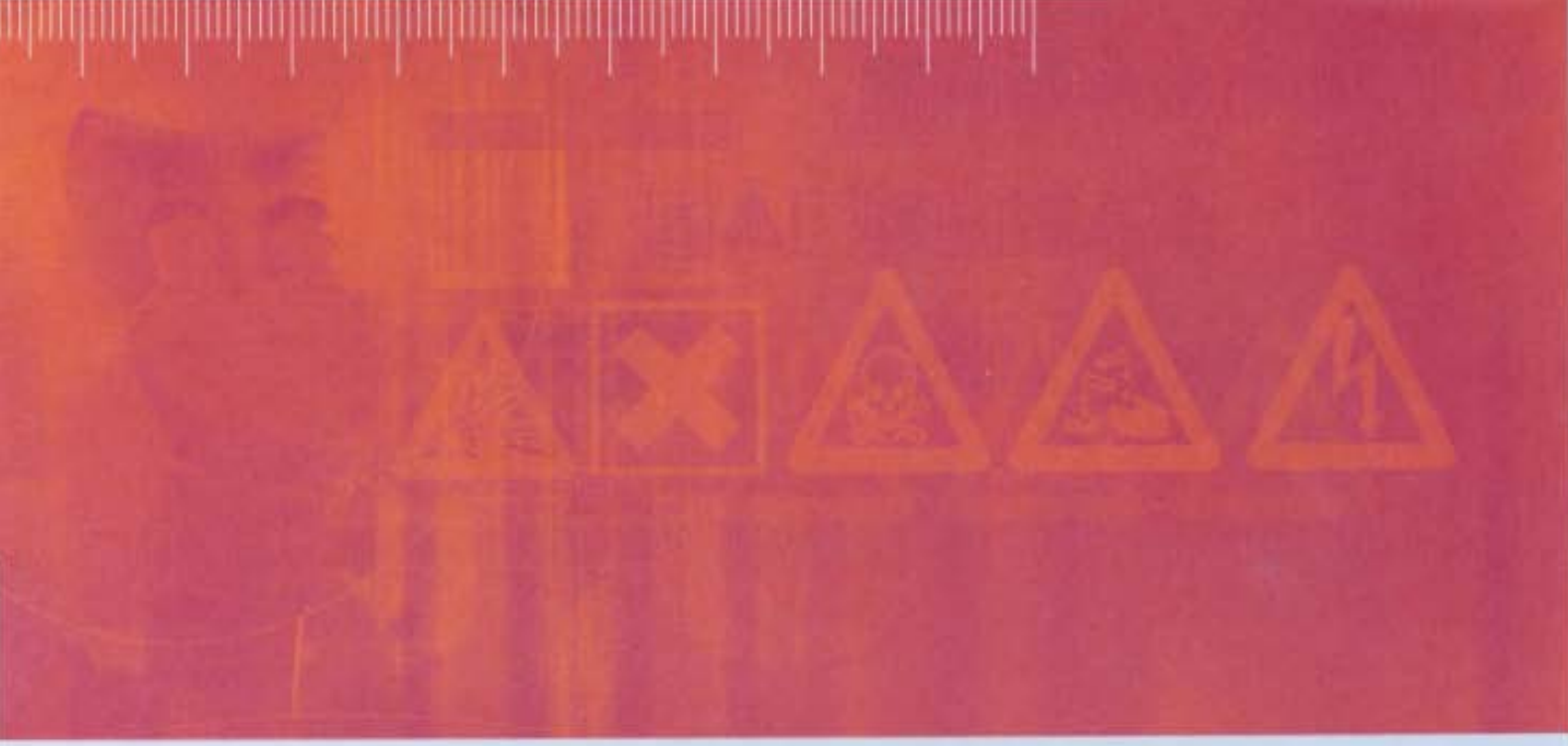


RAPPORT D'ÉTUDE 23/05/2018
N° DRA-17-164432-10199B

ÉVALUATION DE LA PERFORMANCE DES BARRIÈRES TECHNIQUES DE SÉCURITÉ OMEGA 10

INERIS
maîtriser le risque
pour un développement durable

Évaluation de la performance des Barrières Techniques de Sécurité
OMEGA 10

Direction des Risques Accidentels

Verneuil-en-Halatte (60)

Liste des personnes ayant participé à l'étude : Ahmed ADJADJ, Jean-Michel DRANGUET, François MASSÉ

PRÉAMBULE

Les rapports Oméga sont la propriété de l'INERIS. Il n'est accordé aux utilisateurs qu'un droit d'utilisation n'impliquant aucun transfert de propriété.

Le rapport Oméga est établi sur la base des données (scientifiques ou techniques) disponibles et objectives et de la réglementation en vigueur, ainsi que des pratiques et méthodologies développées par l'INERIS. Bien que l'INERIS s'efforce de fournir un contenu fiable, il ne garantit pas l'absence d'erreurs ou d'omissions dans ces documents.

Ce rapport est destiné à des utilisateurs disposant de compétences professionnelles spécifiques dans le domaine des risques accidentels. Les informations qu'il contient n'ont aucune valeur légale ou réglementaire. Ce sont des informations générales et ne peuvent, en aucun cas, répondre aux besoins spécifiques de chaque utilisateur. Ces derniers seront donc seuls responsables de l'utilisation et de l'interprétation qu'ils feront des rapports. De même, toute modification et tout transfert de ces documents se fera sous leur seule responsabilité.

La responsabilité de l'INERIS ne pourra, en aucun cas, être engagée à ce titre. En toute hypothèse, la responsabilité de l'INERIS ne pourra être retenue que sur la base de la version française de ces rapports.

	Rédaction	Relecture	Verification		Approbation
NOM	Ahmed ADJADJ	Franck PRATS	Valérie DE-DIANOUS	Frédéric MERLIER	Sylvain CHAUMETTE
Qualité	Ingénieur de l'unité Quantification des Risques et Performance des Barrières (QRIB) Direction des Risques Accidentels	Référent technique du pôle Analyse et Gestion intégrées des Risques (AGIR) Direction des Risques Accidentels	Responsable de l'unité Quantification des Risques et Performance des Barrières (QRIB) Direction des Risques Accidentels	Délégué Appui à l'administration Direction des Risques Accidentels	Responsable du pôle Analyse et Gestion intégrées des Risques (AGIR) Direction des Risques Accidentels
Visa					

RÉPERTOIRE DES MODIFICATIONS

Révision	Relecture	Application	Modifications
Version 1	Février 2005		Version 1 du document
Version 2	Septembre 2008		Version 2 du document
Version 3	Mai 2018		Version 3 du document

TABLE DES MATIÈRES

1 GLOSSAIRE ET DEFINITION

Barrière technique de sécurité (BTS) : ensemble d'éléments techniques nécessaires et suffisants pour assurer une fonction de sécurité. On les appelle aussi des Mesures de Maîtrise des Risques (MMR).

Barrières à action manuelle de sécurité (BAMS) : barrières qui font intervenir des éléments techniques et humains.

Barrière Instrumentée de Sécurité (BIS) : chaîne de traitement comprenant une prise d'information (capteur, détecteur…), un système de traitement (automate, calculateur, relais…) et une action (actionneur avec ou sans intervention d'un opérateur) et des moyens de communication (analogiques, numériques, Tout Ou Rien) pour réaliser une fonction de sécurité.

