple, si les rondes n'ont pas jusqu'à présent révélé de défaillance ou si la culture de sécurité est faible, l'opérateur peut acquérir progressivement le sentiment voire la conviction de « l'inutilité » de la tâche. La pratique de contrôles de la réalisation de cette tâche (visite impromptue, contrôle par échantillonnage, enregistrement des actions, surveillance instrumentée, ...) peut aider à maintenir l'attention sur l'importance de la tâche au plan de la sécurité.

4.3.2 Deuxième sous-fonction : diagnostic permettant le choix de l'action à réaliser

Décote	Caractéristiques de la situation de travail
0	<p><u>Bonne qualité et accessibilité des informations utiles au diagnostic :</u> Présentation explicite et niveau suffisant d'informations : informations directes non sujettes à interprétation sur l'état du système (et la localisation de l'accident), de l'incident ou du défaut (respect des conventions de présentation des informations, le cas des indicateurs défaillants est signalé, ...etc.). L'opérateur dispose si nécessaire d'un délai confortable pour prendre du recul sur la qualité et le niveau d'information utile, et approfondir le diagnostic.</p> <p><u>ET</u> <u>Niveau de guidage adapté à la situation :</u> L'usage de procédure n'est pas nécessaire ou, dans le cas contraire, la décision est guidée par des procédures explicites (instruction claire et explicitation des conséquences de l'action sur le système) ou aide contextuelle fournie par le système (sur le système de conduite, signalisation à proximité des dispositifs de signalisation ou des organes de commande ...) permettant de déterminer facilement l'action à réaliser.</p>
- 1	<p><u>Qualité acceptable des informations utiles au diagnostic :</u> Présentation des informations non directement utilisables pour faire le diagnostic mais des modalités de traitement sont prévues pour obtenir les informations utiles au diagnostic mais qui peuvent parfois être source d'erreur (certains types de calculs, conversion d'unité, ...)</p> <p>Ou niveau d'informations pas toujours suffisant mais il est possible d'approfondir le diagnostic par la recherche d'informations complémentaires (l'opérateur dispose alors d'un délai raisonnable pour prendre du recul et collecter les informations nécessaires)</p> <p><u>ET/OU</u> <u>Guidage prévu mais parfois insuffisant :</u> Un certain niveau de guidage est nécessaire : les règles générales à appliquer sont connues ou formalisées mais un certain niveau d'interprétation des règles est nécessaire pour décider de la conduite à tenir (par exemple, les procédures traitent de nombreux cas connus mais une réflexion reste nécessaire pour décider).</p>
-2	<p><u>Qualité insuffisante des informations utiles au diagnostic :</u> Informations insuffisamment explicites (ambigües, ou demandant des calculs complexes, des croisements de données, ou une réflexion mobilisant des connaissances non familières).</p> <p>Ou niveau d'informations insuffisant pour identifier le problème ou l'état du système, l'approfondissement du diagnostic est difficilement envisageable compte-tenu du contexte ou de l'organisation du travail (temps disponible insuffisant, isolement géographique, ...).</p> <p><u>OU</u> <u>Guidage insuffisant :</u> Application des règles difficilement envisageable compte-tenu de la situation : règle très générale ou trop précise qui demande des adaptations quasi-systématiques, ou nombre trop important de choix d'actions possibles, la prise de recul ou la sollicitation d'un avis extérieur étant difficile (ressources temporelles nécessaires insuffisantes par rapport au déroulement du scénario ou recours à un tiers non prévu dans l'organisation du travail).</p>

Tableau 5 Estimation du niveau de confiance sur la sous-fonction de traitement de l'information permettant le choix de l'action à réaliser

4.3.3 Troisième sous-fonction : action de sécurité à réaliser

Décote	Caractéristiques de la situation de travail
0	<p><u>Niveau de stress acceptable :</u> Ressources nécessaires à la réalisation de l'action jugées suffisantes : absence de pression temporelle ou temps d'intervention largement inférieur à la cinétique de l'accident, pas d'exposition au danger, expérience significative de la situation, feedback suffisant sur l'action engagée,...</p> <p><u>ET</u> <u>Tâche simple et peu exigeante :</u> Nombre d'actions limité, sans enchaînement complexe (par exemple : fermer plusieurs vannes sans notion d'ordre), système robuste aux erreurs (détrompeur, temporisation, codes couleurs ou symboles évitant le risque de confusion,...) ou permettant d'alerter l'opérateur pour lui donner la possibilité de revenir en arrière. Les moyens d'actions étant facilement accessibles et facilement manœuvrables.</p>
- 1	<p><u>Niveau de stress possible mais tolérable :</u> Ressources nécessaires à la réalisation de l'action jugées pouvant s'avérer insuffisantes, notamment dans certaines conditions difficiles (peu de marge temporelle, exposition au danger, ...)</p> <p><u>ET/OU</u> <u>Tâche moyennement exigeante ou difficile :</u> Nombre d'actions limité mais niveau d'exigence plus élevé : efforts importants de mémorisation ou de concentration, enchaînements stricts à respecter (par exemple : arrêter la pompe P1 puis seulement après, fermer la vanne V1 et ensuite la vanne V2. Modifier l'ordre de ces actions entraînerait un accident) mais le système permet à l'opérateur de revenir en arrière. Ou les moyens d'actions peuvent être moyennement accessibles et manœuvrables.</p>
- 2	<p><u>Niveau de stress important :</u> Fort ressenti de pression : ressources nécessaires à la réalisation de l'action jugés inadaptées par rapport aux objectifs à atteindre (temps jugé insuffisant, exposition au danger, effet de panique, ...).</p> <p><u>OU</u> <u>Tâche très exigeante, difficile ou impossible :</u> Niveau d'exigence trop élevé (nombre d'actions important avec enchaînements stricts, impossibilité d'interrompre les effets d'une action engagée par erreur, ...) et/ou accessibilité ou manœuvrabilité difficile ou impossible des moyens d'action.</p>