Concept éprouvé : un équipement ou un composant est dit de conception éprouvée lorsqu'il est utilisé depuis plusieurs années sur des sites industriels et que le retour d'expérience sur son application est bon, ou qu'il a subi des tests de « qualification » par l'utilisateur ou d'autres organismes. Ce principe doit être utilisé avec précaution, car il n'inclut pas les facteurs autres que la conception (contexte et historique d'utilisation sur un site donné, maintenance, organisation, taux de sollicitation, etc.…). Le concept éprouvé ne présage pas des autres critères (efficacité, temps de réponse et Niveau de Confiance).

Défaillance dangereuse : au regard d'une fonction de sécurité donnée, défaillance qui neutralise ou désactive l'action de sécurité.

Défaillance en sécurité : au regard d'une fonction de sécurité donnée, défaillance qui privilégie l'action de sécurité.

Dispositif de sécurité : élément unitaire, autonome, ayant pour objectif de remplir une fonction de sécurité, dans sa globalité. On distingue des dispositifs actifs et des dispositifs passifs (cf. § 3.1).

Efficacité ou capacité de réalisation : capacité d'une barrière à remplir la mission/fonction de sécurité qui lui est confiée pendant une durée donnée et dans son contexte d'utilisation. En général, cette efficacité s'exprime en pourcentage d'accomplissement de la fonction définie. Ce pourcentage peut varier pendant la durée de sollicitation de la barrière de sécurité.

Fonction de sécurité : fonction ayant pour but la réduction de la probabilité d'occurrence et potentiellement les effets et conséquences d'un événement non souhaité dans un système. Les fonctions de sécurité peuvent être assurées par des barrières techniques de sécurité, des barrières humaines (activités humaines), ou plus généralement par la combinaison des deux. Une même fonction peut être assurée par plusieurs barrières de sécurité.

Fonction Instrumentée de Sécurité (SIF) : fonction de sécurité assurée par un système instrumenté de sécurité (SIS).

Niveau de confiance (NC) : le niveau de confiance est la classe de probabilité pour qu'une barrière, dans son environnement d'utilisation, n'assure pas la fonction de sécurité pour laquelle elle a été choisie. Cette classe de probabilité est déterminée pour une efficacité et un temps de réponse donnés. Ce niveau de confiance est issu des SIL (Safety Integrated Level) définis dans les normes IEC 61508[4] et IEC 61511[5].

Mesure de Maîtrise des Risques (MMR) : les MMR sont définies dans le cadre des études de dangers françaises dans un objectif de prévention et de réduction des accidents majeurs. Elles doivent répondre aux exigences fixées à l'article 4 de l'arrêté du 29 septembre 2005. En particulier, une barrière de sécurité doit, pour être retenue comme MMR pour un scénario d'accident, être indépendante des événements initiateurs conduisant à sa sollicitation, c'est-à-dire :

- un événement initiateur à l'origine du scénario d'accident ne doit pas lui-même entraîner une défaillance ou une dégradation de la performance de la MMR ;
- le scénario d'accident ne doit pas avoir pour origine une défaillance d'un élément de la MMR.

Mesure de Maîtrise des Risques Instrumentée (MMRI) : une MMRI est une MMR constituée par une chaîne de traitement comprenant une prise d'information (capteur, détecteur…), un système de traitement (automate, calculateur, relais…) et une action (actionneur avec ou sans intervention d'un opérateur).

Performance des barrières : l'évaluation de la performance des barrières consiste en l'évaluation de leur efficacité, de leur temps de réponse et de leur niveau de confiance. Il est tenu compte des critères maintenabilité et testabilité permettant de garantir le niveau de performances dans le temps.

Probabilité de défaillance lors d'une sollicitation (PFD) : elle correspond à l'indisponibilité du système relatif à la **sécurité** à un instant donné.

Probabilité de défaillance moyenne lors d'une sollicitation (PFD_{avg}) : c'est la valeur moyenne de la PFD sur un intervalle de temps donné.

Fréquence moyenne de défaillance dangereuse par heure (PFH) : fréquence moyenne d'une défaillance dangereuse d'une barrière de sécurité pour réaliser la fonction de sécurité spécifiée pendant une période de temps donnée.

Processus de qualification : Processus démontrant qu'un équipement est capable de répondre aux exigences de performance spécifiées. La finalité du processus de qualification est d'assurer que l'équipement est adapté à son usage et satisfait les exigences de performance requises (efficacité et temps de réponse).

Redondance : existence, dans un composant, de plus d'un moyen pour accomplir une fonction requise (IEC 6271-1974).

Système instrumenté de sécurité : combinaison de capteurs, d'unité de traitement et d'actionneurs (équipements de sécurité) ayant pour objectif de remplir des fonctions instrumentées de sécurité.

Temps de réponse : intervalle de temps entre la sollicitation et l'exécution dans son intégralité de la mission/fonction de sécurité. Ce temps de réponse est inclus dans la cinétique de mise en œuvre d'une fonction de sécurité, cette dernière devant être en adéquation [significativement plus courte] avec la cinétique du phénomène qu'elle doit maîtriser.

Validé par l'usage : un composant peut être considéré comme « validé par l'usage » lorsqu'une évaluation documentée (basée sur un retour d'expérience quantifié) permet de valider son facteur de réduction de risques et son utilisation dans une fonction de sécurité.

Liste des autres abréviations utilisées dans ce rapport :

AMDE	:	Analyse des Modes de Défaillances, de leurs Effets
API	:	Automate Programmable Industriel
APS	:	Automate Programmable de Sécurité
APIdS	:	Automate Programmable Industriel dédié à la Sécurité
CEM	:	Compatibilité Électro Magnétique
EDD	:	Étude de Dangers
EIReDA	:	European Industry Reliability Data bank
EXERA	:	Association des Exploitants d'Équipements de mesure, de Régulation et d'Automatisme
GT	:	Groupe de Travail
LOPA	:	Layer Of Protection Analysis
NPRD	:	Nonelectronic Parts Reliability Data
OREDA	:	Offshore Reliability Data
REX	:	Retour d'EXpérience
SIF	:	Safety Instrumented Function (terme usuellement utilisé pour désigner une fonction instrumentée de sécurité)
SIL	:	Safety Integrity Level
SNCC	:	Système Numérique de Contrôle Commande

2 OBJECTIFS ET DOMAINES D'APPLICATION

2.1 INTRODUCTION

Les référentiels OMEGA constituent un recueil global formalisant l'expertise de l'INERIS dans le domaine des risques accidentels. Ce recueil concerne les thèmes suivants :

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

Ces rapports ont vocation à présenter les connaissances considérées comme consolidées au moment de leur rédaction. Ces rapports sont mis à disposition des acteurs de la maîtrise des risques d'accidents qui en feront bon usage sous leur responsabilité. Certains de ces rapports sont traduits en anglais en vue d'en favoriser leur diffusion. Les concepts exposés dans ces rapports n'ont pas vocation à se substituer aux dispositions règlementaires.

2.2 OBJECTIFS

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[1] relative à la prévention des risques technologiques et naturels et à la réparation des dommages (JO du 31 juillet 2003).

Cette loi introduit au niveau réglementaire[1] 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. L'évaluation de ces paramètres nécessite une analyse des barrières de sécurité techniques et humaines, appelées aussi mesures de maîtrise des risques. Ainsi l'article 4 de l'arrêté du 29 septembre 2005[2] précise "pour être prises en compte dans l'évaluation de la probabilité, les mesures de maîtrise des risques doivent être efficaces, avoir une cinétique de mise en œuvre en adéquation avec celle des évènements à maîtriser, être testées, maintenues de façon à garantir la pérennité du positionnement précité".

[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.

Par ailleurs, les exploitants doivent qualifier ou quantifier le niveau de maîtrise des risques, en évaluant les mesures de sécurité mises en place, ainsi que les dispositifs et dispositions d'exploitation, techniques, humains ou organisationnels, qui concourent à cette maîtrise.

Ce document a donc pour objectif d'exposer une méthode permettant :

- à l'exploitant de disposer d'une méthodologie pour évaluer la performance des barrières techniques de sécurité (BTS),
- à l'inspection des installations classées et à des organismes tiers-experts de disposer indirectement d'outils permettant d'apprécier l'évaluation des performances des barrières techniques de sécurité faite par l'exploitant des installations et présentée dans les études des dangers et dont le maintien des performances dans le temps sur site pourra faire l'objet d'inspections.

Les barrières techniques de sécurité (BTS) sont évaluées à travers l'analyse des critères **efficacité**, **temps de réponse** et **niveau de confiance**. Il est aussi tenu compte des critères de **maintenance** et de **testabilité** permettant de garantir leur niveau de performance dans le temps.

Ce document vise à présenter les principes généraux d'évaluation. Le site internet PRIMARISK (http://primarisk.ineris.fr/) fournit des éléments d'évaluation spécifiques à différents types d'équipements utilisés pour réaliser des fonctions de sécurité.

Seules les barrières techniques de sécurité sont abordées dans ce document. L'INERIS a développé une démarche d'évaluation analogue pour les barrières humaines de sécurité dans le rapport Ω20[3].

2.3 DOMAINE D'APPLICATION

Ce document présente une démarche permettant d'évaluer la performance des barrières techniques de sécurité mises en place sur un site industriel pour maîtriser les risques.

Il est important de préciser que la démarche présentée dans ce document pour évaluer le niveau de confiance ne se substitue pas aux normes IEC 61508 [4] **(sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité) et IEC 61511**[5] **(Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur de l'industrie de process), qui sont des références internationales dans le domaine.**

L'objectif de la démarche décrite dans ce rapport est avant tout de fournir une méthode relativement simple pour évaluer la performance des barrières techniques de sécurité, applicable en groupe de travail, notamment lors de la réalisation d'analyse des risques.

C'est à partir des performances de chacune des barrières de sécurité (mises en œuvre pour remplir une fonction de sécurité) que la maîtrise des risques d'une installation peut être démontrée, notamment par la diminution du risque induite par les barrières de sécurité.

La démarche proposée découle de travaux menés dans le cadre de programmes d'appui technique financés par le Ministère chargé de l'environnement, de notre veille réglementaire et normative (participation à de nombreux comités de normalisation nationaux et internationaux relatifs aux dispositifs de sécurité) et de notre expertise.

2.4 LIMITES DE L'OMEGA 10

Cette démarche présente une méthode d'analyse qualitative et semi-quantitative[2] permettant d'évaluer la performance des barrières de sécurité par rapport à un risque donné. Elle intègre notamment la détermination semi-quantitative d'un facteur de réduction de risque. Pour ce faire, elle s'affranchit des approches quantitatives plus lourdes à mettre en œuvre et nécessitant des données de retour d'expérience représentatives du contexte d'utilisation.

Les performances des installations de procédés assurant une fonction de sécurité (colonne d'abattage par exemple) ne peuvent pas être évaluées en mettant en œuvre directement la méthode OMEGA 10. Il est alors nécessaire de réaliser, en plus de l'analyse des risques associés à ces installations, une analyse des dysfonctionnements amenant ces installations à être indisponibles et à intégrer cette analyse sous forme d'une porte ET dans le nœud papillon. Il est à noter que pour que ces installations aient une meilleure disponibilité, des barrières de sécurité peuvent être mises en œuvre et évaluées selon les méthodes Omega 10 et 20.

2.5 PRÉSENTATION DES MODIFICATIONS DE L'OMEGA 10

Cette nouvelle version de l'OMEGA 10 est une mise à jour de la méthode qui prend en compte :

- le retour d'expérience des utilisateurs,
- les évolutions des normes de sécurité fonctionnelles IEC 61511[5] et IEC 61508[4],
- les prescriptions de la doctrine MMRI[6] et du guide de maîtrise du vieillissement des MMRI[7].

Jusqu'à présent, la méthode OMEGA 10 était basée sur les principes de tolérance à la défaillance (tableau de définition des NC) tels que définis dans la norme IEC 61508[4] pour les systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité. La norme IEC 61511[5], quant à elle, fixe des exigences pour la maîtrise des systèmes instrumentés de sécurité qui assurent des fonctions/barrières de sécurité (c'est donc une norme pour les utilisateurs de dispositifs de sécurité). Elle concerne les systèmes instrumentés de sécurité qui sont basés sur l'utilisation de capteurs, de systèmes de traitement et d'éléments

[2] Le terme qualitatif ou semi-quantitatif s'oppose aux méthodes quantitatives basées sur les calculs de fiabilité.

terminaux, quelle que soit leur technologie. Elle est donc adaptée à un industriel qui met en œuvre ses dispositifs de sécurité pour maitriser la sécurité de ses procédés.

La méthode d'évaluation du NC d'une barrière présentée dans cette nouvelle version de l'OMEGA 10 intègre les évolutions des deux normes et en particulier les modifications des contraintes d'architecture définies dans la révision de la norme IEC 61511[5] :

- les notions de systèmes simples ou complexes ont disparu,
- la proportion de défaillances sûres a été remplacée par des notions qualitatives.

3 TYPES DE BARRIÈRES DE SÉCURITÉ TRAITÉES

3.1 TYPOLOGIE DES BARRIÈRES DE SÉCURITÉ

Les barrières de sécurité sont de trois types :

- les barrières techniques,
- les barrières humaines,
- les barrières qui font intervenir les barrières techniques et humaines. Ces barrières sont appelées **barrières à action manuelle de sécurité (BAMS).**

Dans la catégorie des barrières techniques de sécurité, il peut s'agir de **dispositifs de sécurité** ou de **barrières instrumentés de sécurité (BIS)**.

Note : la bonne conception des installations ainsi que le respect des standards ne sont pas considérés dans ce document comme des barrières de sécurité, même s'ils participent effectivement à la maîtrise des risques. Ces éléments doivent être intégrés dans la démarche d'analyse des risques au niveau de la fréquence des événements initiateurs associés ou au niveau de la possibilité des scénarios d'accidents.