Tableau 6 : Estimation du niveau de confiance sur la sous-fonction de réalisation de l'action de sécurité

4.3.4 Condition de décote complète de la barrière : Cas de la barrière humaine de sécurité faisant intervenir plusieurs acteurs

Il est nécessaire dans ce cas de s'assurer que les rôles et les responsabilités des différents acteurs sont clairement établis et connus de leur part, que les informations transmises sont sans ambiguïté (désignation des équipements, des dispositifs, de l'action de sécurité...) et que les outils de communication sont clairement identifiés et performants.

Dans le cas contraire la barrière humaine de sécurité ne sera pas retenue (NC=0).

4.4 APPLICATION AU CAS DES BARRIERES MIXTES A COMPOSANTES TECHNIQUES ET HUMAINES : LES SAMS

Comme indiqué au paragraphe 2.1.1, une barrière humaine de sécurité peut inclure un dispositif technique de sécurité.

Dans ce cas, il conviendra d'évaluer séparément chacune des composantes¹¹ selon le principe d'indépendance et les critères de capacité de réalisation, de temps de réponse et de niveau de confiance.

Puis, l'évaluation de la barrière de sécurité englobant les composantes humaine et technique suit les principes suivants :

- L'indépendance de la barrière est assurée si chacune des composantes est indépendante.
- L'efficacité globale de la barrière sera évaluée en référence à la fonction de sécurité assurée par l'ensemble des composantes techniques et humaines constituant la barrière.
- Le temps de réponse global sera la somme des temps de réponse de chacune des composantes.
- Le niveau de confiance retenu pour la barrière sera le minimum des niveaux de confiance de chaque composante.

¹¹ Pour la composante technique, le lecteur pourra s'appuyer utilement sur le rapport Q10 "Evaluation des dispositifs de prévention et de protection utilisés pour réduire les risques d'accidents majeurs".

5. AGREGATION DES BARRIERES HUMAINES DE SECURITE

Dans le cadre de la démonstration de la maîtrise des risques sur un scénario, on peut être amené à évaluer les performances de chacune des barrières agissant sur le scénario pour évaluer le niveau de réduction des risques apporté par l'ensemble des mesures de maîtrise des risques sur ce scénario. Dans ce cas précis, on peut être amené à vouloir agréger plusieurs barrières humaines de sécurité entre elles en additionnant les niveaux de confiance de chacune des barrières.

5.1 EXAMEN DE L'EXISTENCE DE MODE COMMUN DE DEFAILLANCE ENTRE LES BHS A AGREGER

Pour agréger sur un même scénario plusieurs barrières humaines de sécurité, il faut s'assurer que les barrières sont bien **indépendantes entre elles**.

Il conviendra donc d'examiner l'existence de mode commun de défaillance entre les BHS qu'on souhaite agréger : par exemple, lorsque les deux BHS ont un **même élément technique** (même vanne à actionner dans les deux barrières ou même moyen de communication) **ou humain** (même opérateur en charge des deux barrières). Si c'est le cas et si ces deux barrières assurent la même fonction de sécurité, on ne pourra retenir le niveau de confiance que d'une seule de ces barrières (celle dont le niveau de confiance est le plus faible).

En l'absence de mode commun de défaillance entre les BHS qu'on souhaite agréger, on pourra sommer les niveaux de confiance des barrières entre elles. Ceci équivaut à considérer la performance des barrières indépendamment les unes des autres. Toutefois, **il faudra s'assurer que le temps de réponse global est bien évalué en prenant en compte l'ensemble des barrières de sécurité agissant sur le scénario et que ce dernier est en adéquation avec la cinétique du scénario**.

Notamment dans le cas où deux barrières interviendraient au cours de la séquence accidentelle, la seconde barrière sera sollicitée en cas d'échec de la première, les temps de réponse des deux barrières vont donc s'additionner ; la seconde barrière ne sera performante que si ce temps total est compatible avec la cinétique de l'accident.

Nota : Une exception à ce principe peut être faite dans le cas où l'élément commun serait un opérateur en charge à la fois :

- d'une barrière qui intervient en amont de la séquence accidentelle en préalable à l'activité à risque (cas de la barrière de vérification),
- et d'une barrière qui intervient en rattrapage d'une séquence accidentelle déjà initiée (cas de la barrière de rattrapage).

Dans ce cas, les activités concernées par les deux barrières sont bien distinctes de par leur position dans la séquence accidentelle : l'addition des niveaux de confiance des deux barrières est possible à la condition qu'il n'y ait pas d'autre mode commun de défaillance.

5.2 CAS PARTICULIER DE L'AGREGATION SUR UN SCENARIO D'ACCIDENT DE BARRIERES HUMAINES DE SECURITE ASSURANT LA MEME FONCTION DE SECURITE

Pour les barrières agissant en préalable à l'activité à risques, étant entendu qu'il n'existe pas de pression temporelle par rapport à la cinétique d'un scénario, il est possible de considérer une capacité de rattrapage par la mise en œuvre d'une étape de vérification supplémentaire.

Exemple : Le démarrage d'une réaction chimique est conditionné par le pH d'un milieu réactionnel ; ce pH est contrôlé une première fois par l'opérateur de production puis par le laboratoire de l'entreprise.