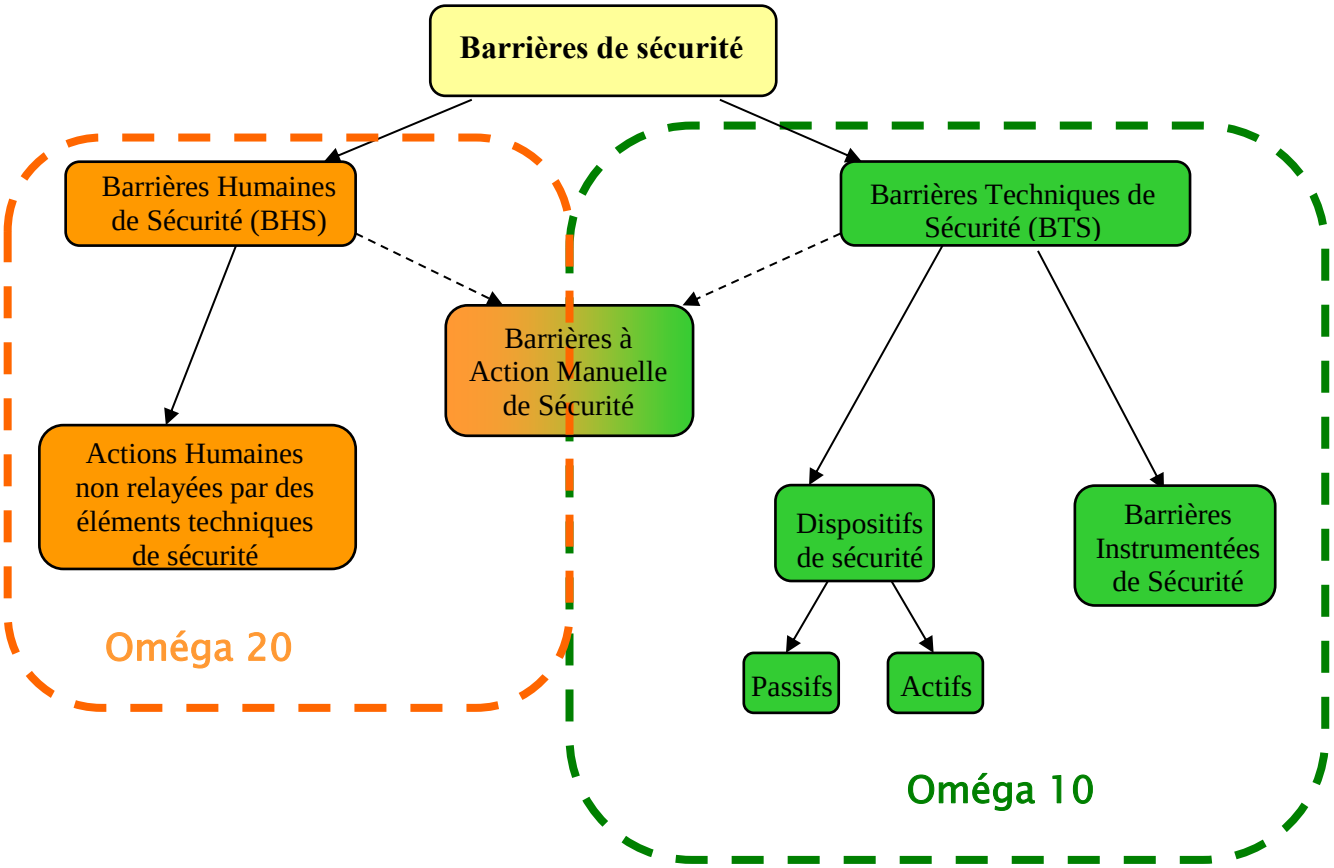


Figure 1 : Typologie des Barrières de Sécurité

À noter qu'en France dans le cadre des établissements soumis à autorisation, les barrières de sécurité peuvent être classées sous la terminologie générale MMR (Mesures de Maîtrise des Risques) et les BIS sous la terminologie MMRI (Mesures de Maîtrise des Risques Instrumentées). Les BAMS peuvent également, sous conditions[6], être classées sous la terminologie MMRI.

3.2 DISPOSITIFS DE SÉCURITÉ (PASSIFS OU ACTIFS)

Un dispositif de sécurité est en général un élément unitaire, autonome, ayant pour objectif de remplir une fonction de sécurité, dans sa globalité.

Un dispositif peut être classé en 2 catégories :

- Les **dispositifs passifs** qui ne mettent en jeu aucun système mécanique pour remplir leur fonction et qui ne nécessitent ni action humaine (hors intervention de type maintenance), ni action d'une mesure technique, ni source d'énergie externe pour remplir leur fonction. On retrouve notamment dans cette catégorie les cuvettes de rétention, les disques de rupture, les arrête-flammes ainsi que les murs coupe-feu.
- Les **dispositifs actifs** qui mettent en jeu des dispositifs mécaniques (ressort, levier…) pour remplir leur fonction. On retrouve notamment dans cette catégorie les soupapes de décharge et les clapets limiteurs de débit.

Remarque : une vanne de sécurité n'est pas considérée comme un dispositif de sécurité, car elle n'assure pas à elle seule une fonction de sécurité dans sa globalité. Il faut une action humaine et/ou une source d'énergie externe (cf. § 3.3 - BIS) pour l'actionner.

Le tableau ci-dessous présente des exemples de dispositifs classés selon leur type.

Dispositif actif	Dispositif passif
Soupape de sécurité	Murs de confinement
Clapet anti-retour	Murs coupe-feu sans ouverture
Double clapet de rupture	Écrans de protection mécanique ou thermique
Clapet excès de débit	Talus de réservoirs
	Arrête-flamme
	Ignifugeage
	Disque de rupture
	Cuvette de rétention
	Réducteur de débit sans ressort

Tableau 1 : Exemples de dispositifs actifs et passifs

3.3 BARRIÈRES INSTRUMENTÉES DE SÉCURITÉ (BIS)

Les barrières instrumentées de sécurité sont constituées par une chaîne de traitement comprenant une prise d'information (capteur, détecteur…), un système de traitement (automate, calculateur, relais…) et une action (actionneur avec ou sans intervention

d'un opérateur) et des moyens de communication (analogiques, numériques, Tout Ou Rien) pour réaliser une fonction de sécurité.

Les composants d'une B.I.S nécessitent une alimentation en énergie et en utilités pour fonctionner.

La figure suivante montre une représentation schématique générique d'une BIS.

Figure 2 : Schéma générique d'une BIS

Trois sous-fonctions principales composent une BIS : il s'agit des sous-fonctions « détection », « traitement de l'information » et « action ». Celles-ci sont décrites dans les paragraphes qui suivent. La transmission des informations entre ces sous-fonctions est décrite au paragraphe 3.3.4.

3.3.1 SOUS-FONCTION DE SÉCURITÉ « DÉTECTION »

Cette sous-fonction de sécurité peut être assurée par différents détecteurs de paramètres physiques sur le procédé (pression, température, niveau, débit, concentration, vibrations, survitesse…) et des détecteurs de phénomènes « externes » au procédé (détection feu et gaz par exemple). Ils sont présentés ici de façon générique.

Un **détecteur** de paramètre est généralement constitué de 2 éléments :

- **le capteur** qui est l'élément sensible assurant la transformation d'une information physique (pression, température, débit, concentration…) en grandeur électrique adaptée au traitement,
- et **le transmetteur** qui assure le conditionnement du signal émis par le capteur pour l'interface utilisateur. Le signal transmis peut être un signal analogique 4-20 mA, un signal numérique ou un signal de type binaire Tout ou Rien (1/0). Le transmetteur, suivant les cas (et ses possibilités), est connecté soit à l'entrée d'un système de traitement, soit directement à un actionneur.

La figure suivante présente les différentes possibilités de liaisons du détecteur.

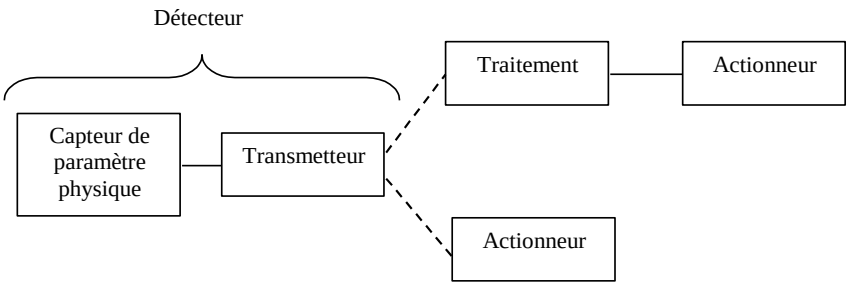


Figure 3 : Architecture depuis le capteur jusqu'à l'actionneur

3.3.2 SOUS-FONCTION DE SÉCURITÉ « TRAITEMENT DE L'INFORMATION »

La sous-fonction "traitement de l'information" peut être plus ou moins complexe. Elle est principalement réalisée par des relais ou par des automates programmables. Elle peut se résumer simplement à acquérir une grandeur mesurée par un capteur et à l'indiquer. Elle peut aussi consister à activer la commande d'un ou plusieurs actionneurs à partir d'une fonction combinatoire des informations délivrées par différents capteurs. Les **systèmes de traitement** peuvent être classés en deux catégories :

1. **Les systèmes électromécaniques, de deux types :**

   a. Les systèmes à base de logique à relais

   Il s'agit de technologies à base de modules/relais électromécaniques. Dans ce cas, pour les capteurs analogiques, le signal doit être converti en signal logique via des modules de relais à seuil.

   Les relais peuvent être classés en deux familles :

   - les relais dits "standard",
   - les relais dits "de sécurité".

   Un relais standard (cf. Exemple 2 de l'Annexe C) est un interrupteur électromécanique qui permet de fermer ou ouvrir des contacts, laissant passer ou isolant un courant dans un circuit électrique. Pour une utilisation en sécurité, il faut que la position de repos du contact corresponde à l'action de sécurité.

   Un relais de sécurité a une conception basée sur la combinaison de contacts en redondance et à guidage forcé (contacts liés) pour la commutation de sécurité. Il est également équipé d'un circuit de surveillance et détection de défaillances (contact collé, …)

   b. Les systèmes à base de logique statique de sécurité

   Ces systèmes sont utilisés pour des applications spécifiques impliquant un très haut niveau de confiance des fonctions de sécurité. Ils sont réalisés avec des composants non programmables : aucun microprocesseur ou aucune puce programmée n'est utilisé pour les fonctions de sécurité. La logique de sécurité est basée sur des éléments matériels électriques et électroniques (de type résistance, transistors…). Ils peuvent être également appelés Solid State Logic Solver.

2. **Les systèmes de traitement programmables ou paramétrables :**

   En technologie numérique, ce sont généralement des calculateurs (Systèmes Numérique de Contrôle Commande (SNCC) ou Basic Process Control System (BPCS), des Automates Programmables Industriels standard (API) ou Programmable Logic Controller (PLC) ou des Automates Programmables de Sécurité (APS).

   Suivant la taille, la complexité de l'unité et la modularité de l'unité, la fonction d'automatismes est remplie par un ou plusieurs modules (API, SNCC, PLC, APS) ou toute association de ces modules.

Le choix du système de traitement pourra dépendre de la complexité des fonctions à traiter ou des positions des éléments à raccorder. Pour des systèmes peu complexes, des relais pourront être utilisés. Pour des fonctions plus complexes nécessitant des traitements de l'information plus lourds, les automates seront préférés.

3.3.3 SOUS-FONCTION DE SÉCURITÉ « ACTION »

La sous-fonction "action" est réalisée par des actionneurs et des éléments terminaux.

Les **actionneurs** transforment un signal (électrique, pneumatique ou hydraulique) en phénomène physique qui permet de commander le démarrage d'une pompe, la fermeture ou l'ouverture d'une vanne… Selon l'énergie motrice, on parle d'actionneur électrique, pneumatique ou hydraulique. Ils sont couplés aux éléments terminaux.

Les **éléments terminaux** sont commandés par des actionneurs. On retrouve notamment sous cette terminologie : les vannes, les machines tournantes (pompe, compresseur …), les alarmes sonores et visuelles.

Il faut bien avoir à l'esprit que la finalité de la fonction de sécurité remplie par la BIS réside d'une part dans la détection d'une dérive ou du phénomène dangereux et d'autre part dans la mise en position finale de sécurité de ses éléments (ouvert/fermé, arrêt/démarrage). La BIS doit assurer la fonction totalement (détection, traitement, action finale). Si les sous-fonctions « détection » et « traitement » avec déclenchement d'une alarme sont assurées par des éléments techniques et que l'action finale est ensuite réalisée par une intervention humaine, on parlera dans ce cas de BAMS.

3.3.4 TRANSMISSION DES INFORMATIONS DES BIS

L'unité de traitement est reliée aux capteurs et aux actionneurs par des moyens de transmission. Il peut s'agir de câbles électriques, d'ondes électromagnétiques (transmission sans-fil), de fibres optiques (bus de terrain) ou de tuyauteries (transmission pneumatique ou hydraulique).

Les informations utiles au fonctionnement des BIS peuvent être de plusieurs types :

- logiques ou binaires quand leur valeur (ou la condition qu'elles représentent) est vraie ou fausse,
- analogiques quand elles représentent des grandeurs physiques associées à des échelles de mesure.

Ces informations peuvent être échangées sous plusieurs formes : électrique, pneumatique, hydraulique ou numérique.

Type de signal	Valeur logique	Valeur analogique
Électrique	Contact fermé ou ouvert Présence ou absence tension	4-20 mA 1-5 V
Pneumatique / hydraulique	Présence ou absence pression	0,2-1 bar ; 3-15 PSI
Numérique	Bit	Mot de n bits

Tableau 2 : Type de signaux et valeur dans une BIS

Dans l'industrie les modes d'échange les plus répandus sont le mode électrique, et depuis quelques décennies déjà, le mode numérique. La transmission de ces signaux est filaire (ou câblée), ou par réseau de communication (sur support électrique, optique ou électromagnétique).

Mode électrique :

La transmission de signaux (logiques ou analogiques) de manière filaire est simple, fiable et facile à tester ; elle doit être privilégiée quand les conditions le permettent (petites distances et nombre limité d'informations à transmettre).

La transmission de signaux analogiques par boucle de courant 4-20 mA, proportionnelle à la grandeur mesurée, est la plus répandue. Cette plage de valeur est parfois étendue à 0-22 mA pour permettre des fonctions de diagnostic type rupture de boucle ou défaut capteur (voir tableau suivant qui présente les plages de fonctionnement d'un signal analogique).

Plage en mA				
0 – 3,6 Défaut dans la boucle (coupure d'un conducteur ou défaut de l'alimentation)	3,6 – 4 Indéfini	4 – 20 Normale (possibilité d'étendre la plage à 3,8 – 20,5)	20 – 21 Indéfini	≥ 21 Défaut interne capteur ou court-circuit sur la boucle

Tableau 3 : Plage de valeurs d'un signal analogique

La plage de fonctionnement normal d'un capteur analogique est de 4 à 20 mA. Entre 3,6 et 4 mA et entre 20 et 21 mA, les valeurs sont non définies. La plage de fonctionnement normal peut être étendue entre 3,8 et 20,5 mA (mais très peu utilisée). Entre 0 et 0,2 mA, la plage correspond à une rupture de ligne. Pour des valeurs ≤ à 3,6 mA ou ≥ à 21 mA, cela correspond à un défaut (interne ou dans la boucle de mesure) du capteur.

Mode numérique :

Pour la transmission de signaux numériques, les réseaux locaux industriels ou réseaux de terrain (ou encore bus de terrain), sont de plus en plus utilisés. Ce sont des dispositifs assurant la transmission d'informations entre les différents éléments d'une BIS par l'intermédiaire d'un support unique (câble, fibre optique, radio, etc.).