La mise en œuvre d'une opération de test ou de contrôle supplémentaire est considérée comme susceptible d'augmenter le niveau de confiance de l'activité d'un niveau au maximum, le niveau de confiance maximal associé à la fonction de sécurité assurée étant alors de 3. Dans ce cas, et de façon prudente, les niveaux de confiance ne sont pas sommés pour prendre en compte la possibilité de défaillance de mode commun (par exemple : arrangements informels entre opérateurs découlant d'une confiance mutuelle).

6. GLOSSAIRE & DÉFINITIONS

BHS	:	Barrière Humaine de Sécurité
BTS	:	Barrière Technique de Sécurité
ICPE	:	Installations Classées pour la Protection de l'Environnement
JRC	:	Joint Research Center- European Commission
MEDD	:	Ministère de l'Ecologie et du Développement Durable
NC	:	Niveau de Confiance
PFDD	:	Probability of Failure on Demand ou Probabilité moyenne de Défaillance sur Demande
POI	:	Plan d'Opérations Internes
PPR	:	Plan de Prévention des Risques
SAMS	:	Système à Action Manuelle de Sécurité
SGS	:	Système de Gestion de la Sécurité

DEFINITIONS :

L'INERIS propose ici des définitions des principaux termes techniques utilisés dans ce document. On notera que certaines des définitions suivantes sont issues du glossaire technique des risques technologiques publié par le MEDD.

Accident : Evénement non désiré, tel qu'une émission de substance toxique, un incendie ou une explosion résultant de développements incontrôlés survenus au cours de l'exploitation d'un établissement qui entraîne des conséquences/ dommages vis à vis des personnes, des biens ou de l'environnement et de l'entreprise en général. C'est la réalisation d'un phénomène dangereux, combinée à la présence de cibles vulnérables exposées aux effets de ce phénomène.

Accident majeur : « Evénement tel qu'une émission, un incendie ou une explosion d'importance majeure résultant de développements incontrôlés survenus au cours de l'exploitation d'un établissement, entraînant pour les intérêts visés à l'article L.511-1 du code de l'environnement, des conséquences graves, immédiates ou différées, et faisant intervenir une ou plusieurs substances ou des préparations dangereuses. » (Arrêté du 10 mai 2000 modifié)

Activité : L'activité correspond au travail réel : c'est ce que l'opérateur fait réellement lorsqu'il est confronté à une situation concrète. Deux composantes sont en jeu dans l'activité d'un individu (c'est à dire la réalisation effective de la tâche) : une composante physique qui comprend les gestes et postures et une composante mentale qui est relative au traitement de l'information et aux processus de pensée.

Barrière Humaine de Sécurité (BHS) : Les barrières humaines de sécurité sont constituées d'une activité humaine (une ou plusieurs opérations) qui s'oppose à l'enchaînement d'évènements susceptibles d'aboutir à un accident.

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'évènements susceptibles d'aboutir à un accident.

Efficacité : L'efficacité d'une barrière de sécurité 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 de sécurité.

Ergonomie : L'ergonomie est la discipline scientifique qui vise la compréhension fondamentale des interactions entre les humains et les autres composantes d'un système, et l'application de méthodes, de théories et de données pour améliorer le bien-être des personnes et la performance globale des systèmes. Les ergonomes contribuent à la conception et à l'évaluation des tâches, des emplois, des produits, des environnements et des systèmes en vue de les rendre compatibles avec les besoins, les capacités et les limites des personnes. (International Ergonomic Association, 2000)

L'ergonomie utilise des connaissances issues, entre autres, de la psychologie cognitive (mémoire, attention, perception, apprentissage...) et de la psychophysiology (vigilance, postures, conditions de travail...).

Événement initiateur : Événement, courant ou anormal, interne ou externe au système, situé en amont de l'événement redouté central dans l'enchaînement causal et qui constitue une cause directe dans les cas simples ou une combinaison d'événements à l'origine de cette cause directe. Dans la représentation en « nœud papillon » (ou arbre des causes), cet événement est situé à l'extrémité gauche.

Événement redouté central : Événement conventionnellement défini, dans le cadre d'une analyse de risque, au centre de l'enchaînement accidentel. Généralement, il s'agit d'une perte de confinement pour les fluides et d'une perte d'intégrité physique pour les solides. Les événements situés en amont sont conventionnellement appelés « phase pré-accidentelle » et les événements situés en aval « phase post-accidentelle ».

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 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.

Mesure de maîtrise des risques (ou mesure de sécurité ou barrière de sécurité) : Ensemble d'éléments techniques et/ou organisationnels nécessaires et suffisants pour assurer une fonction de sécurité.

Niveau de confiance : C'est une adaptation par l'INERIS des exigences des normes NF-EN 61508 [8] et NF-EN 61511[6], notamment quant aux architectures des systèmes pour tous les équipements de sécurité, quelle que soit leur technologie. Le terme niveau de confiance est conservé pour les mesures de maîtrise des risques activées ou assurées par l'homme.

Performance des barrières : L'évaluation de la performance se fait au travers de leur efficacité, de leur temps de réponse et de leur niveau de confiance au regard de leur architecture

Scénario d'accident (majeur) : Enchaînement d'événements conduisant d'un événement initiateur à un accident (majeur), dont la séquence et les liens logiques découlent de l'analyse de risque. En général, plusieurs scénarios peuvent mener à un même phénomène dangereux pouvant conduire à un accident (majeur) : on dénombre autant de scénarios qu'il existe de combinaisons possibles d'événements y aboutissant. Les scénarios d'accident obtenus dépendent du choix des méthodes d'analyse de risque utilisées et des éléments disponibles.