Le bus de terrain est un système de communication numérique dédié qui respecte le modèle d'interconnexion des systèmes ouverts (OSI) de l'Organisation de Standardisation Internationale (ISO 7498[8]). Il est basé sur la restriction du modèle OSI à 3 couches :

1. couche Application (couche logiciel),
2. couche Liaison (couche matérielle),
3. couche Physique (couche matérielle).

La couche physique (support de transmission unique) relie les différents types d'équipements : E/S déportées, Capteur / Actionneur, Automate programmable (API), Calculateur, PC Industriel...

La communication entre les différents équipements est assurée via la couche application par un protocole de communication. Le protocole de communication est le langage commun (règles de dialogue) que doivent connaître et utiliser les équipements connectés sur le support de transmission pour dialoguer.

Ces réseaux n'ont pas été spécifiés et conçus pour la transmission d'informations relatives à la sécurité et des risques potentiels liés à l'implication de ces réseaux dans le maintien d'une fonction de sécurité peuvent avoir pour cause :

- soit une altération du traitement des informations,
- soit un retard dans le traitement des informations.

Ces spécificités doivent être prises en compte dans la performance d'une BIS.

Il existe des réseaux de terrain dits de sécurité capables de répondre à des exigences de niveau SIL (1, 2 ou 3). Ils intègrent des mécanismes permettant d'être tolérant à un certain nombre de défauts. Le niveau de sécurité atteint dépend du paramétrage.

3.4 BARRIÈRES À ACTION MANUELLE DE SÉCURITÉ

Les barrières à action manuelle de sécurité sont des barrières mixtes à composantes techniques et humaines : l'opérateur est en interaction avec les éléments techniques du système de sécurité qu'il surveille ou sur lesquels il agit.

Par exemple, la mise en position de sécurité d'une vanne de sécurité par actionnement manuel d'un bouton d'arrêt d'urgence suite à une détection de fuite de gaz au cours d'une ronde de surveillance est assimilée à une barrière à action manuelle de sécurité.

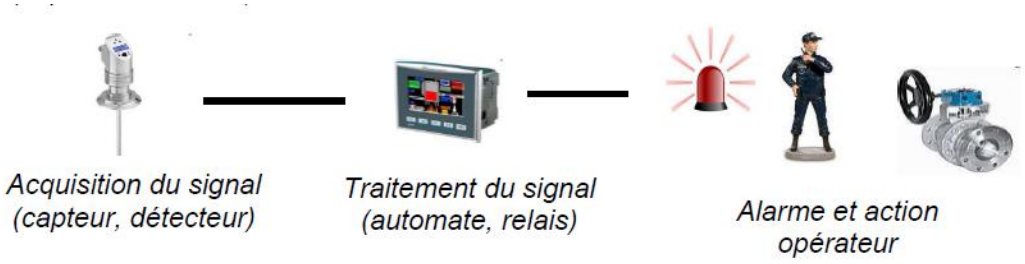


Figure 4 : Schéma générique d'une BAMS

La démarche d'évaluation présentée dans ce document s'applique exclusivement à la composante technique du système. Pour disposer d'une évaluation complète, le lecteur devra faire le lien avec la démarche présentée dans le rapport Ω20[3] relatif à la démarche d'évaluation des Barrières Humaines de Sécurité.

À noter que lorsque l'action humaine se situe uniquement au niveau de l'actionneur pour commander un élément technique, la BAMS peut être considérée en tant que MMRI au sens de la doctrine MMRI du 2 octobre 2013[6].

4 ÉVALUATION DES BARRIÈRES TECHNIQUES DE SÉCURITÉ – DISPOSITIFS ACTIFS ET BARRIÈRES INSTRUMENTÉES DE SÉCURITÉ

4.1 RAPPEL SUCCINCT DE L'APPROCHE BARRIÈRE

Une analyse des risques a pour but d'identifier l'ensemble des phénomènes dangereux pouvant se produire sur un site et pouvant conduire à des accidents. La fréquence d'occurrence des différents événements initiateurs pouvant conduire aux phénomènes dangereux est estimée et l'ensemble des barrières de sécurité susceptibles de réduire les probabilités d'occurrence annuelle des phénomènes dangereux est listé.

Pour être retenues dans l'évaluation des probabilités d'occurrence annuelle des phénomènes dangereux, les barrières de sécurité doivent être indépendantes des événements initiateurs pouvant conduire aux phénomènes dangereux et avoir les performances en adéquation avec les scénarios étudiés (efficacité, temps de réponse).

L'approche par barrière consiste tout d'abord à vérifier, sur la base de certains critères, que les barrières de sécurité peuvent être retenues pour le scénario étudié, puis à leur attribuer un facteur de réduction de risque. La combinaison de la fréquence d'occurrence de l'événement initiateur et des facteurs de réduction de risques des barrières de sécurité agissant sur un même scénario, permet d'estimer une classe de probabilité d'occurrence pour le phénomène dangereux. L'INERIS qualifie le facteur de réduction de risques par le niveau de confiance (NC) des barrières de sécurité.

La probabilité d'occurrence du phénomène dangereux est ainsi évaluée en considérant le dysfonctionnement de la barrière. Mais le bon fonctionnement de certaines barrières pourra conduire également à des phénomènes dangereux complémentaires (scénarios résiduels) dont les intensités seront liées aux performances des barrières.

4.2 IDENTIFICATION DES BARRIÈRES TECHNIQUES DE SÉCURITÉ : CRITÈRES MINIMAUX

Des critères minimaux sont à respecter pour retenir une barrière technique de sécurité. Ces critères sont les suivants :

- **indépendance** : la BTS doit être indépendante des événements initiateurs pouvant conduire à sa sollicitation pour pouvoir être retenue en tant que barrière agissant sur le scénario induit par ces événements initiateurs. Ses performances ne doivent pas être dégradées par l'occurrence des évènements initiateurs.

  Ainsi, si une chaîne de sécurité de pression haute est raccordée sur le même capteur que celui utilisé pour la régulation, on ne pourra pas considérer que cette chaîne de sécurité agit comme une barrière de sécurité (partie détection) pour un évènement critique initié par une défaillance de la régulation de pression.

  De même, si un incendie est identifié comme cause potentielle de rupture de canalisation, on ne pourra pas retenir la fonction de sécurité associée à la fermeture d'une vanne de sécurité sur la canalisation si la vanne n'est pas à sécurité feu et qu'elle est située dans les effets de l'incendie.

- **utilisation pour la sécurité** : a minima, le descriptif technique de la BTS doit préciser qu'elle est identifiée pour la sécurité. Elle doit donc être conçue et traitée en tant que tel (Cahier des Charges spécifique, suivi dans le SGS, …).

Lorsque ces conditions sont remplies, la barrière peut être retenue comme barrière de sécurité et l'étude de ses performances peut être réalisée en analysant les 3 critères :

- Efficacité,
- Temps de réponse,
- Niveau de confiance (NC).

4.3 CRITÈRE 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'efficacité est évaluée notamment pour un scénario d'accident précis.

La mesure d'efficacité **s'exprime en pourcentage d'accomplissement** de la fonction de sécurité définie, en considérant un fonctionnement normal de la barrière (non dégradé). Le pourcentage d'efficacité peut varier pendant la période de sollicitation de la BTS.