Systèmes à Actions Manuelles de Sécurité : Ils sont une combinaison d'une barrière technique de sécurité et d'une activité humaine pour mener à bien une fonction de sécurité (appui sur un bouton d'arrêt d'urgence, alarme débit bas suivie de la fermeture manuelle d'une vanne de sécurité...).

Tâche : La tâche est le résultat qui est plus ou moins explicitement attendu de l'individu dans des conditions imposées pour l'exécution (à distinguer de l'activité). La tâche correspond au travail prescrit.

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.

7. REFERENCES

- [1] N. Le, V. De Dianous, "Evaluation des dispositifs de prévention et de protection utilisés pour réduire les risques d'accidents majeurs" Ω10, Rapport d'étude n°DRA-08-95403-01561B, 01/09/2008 : INERIS pour le Ministère chargé de l'environnement, rapport disponible sur www.ineris.fr
- [2] E. Miché, F. Prats, S. Chaumette, Démarche d'évaluation des Barrières Humaines de Sécurité. Ω 20, Rapport d'étude n° 46055, 21/12/2006
- [3] Rasmussen J., Information Processing and Human-Machine Interaction, Amsterdam, North-Holland, 1986
- [4] Hollnagel E., Cognitive reliability and error analysis method : CREAM. Elsevier, 1998
- [5] Swain A.D., Guttman, H.E., Handbook of Human Reliability Analysis with emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, Washington, D.C. : US Nuclear Regulatory Commission, 1983
- [6] NF-EN 61511, parties 1 à 3 : Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur de l'industrie de process, mars 2005
- [7] Human Factors Reliability Benchmark Exercise, Reactor Safety Programme 1985-1987, Nuclear Science and Technology, Commission of the European Communities, August 1989 – EUR 12222 EN.
- [8] NF-EN 61508, parties 1 à 7 : Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité, mars 2002

8. LISTE DES ANNEXES

Repère	Désignation	Nombre de pages
Annexe A	Exemples d'application de l'ensemble de la démarche	12

ANNEXE A :

**EXEMPLES D'APPLICATION
DE L'ENSEMBLE DE LA DEMARCHE**

FICHE-EXEMPLE N°1 : TACHE DE VERIFICATION DE FERMETURE D'UNE VANNE DE FOND PREALABLEMENT AU REMPLISSAGE D'UN REACTEUR

Dans un atelier de fabrication de peinture, les mélanges sont réalisés par un opérateur dans un réacteur. La vanne de fond de réacteur (vanne quart de tour) est située au rez-de-chaussée et le chargement se fait au premier étage. Cette tâche est réalisée environ 1000 fois par an par le même opérateur. Une fois que le mélange est considéré comme satisfaisant, le réacteur est vidé via la vanne de fond. Puis le réacteur est nettoyé. A la fin des opérations de nettoyage, l'opérateur referme la vanne de fond du réacteur.

L'action de sécurité consiste à ce que l'opérateur vérifie que la vanne de fond est fermée avant de verser les produits dans le réacteur.

<i>Indépendance</i>	<p><i>Cette tâche pourra être considérée comme indépendante du moment que la vérification de la fermeture de la vanne est :</i></p> <ul style="list-style-type: none"> - <i>réalisée par une personne différente, cette personne donnant le feu vert à l'opérateur de chargement ("redondance organisationnelle"),</i> - <i>réalisée par le même opérateur, du moment que cette vérification est réalisée dans une séquence de travail différente ("redondance temporelle") :</i> <ol style="list-style-type: none"> a) <i>Si la vérification est directement accolée à l'opération de nettoyage, cette tâche ne peut pas être considérée comme indépendante.</i> b) <i>Si une autre opération est réalisée préalablement à cette vérification (par exemple : établissement des connexions nécessaires à la réalisation du prochain mélange, vérification de la qualité des matières premières pour le prochain mélange, ...) cette tâche peut être considérée comme indépendante.</i> <p><i>Dans cet exemple, on considérera que l'on est dans le ce dernier cas (b).</i></p>
<i>Efficacité</i>	<p><i>Personnel formé, tâche identifiée dans un mode opératoire.</i></p> <p><i>La tâche est essentiellement physique, tourner la vanne ne nécessite pas de force particulière ni d'outil</i></p>
<i>Temps de réponse</i>	<i>non concerné</i>
<i>NC</i>	<p><u><i>Détection "active" : l'opérateur doit aller vérifier la position de la vanne</i></u></p> <ol style="list-style-type: none"> 1. <i>L'information est facile à obtenir (la vanne de fond est située dans un atelier couvert et éclairé) d'autant plus qu'il s'agit d'une vanne 1/4 de tour (quand la vanne est en position fermée, l'actionneur est perpendiculaire à la canalisation). Cependant il peut y avoir un léger risque de confusion avec la vanne de fond d'un autre réacteur (en particulier compte-tenu des allers-retours entre les 2 étages).</i>

2. La tâche est bien prévue et dimensionnée dans le plan de charge de l'opérateur, et l'ensemble des tâches de l'opérateur est planifié (mode opératoire précis). Cependant, la nature de la tâche (tâche assez répétitive et présentant un certain caractère de pénibilité dû au trajet 1^{er} étage – rez-de-chaussée et retour à réaliser) peut être perçue comme assez contraignante par l'opérateur et affecter l'engagement de l'opérateur face à cette tâche.

*Conclusion partielle : le facteur 1, comme le facteur 2 justifie la **décote d'un niveau (-1)***

Diagnostic et choix de l'action :

1. L'opérateur a directement l'information sur l'état de la vanne (vanne 1/4 de tour)
2. La règle de choix d'action est connue (pas de procédure nécessaire sur le choix d'action)

Conclusion partielle : pas de décote

Action de sécurité :

1. Il n'y a pas de pression particulière liée au scénario d'accident redouté
2. La tâche est simple : si la vanne était ouverte, alors la fermer

Conclusion partielle : pas de décote

Activité impliquant plusieurs acteurs : sans objet

(Rappel : niveau de confiance maximal = 2)

Somme des décotes = 1

Niveau de confiance estimé = 2-1 = 1

FICHE-EXEMPLE N°2 : TACHE DE MESURE DE PH PREALABLEMENT AU DEMARRAGE DE LA REACTION

La réaction est catalysée en milieu acide et le pH doit être compris dans une plage de sécurité pour minimiser les risques d'emballement thermique. Le pHmètre est étalonné tous les jours.

Cette vérification est réalisée sur un échantillon prélevé dans le réacteur de synthèse avant la mise en chauffe du réacteur. Les opérateurs sont postés. Un opérateur réalise entre 150 à 200 synthèses de ce type par an. L'atelier comporte cinq réacteurs de synthèse pouvant être opérés en même temps.

L'action de sécurité consiste à mesurer le pH du milieu réactionnel et ne démarrer la réaction (mise en chauffe du réacteur) que si le pH est dans la plage de sécurité. La consigne de travail précise qu'en cas de pH hors plage de sécurité, la conduite à tenir est d'évacuer le contenu du réacteur après accord du chef de quart

<i>Indépendance</i>	<i>Oui : ce contrôle constitue la condition pour le démarrage de la synthèse, la tâche est réalisée dans une séquence de travail distincte du démarrage ("redondance temporelle")</i>
<i>Efficacité</i>	<i>Personnel formé, tâche identifiée dans feuille de marche. Mesure réalisée sur un échantillon prélevé dans le milieu réactionnel. Le pHmètre est étalonné une fois par poste (enregistré sur le cahier d'étalonnage)</i>
<i>Temps de réponse</i>	<i>non concerné</i>
NC	<p><u>Détection "active" : l'opérateur doit aller prélever un échantillon et effectuer une mesure de pH</u></p> <ol style="list-style-type: none"> 1. <i>L'information est facile à obtenir (l'atelier est couvert, le prélèvement de réactif ne pose pas de problème, la mesure de pH se fait dans un laboratoire dédié à l'atelier et situé à l'étage des réacteurs, l'opérateur est compétent pour effectuer la mesure de pH).</i> 2. <i>La tâche est bien prévue et dimensionnée dans le plan de charge de l'opérateur, et l'ensemble des tâches de l'opérateur est planifié (mode opératoire précis) cependant l'opérateur peut manquer de disponibilité : il a plusieurs réacteurs à gérer et il peut être pressé par les autres tâches à réaliser</i> <p><i>Conclusion partielle : le facteur 2 justifie la décote d'un niveau (-1)</i></p> <p><u>Diagnostic et choix de l'action :</u></p> <ol style="list-style-type: none"> 1. <i>Une fois que le pH est mesuré, l'opérateur n'a plus qu'à comparer le pH avec la plage de tolérance inscrite sur la feuille de marche</i> 2. <i>Le choix d'action est clairement déterminé dans l'instruction : le contenu du réacteur doit être évacué après validation du chef de quart</i> <p><i>Conclusion partielle : pas de décote</i></p>

Action de sécurité :

1. La pression liée au scénario d'accident redouté est maîtrisée tant que le réacteur n'est pas redémarré : des situations analogues ont pu être vécues par l'opérateur
2. La tâche est simple : l'action consiste à ne pas démarrer la réaction (et avertir le chef de quart). Il est seul à gérer les réactions donc il n'y a pas de possibilité que quelqu'un d'autre que lui démarre la réaction.

Conclusion partielle : pas de décote

Activité impliquant plusieurs acteurs :

Pendant chaque poste, il n'y a qu'une personne qui est assignée à cette tâche. Toutefois, du fait de changement de poste et que le contrôle de pH peut avoir eu lieu à la fin d'un poste, il se peut que l'opérateur suivant n'ait pas connaissance du résultat de la mesure du pH et ainsi démarrer une réaction dans de mauvaises conditions. Pour pallier à cela, il est prévu une période de recouvrement et la transmission des informations sur la base d'un cahier de consignes.

(Rappel : niveau de confiance maximal = 2)

Somme des décotes = 1

Niveau de confiance estimé = 2-1 = 1

FICHE-EXEMPLE N°3 : EXTINCTION D'UN INCENDIE PAR UN RONDIER

Une installation de stockage d'hydrocarbure liquide est constituée :

- d'une cuve sur rétention,
- d'une installation de diffusion d'émulseur à action manuelle installée en périphérie de la cuvette de rétention,
- d'un mur coupe-feu de degré 2 h qui protège un réservoir de gaz liquéfié implanté à proximité.

On cherche à estimer le niveau de confiance de la tâche d'extinction d'un incendie d'hydrocarbure par un rondier sachant qu'une ronde est réalisée toutes les 1h30. L'objectif est de prévenir le BLEVE des réservoirs de gaz liquéfié.