Généralement, l'efficacité est de 100%. Ainsi, une soupape de sécurité correctement dimensionnée permettra de prévenir l'éclatement du réservoir qu'elle protège. De même, une vanne parfaitement étanche permettra d'isoler une fuite de substance en cas de perte de confinement sur une canalisation.
Mais une barrière de sécurité peut ne pas être efficace à 100% ; elle sera alors retenue comme barrière de sécurité mais l'intensité du phénomène dangereux associé au fonctionnement de la barrière est alors évaluée en tenant compte de l'efficacité réelle de la barrière. Ainsi, un rideau d'eau peut abattre un nuage de X%. Le rideau d'eau peut être retenu comme barrière mais le phénomène dangereux associé à son bon fonctionnement fait intervenir la part du nuage non abattu, soit (100-X)%.
De même, une vanne peut être étanche à Y%. La vanne est alors retenue comme barrière mais le phénomène dangereux associé à son bon fonctionnement fait intervenir le débit de substance non arrêté par la vanne, soit (100-Y)%.

On notera que l'efficacité à 100% d'une BTS ne signifie pas qu'il n'existe pas de phénomène dangereux résiduel associé au fonctionnement de la barrière.

En effet, des scenarios résiduels peuvent résulter du bon fonctionnement de la barrière, par exemple :

- Le temps de fermeture d'une vanne peut conduire à un rejet dangereux.
- De même, le fonctionnement d'une soupape de sécurité conduira à un phénomène dangereux de rejet par la soupape.

Pour attester de l'efficacité d'une BTS, il faut :

- établir les scénarios de référence vis-à-vis desquels la barrière a été dimensionnée pour vérifier son adéquation,
- faire le bilan des informations connues afférant à ce critère et aux principes qui lui sont associés, ces informations provenant en partie du dossier technique du dispositif,
- et, à moins qu'il n'existe un solide retour d'expérience (document avec bonne traçabilité de l'utilisation sur le site, PV d'essais...) ou un dossier de qualification/validation, réaliser des essais, suivant un protocole défini, pour vérifier si la barrière est bien apte à remplir, dans son contexte d'utilisation, la fonction de sécurité qui lui est attribuée.

L'évaluation de l'efficacité repose en premier lieu sur les principes de **dimensionnement adapté** et de **résistance aux contraintes spécifiques**. D'autres paramètres, comme **le positionnement,** peuvent également, selon la barrière étudiée, influencer l'efficacité.

L'efficacité peut également être dégradée dans le temps. Pour diverses raisons (usure, corrosion, défaillances…), une barrière de sécurité peut ne plus remplir sa fonction de façon optimale. Ce manque d'efficacité peut avoir des conséquences indésirables sur la sécurité de l'installation.
L'exploitant doit s'assurer, au travers notamment de son système de gestion de la sécurité, que sa barrière est toujours en état de remplir sa fonction de sécurité avec l'efficacité telle qu'elle a été définie. Dans le cas où les performances se dégraderaient, l'exploitant doit préciser les mesures appropriées.

4.3.1 PRINCIPE DE DIMENSIONNEMENT ADAPTÉ

Les éléments constituant la barrière satisfont au principe de dimensionnement adapté lorsqu'ils sont conçus sur la base des normes et standards reconnus. Leur dimensionnement doit également tenir compte des événements redoutés à maîtriser et des conditions de fonctionnement du procédé.

L'ensemble de ces informations peut se retrouver dans des documents spécifiques (par exemple cahier des charges, dossier de spécification, fiche de vie, …).

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

- La technologie est-elle adaptée à la fonction de sécurité ?
- Existe-t-il des notes de calcul, des études spécifiques sur le dimensionnement de la BTS ?
- Existe-t-il des normes ou des standards professionnels concernant cette barrière ?
- Quelles sont les hypothèses (notamment relatives au déroulement de l'accident) qui ont servi de base pour le dimensionnement de ce dispositif ? Cette question est essentielle pour tous les dispositifs.

- Est-ce que le dispositif mis en place est bien dimensionné par rapport aux évènements susceptibles de se produire ? Par exemple, le débit d'extraction et le diamètre de la cheminée d'un local confiné sont-ils bien dimensionnés pour évacuer l'ammoniac susceptible d'être rejeté dans le local suite à la perte d'intégrité d'une canalisation…Ou le quench[3] sur un réacteur en phase initiale d'emballement permet-il de stopper l'emballement si celui-ci est dû à une perte du système d'agitation ?
- Des essais ont-ils été réalisés (in situ, en laboratoire) ?
- Quel est le retour d'expérience sur l'utilisation de ce dispositif ?

4.3.2 PRINCIPE DE RÉSISTANCE AUX CONTRAINTES SPÉCIFIQUES

Ce principe consiste à vérifier que la BTS a été conçue pour résister aux contraintes spécifiques liées :

- aux produits mis en jeu (corrosifs, …),
- à l'environnement (conditions météorologiques, risques sismiques...),
- à l'exploitation (pression de travail élevée, température élevée, …),
- à la tenue, le cas échéant, à des surpressions, aux effets thermiques…

La résistance aux contraintes spécifiques doit être validée par des notes de calcul, des essais ou par des attestations du constructeur.

La liste des questions suivantes (non exhaustives) permet de caractériser le principe de résistance aux contraintes spécifiques :

- Le dispositif est-il conçu pour résister aux contraintes liées à son utilisation et son environnement en situation normale et en situation dégradée du fait de l'accident (propriétés physico-chimiques, pression et température du procédé, température ambiante, hygrométrie, poussière, vibration, CEM, …) ?
- Est-ce que la barrière est adaptée pour la maîtrise des risques liés aux produits mis en jeu ? Par exemple, le matériau d'un organe d'isolement est-il compatible avec l'ensemble des produits (de production, de tests, de nettoyage…) susceptibles de circuler dans la canalisation ?
- Est-ce que la barrière est apte à travailler dans des conditions particulières (de météorologie, de température, de pression…) notamment celles dans lesquelles l'installation peut se trouver en fonctionnement normal ou dégradé 'en cas d'incendie par exemple) ?

[3] Système permettant l'inhibition d'une réaction chimique par un brusque refroidissement.

4.3.4 POSITIONNEMENT

Dans certains cas, le positionnement de la barrière permet d'optimiser son aptitude à remplir la fonction qui lui est dévolue. Il s'agit par exemple :

- des capteurs (de gaz, de flamme, de température, de pression…),
- des systèmes d'extraction (position du conduit d'extraction dans le bâtiment en partie inférieure ou supérieure du local),
- de murs coupe-feu,
- de vannes (optimiser leur positionnement vis à vis des fuites),
- etc…

Pour l'évaluation du critère « Positionnement adéquat », les documents suivants pourront être nécessaires :

- descriptif technique de la barrière,
- notes de calculs, études spécifiques,
- résultats d'essais,
- "standards" de la profession, quand ils existent.

Le positionnement et l'accessibilité de la barrière peuvent également avoir leur importance dans la réalisation des opérations de maintenance, de contrôle, de tests, d'étalonnage, car ces opérations ont une influence sur le maintien dans le temps de la performance de la barrière de sécurité (Cf. chapitre 7).

4.4 CRITÈRE 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.

Selon cette définition, le temps de réponse intègre :

- le temps nécessaire au fonctionnement d'une détection de l'incident suite à sa sollicitation,
- le temps nécessaire à la transmission et au traitement de l'information jusqu'aux éléments devant remplir l'action de sécurité,
- le temps nécessaire à la réalisation de l'action de sécurité.