<i>Indépendance</i>	<i>La tâche de surveillance est indépendante d'un quelconque scénario de fuite</i>
<i>Efficacité</i>	<p><i>Le circuit de ronde est réalisable, un feu de nappe dans la cuve de rétention sera bien visible à condition que le circuit de ronde soit respecté, le système d'extinction est dimensionné pour répondre au scénario d'incendie.</i></p> <p><i>Rondier formé et entraîné.</i></p> <p><i>Le bouton d'extinction reste bien accessible et protégé en cas d'incendie.</i></p>
<i>Temps de réponse attendu</i>	<i>Le délai maximal d'intervention est de 2 heures (après ce temps le mur coupe-feu est supposé inopérant).</i>
<i>Temps de réponse estimé</i>	<p><i>Le temps de réponse intègre le temps nécessaire à la réalisation de la ronde et de la mise en fonctionnement du système d'extinction. Le rondier passe toutes les 1h30 au même endroit et la mise route des moyens d'extinction lui prend quelques minutes.</i></p> <p><i>Le temps de réponse est du même ordre que la cinétique de l'accident.</i></p>
NC	<p><u><i>Détection "active" : le rondier doit aller chercher l'information en se rendant au bord de la cuvette</i></u></p> <ol style="list-style-type: none"> <i>1. La détection de l'incendie lors de la ronde de surveillance est claire (détection visuelle de flammes et de fumées).</i> <i>2. La ronde est la tâche principale du rondier et la périodicité de la ronde est définie comme impérative (1h30 soit env. 5 rondes par poste). Cependant le rondier est aussi affecté à d'autres tâches : compte-tenu des ces conditions générales et de l'organisation du travail, il est considéré qu'il existe un risque (modéré) de dérive ou de report de la ronde (impactant également sur la régularité des rondes)</i> <p><i>Conclusion partielle : décote d'un niveau (-1)</i></p>

	<p><u>Diagnostic et choix de l'action :</u></p> <ol style="list-style-type: none"> 1. La manifestation de l'information à traiter est suffisamment explicite (le phénomène dangereux lui-même) et suffit à diagnostiquer le problème. 2. L'opérateur connaît la signification de l'événement et maîtrise la conduite à tenir (mise en route du système d'extinction : ce pour quoi il est formé). <p>Conclusion partielle : pas de décote.</p> <p><u>Action de sécurité :</u></p> <ol style="list-style-type: none"> 1. Le temps de réponse est légèrement inférieur (env. 1h35) par rapport au temps de réponse maximal attendu (2h) ce qui induit une certaine pression (temporelle et liée au phénomène dangereux pouvant être très développé). 2. La tâche de mise en œuvre de l'extinction ne présente pas de complexité, le rondier est formé et régulièrement entraîné à ce type d'interventions. <p>Conclusion partielle : Le niveau de stress occasionné par le manque de temps notamment justifie une décote partielle de cette barrière (-1).</p> <p><u>Activité impliquant plusieurs acteurs :</u> sans objet</p> <p>(Rappel : niveau de confiance maximal = 2)</p> <p>Somme des décotes = 2</p> <p>Niveau de confiance estimé = 2-2 = 0</p>
Commentaires	<p>L'industriel a intégré dans la ronde un point de passage obligé au niveau de l'astreinte d'intervention avec indication de l'heure de passage sur un registre. D'autre part, l'organisation du travail du rondier a été modifiée de manière à ce que les autres tâches qui lui sont affectées soient réduites. Des dispositions sont prises pour que le rondier puisse disposer de l'autonomie suffisante pour réaliser prioritairement la ronde en toute situation. Un rappel concernant l'importance du respect de la périodicité de la ronde est fait régulièrement. Le groupe de travail estime que compte-tenu de l'ensemble de ces dispositions, la disponibilité et l'engagement du rondier est suffisant. Le NC peut alors être porté à 1.</p>

FICHE-EXEMPLE N°4 : NOYAGE D'UN REACTEUR EN CAS D'EMBALLLEMENT DE REACTION

Description des installations

On suppose un atelier de synthèses chimiques sur deux étages :

Le deuxième étage est dédié à la préparation des réactifs préalablement à l'introduction dans les réacteurs de synthèse. Les cuves de préparation des réactifs sont utilisées pour les différents réacteurs de synthèse de l'atelier. Le choix du réacteur de destination s'effectue par un jeu de vannes. Le dispositif de noyage de la réaction est situé à cet étage.

Le premier étage accueille les réacteurs de synthèses (au nombre de 4).

Le rez-de-chaussée est affecté à la mise en fûts des produits de réaction.

L'ensemble des transferts entre les étages se fait de façon gravitaire.

Un réacteur type de synthèse est équipé pour l'exploitation :

- d'un agitateur entraîné par un moteur électrique,
- d'un dispositif de chauffage séparé,
- d'un dispositif de refroidissement séparé,
- d'une mesure de la température,
- d'une mesure de la pression.

Un réacteur type de synthèse est équipé pour la sécurité :

- d'une mesure de la température,
- d'une mesure de la pression,
- d'un dispositif de noyage du réacteur (cuve remplie d'une quantité d'eau suffisante pour arrêter un emballement thermique). Cette cuve est équipée en pied de la vanne d'ouverture du circuit vers le réacteur,
- d'un disque de rupture permettant l'envoi des gaz de réaction en cheminée.

Nota : Cette description, relativement succincte, correspond à un cas pédagogique et à ce titre n'expose pas l'ensemble des dispositifs susceptibles d'être rencontrés sur un réacteur industriel.

Description des opérations de synthèse

Après avoir réalisé le chargement et la mise en chauffe du réacteur, l'opérateur est affecté à :

- la conduite et la surveillance du déroulement de la synthèse suivant les conditions définies dans la feuille de marche,
- l'arrêt de la synthèse et le coulage des produits de réaction vers la mise en fûts.

La conduite des opérations de synthèse est assurée par un opérateur posté. L'atelier fonctionne 24h/24. Un opérateur réalise entre 150 et 200 synthèses par an. L'atelier comporte quatre réacteurs de synthèse pouvant être opérés en même temps.

Barrière humaine de sécurité vis-à-vis du scénario d'emballement de réaction :

L'opérateur doit procéder au noyage de la réaction sur atteinte :

- d'un seuil de vitesse de montée en température de 1°C/min,
- d'un seuil de température haute,
- d'un seuil de pression haute.

Pour les besoins de cet exemple deux cas de conduite de la synthèse seront étudiés :

- Conduite et surveillance par lecture des capteurs de température et de pression sur le réacteur. Pour la lecture de la température l'opérateur dispose d'un écran permettant la visualisation de la courbe de température en fonction du temps,
- Conduite et surveillance à l'aide d'un système de supervision reporté en salle de contrôle. Les différents modes de représentation nécessaires au suivi des réactions sont reportés sur un écran spécifique.

Etude du cas 1 : Conduite et surveillance par opérateur

Indépendance	Ok – La surveillance du déroulement de la synthèse est identifiée comme une tâche spécifique indépendante du scénario d'accident.
Efficacité	<p>Le système de noyage de la réaction peut être considéré comme un système de concept éprouvé (largement diffusé dans l'industrie chimique). La vanne permettant de l'actionner est accessible à l'opérateur et manœuvrable.</p> <p>Le volume d'eau a été déterminé pour le milieu réactionnel (note de calcul).</p> <p>Le personnel est formé et entraîné. Des exercices sont réalisés en lui indiquant que le réacteur est en emballement et en lui demandant de réagir au problème. L'entraînement réalisé n'est pas optimal et n'a pas permis de mettre en évidence la difficulté du diagnostic de la situation accidentelle. Cet entraînement ne permet pas de prendre en compte la réalité de la situation accidentelle telle qu'elle se réaliserait. De manière conservatoire, il peut être considéré que cela suffit à annuler le niveau de confiance de la barrière.</p>
Temps de réponse attendu	Le délai maximal d'intervention est supposé égal à 10 minutes (dépend de la cinétique d'emballement).
Temps de réponse estimé	Le temps de réponse intègre le temps nécessaire à la détection de la situation accidentelle (calcul de la vitesse de montée en température et éventuellement confirmation) + le temps nécessaire pour ouvrir le circuit de vidange de l'eau dans le réacteur sachant que la vanne se situe à l'étage. Le deuxième étage étant dédié à la préparation des réactifs, l'accès à la vanne risque d'être difficile de par la présence de fûts ou sacs de matières premières. De plus, il convient de noter que l'opérateur peut être amené à s'éloigner temporairement (temps difficilement estimable). Le temps de réponse ne semble pas optimal, de l'ordre de 6 minutes avec des hypothèses optimistes.
NC	<p><u>"Détection active" : l'opérateur doit consulter les indicateurs disponibles donnant les paramètres du procédé</u></p> <ol style="list-style-type: none"> 1. L'information est donnée soit par les indicateurs, soit par une courbe de montée en température. La lecture de l'information est facile (indicateurs et courbe lisibles). 2. L'opérateur est censé être à proximité du réacteur durant la phase à risque mais peut être amené à s'éloigner temporairement. Dans ce cas il n'y a pas d'alarme prévue. La disponibilité de l'opérateur n'est pas optimale. <p>Conclusion partielle : le groupe de travail a estimé une décote d'un niveau (-1) par rapport à l'indisponibilité de l'opérateur (possibilité d'autres phases à risques sur plusieurs réacteurs en même temps).</p> <p><u>Diagnostic et choix de l'action :</u></p> <ol style="list-style-type: none"> 1. La détection précoce de l'emballement de réaction demande de déterminer une vitesse de montée de température. Cette information n'est pas disponible directement et résulte d'un calcul ou d'une extrapolation sur une courbe dont l'échelle ne présente pas forcément la sensibilité adaptée au seuil de détection (par exemple : division du temps : 1 minute, division de température : 5°C). La tâche de détermination par calcul de la vitesse de montée en température peut conduire à des erreurs et demande donc au moins une confirmation.

2. *Choix d'action facile – L'opérateur connaît la signification d'une telle montée en température et maîtrise la conduite à tenir (ouverture du système de noyage). Il sait parfaitement que toute tentative de refroidissement autre que le noyage ne serait pas assez rapide.*

Conclusion partielle : La difficulté de traitement de l'information justifie la décote complète de cette barrière (-2).

Action de sécurité :

1. *Le temps de réponse est au moins de 6 min (à condition que l'opérateur soit présent) alors que le délai maximal d'intervention de 10 min : il y a une pression temporelle et un niveau de stress non négligeable.*

2. *La tâche d'ouverture de la vanne du système de noyage ne présente pas de complexité et la vanne est facilement manœuvrable (vanne quart de tour).*

Conclusion partielle : Le temps de réponse optimiste de l'ordre de 6 minutes (à condition que l'opérateur soit présent) par rapport au temps de réponse attendu de 10 minutes. Ce temps de réponse à lui seul justifie également la décote complète de cette barrière d'autant plus qu'il s'agit d'un temps de réponse optimiste (-2).

Activité impliquant plusieurs acteurs : sans objet

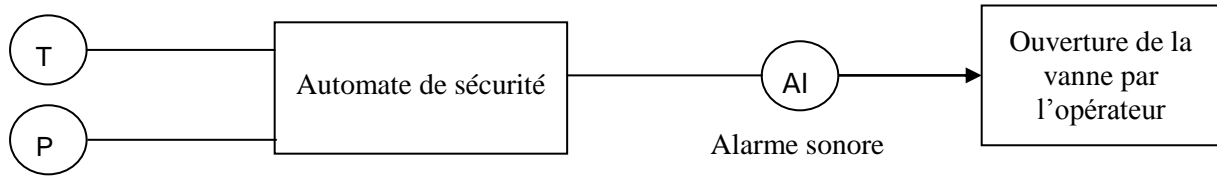
(Rappel : niveau de confiance maximal = 2)

Somme des décotes = 5

Niveau de confiance estimé = 2-5, donc le niveau de confiance = 0, celui-ci ne pouvant être inférieur à 0

Etude du cas 2 : Conduite et surveillance de la synthèse par le biais d'un système de supervision

Dans ce cas là la barrière de sécurité peut être décrite par le schéma suivant.



Sur atteinte d'un seuil de sécurité (température ou pression) une alarme sonore est déclenchée dans l'atelier et l'information de la situation accidentelle est indiquée sur l'écran de surveillance (voir ci-après).

Dans un premier temps, la composante humaine de cette barrière est étudiée en détail. Puis les composantes techniques sont décrites afin d'estimer le niveau de confiance global de la barrière.

Composante humaine :

<i>Indépendance</i>	<i>Ok – La surveillance du déroulement de la synthèse est identifiée comme une tâche spécifique indépendante du scénario d'accident. Cette surveillance est réalisée en salle de contrôle.</i>
<i>Efficacité</i>	<i>Le système de noyage de réaction peut être considéré comme un système de concept éprouvé (largement diffusé dans l'industrie chimique). Le volume d'eau a été déterminé pour le milieu réactionnel (note de calcul). La vanne permettant de l'actionner est accessible à l'opérateur et manœuvrable. L'alarme sonore est nettement audible dans tout l'atelier. Le personnel est formé et entraîné. Des exercices sont réalisés en lui indiquant l'alarme sollicitée et en lui demandant de diagnostiquer et de réagir au problème. Cet entraînement permet a priori de prendre en compte la réalité de la situation accidentelle telle qu'elle se réaliserait.</i>
<i>Temps de réponse attendu</i>	<i>Le délai maximal d'intervention est supposé égal à 10 minutes (dépend de la cinétique d'emballement).</i>
<i>Temps de réponse estimé</i>	<i>Le temps de réponse correspond au temps nécessaire pour identifier l'alarme et ouvrir le circuit de vidange de l'eau dans le réacteur sachant que la vanne se situe à l'étage. Dans le cas où l'opérateur s'est éloigné du poste de surveillance, étant donné que l'alarme est sonore, le temps de réaction de l'opérateur est limité au temps de retour au poste (environ 2 minutes) : l'opérateur peut facilement interrompre les activités dont il a la charge. Le deuxième étage étant dédié à la préparation des réactifs, l'accès à la vanne risque d'être difficile de par la présence de fûts ou sacs de matières premières. (environ 3 minutes). Le temps de réponse maximal peut être estimé à 5 minutes.</i>

NC	<p><u>Détection "passive" (alarme) :</u></p> <ol style="list-style-type: none"> 1. L'information est clairement identifiable : L'écran de surveillance signale le dépassement des seuils (indication du réacteur concerné et du seuil de sécurité atteint - utilisation d'un code d'affichage permettant de mettre en contraste cette information), et une alarme sonore est retransmise dans l'atelier donc la détection est évidente. 2. L'opérateur est normalement en salle de contrôle pendant la phase à risque mais il peut être amené à s'éloigner temporairement. Dans ce cas une alarme sonore (diffusée dans tout l'atelier) est prévue et il abandonne toute autre activité en cours. <p>Conclusion partielle : pas de décote</p> <p><u>Diagnostic et choix de l'action :</u></p> <ol style="list-style-type: none"> 1. L'information est suffisante et explicite : la tâche de détermination par calcul de la vitesse de montée en température est automatisée. 2. Choix d'action facile - L'opérateur connaît la signification de l'alarme et maîtrise la conduite à tenir (ouverture du système de noyage). Il sait parfaitement que toute tentative de refroidissement autre que le noyage ne serait pas assez rapide. <p>Conclusion partielle : pas de décote.</p> <p><u>Action de sécurité :</u></p> <ol style="list-style-type: none"> 1. Le temps de réponse est au moins de 5 min (au maximum) alors que le délai maximal d'intervention de 10 min : la situation peut s'avérer relativement stressante compte-tenu du temps de réponse et de l'éloignement avec la vanne à actionner. 2. La tâche d'ouverture de la vanne du système de noyage ne présente pas de complexité et la vanne est facilement manœuvrable (vanne quart de tour). <p>Conclusion partielle : La situation peut s'avérer stressante ce qui justifie la décote partielle de cette barrière (-1).</p> <p><u>Activité impliquant plusieurs acteurs :</u> sans objet</p> <p>(Rappel : niveau de confiance maximal = 2)</p> <p>Somme des décotes = 1</p> <p>Niveau de confiance estimé = 2-1 = 1</p>
----	---

Composante technique :

Nous supposons dans ce cas d'étude que le niveau de confiance global de la barrière ne sera égal à 1 que si le niveau de confiance de chacun des éléments techniques constitutifs de la barrière (capteur de température et de pression, automate de sécurité, alarme, vanne) est au moins égal à 1.

Afin d'estimer finement le niveau de confiance des composantes techniques (sur un cas détaillé) le lecteur pourra s'appuyer utilement sur le rapport Ω 10 [1].