Ainsi, le temps de réponse défini précédemment n'intègre pas le temps nécessaire pour que le flux de danger (par exemple un nuage de gaz) atteigne ou sollicite un capteur (temps entre la défaillance du procédé et la sollicitation de la barrière). Ce temps dépendra, notamment, pour des capteurs de gaz, de l'implantation des différents systèmes de détection par rapport à un point de fuite et donc de la configuration de l'installation étudiée (paramètre pris en compte dans l'*efficacité*). Ce temps doit être pris en compte et ajouté au temps de réponse pour comparaison avec la cinétique du phénomène.

Le temps de réponse de la barrière technique de sécurité peut a priori être obtenu de deux façons :

- soit en réalisant des mesures de temps de réponse, sur site, des barrières de sécurité (dispositifs de sécurité, équipements de sécurité et chaîne complète de sécurité),
- soit en additionnant les temps de réponse des dispositifs constituant la barrière de sécurité. Ces temps de réponse peuvent être fournis par les constructeurs. L'INERIS émet de fortes réserves pour cette 2ème solution : la transposition des informations communiquées par les constructeurs au contexte réel du site doit être ainsi réalisée avec précaution en comparant les conditions de détermination des temps de réponse avec les conditions réelles d'utilisation. D'autre part, il est à noter qu'il faut être prudent avec les performances annoncées des dispositifs de sécurité par les fabricants.

Ainsi, hormis un solide retour d'expérience, une validation sur site par des essais restent la seule solution pour vérifier si les performances réelles d'un équipement de sécurité dans son contexte d'utilisation, correspondent bien aux résultats attendus.

Si la réalisation d'essais n'est pas possible en raison du type d'installation étudiée (procédé en continu…), d'impossibilités techniques…, les temps de réponse fournis par les constructeurs ou le groupe de travail, peuvent être pris en compte pour évaluer le temps de réponse de la barrière. Il faudra, dans ce cas, veiller à bien préciser la référence des données dans l'étude et à adapter ces données au contexte d'utilisation.

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 inférieur à la cinétique. Il est donc essentiel que le temps de réponse soit clairement documenté.

Le temps de réponse de la barrière intervient ensuite dans l'évaluation des effets du phénomène dangereux : ainsi, le temps de fermeture de vanne (nécessairement non nul) conduira à un rejet dangereux.

4.5 NIVEAU DE CONFIANCE

4.5.1 FACTEUR DE RÉDUCTION DE RISQUES

4.5.1.1 LIEN ENTRE NC ET RÉDUCTION DE RISQUES

L'évaluation des probabilités d'occurrence des phénomènes dangereux fait intervenir les facteurs de réduction de risques induits par les barrières de sécurité. L'INERIS a retenu pour qualifier le facteur de réduction de risques le niveau de confiance (NC) de la barrière.

Le NC correspond à une réduction de risques (RR) telle que : $10^{NC}<RR\leq 10^{NC+1}$.

De manière conservatrice, on retient souvent que le NC est associé à une réduction de risques de 10^{NC}.

En revanche, si la probabilité de défaillance moyenne à la sollicitation de la barrière de sécurité a été calculée, cette valeur pourra être prise en compte pour une estimation plus précise de la fréquence d'occurrence de l'événement redouté analysé.

À noter que l'intensité du phénomène dangereux avec la probabilité d'occurrence réduite par le facteur de réduction de risques est **évaluée en considérant la défaillance de la barrière**.

Le principe d'allocation d'un NC à une BTS est explicité au paragraphe 4.5.4. Cependant une analyse qualitative préalable de la BTS est nécessaire. Les éléments faisant l'objet de cette analyse sont précisés au paragraphe 4.5.3.

4.5.1.2 PRINCIPE DE LA MÉTHODE D'ALLOCATION DES NC ET EXTRAPOLATION AUX AUTRES BARRIÈRES

Le tableau de la norme IEC 61511[5] permet d'attribuer un NC pour les barrières **instrumentées de sécurité**. Puis le NC est ensuite directement corrélé avec le facteur de réduction de risques. L'INERIS a étendu l'approche de la norme IEC 61511[5] aux **dispositifs actifs** (soupapes par exemple).

Pour les **dispositifs passifs**, l'évaluation du NC repose sur des principes différents qui sont détaillés au chapitre **5**.

4.5.1.3 LIEN AVEC LES PARAMÈTRES DE LA NORME IEC 61511[5]

La norme IEC 61511-1[9] présente des tableaux faisant le lien entre les diverses caractéristiques des systèmes (SIL, PFD_{avg}, PFH_{avg}).

Ils font apparaître trois types de systèmes :

- **Ceux fonctionnant en mode faible sollicitation** : mode de fonctionnement où la fonction de sécurité est effectuée uniquement sur sollicitation, afin de mettre le processus dans un état sûr spécifié, et quand la fréquence des sollicitations est inférieure à une fois par an.

  Autrement dit, une fonction de sécurité a un mode de fonctionnement de ce type (au sens de la norme), si un danger potentiel apparaît en cas de défaillance de la fonction de sécurité alors qu'un événement indésirable s'est produit dans le processus (dérive, erreur opératoire, …).

  Le SIL est alors relié à la probabilité moyenne de défaillance (PFD_{avg}) du système et à un facteur de réduction de risques.

- **Ceux fonctionnant en mode forte sollicitation** : mode de fonctionnement où la fonction de sécurité est effectuée uniquement sur sollicitation, afin de mettre le processus dans un état sûr spécifié, et quand la fréquence des sollicitations est supérieure à une fois par an.

  Le SIL est alors relié à la fréquence moyenne de défaillance par heure (PFH_{avg}) du système.

- **Ceux fonctionnant en mode continu** : mode de fonctionnement où la fonction de sécurité conserve le processus dans un état sûr dans le cadre de son fonctionnement normal.

  Autrement dit, une fonction de sécurité a un mode de fonctionnement de ce type (au sens de la norme) lorsqu'en cas de défaillance de la fonction de sécurité, un danger potentiel peut apparaître, sans autre défaillance.

  Le SIL est alors relié à la fréquence moyenne de défaillance par heure (PFH_{avg}) du système.

La sollicitation d'une fonction de sécurité, telle que définie précédemment, correspond à une mise en sécurité du process (automatique ou manuelle) dans le cadre d'un scénario accidentel. Les autres types d'activations de la fonction de sécurité (fonctionnement normal du process[4], test et déclenchement intempestif) ne sont pas considérés comme une sollicitation et ne sont donc pris en compte dans la fréquence de sollicitation.

Dans le cadre de l'approche barrière, on s'intéresse aux systèmes fonctionnant à la sollicitation (faible ou forte), pour lesquels on cherche à évaluer des facteurs de réduction de risques. Les systèmes fonctionnant en mode continu ne peuvent donc pas être considérés comme barrière car ils ne respectent pas le principe d'indépendance vis-à-vis du scénario d'accident.

Que ce soit une barrière fonctionnant à faible sollicitation ou forte sollicitation, l'évaluation du Niveau de Confiance (ou du facteur de réduction de risques) conformément à la méthode présentée dans ce rapport suit la même logique décrite au paragraphe 4.5.4. Elle reste liée au facteur de réduction de risque (RR). Néanmoins, la barrière sera spécifiée de manière différente pour sa conception : par une PFD_{avg} dans le cas d'une faible sollicitation et PFH_{avg} dans le cas d'une forte sollicitation.

Le tableau issu de la norme IEC 61511-1[9] pour le mode de fonctionnement à la sollicitation (dans lequel SIL a été remplacé par NC et pour lequel la ligne associée à NC 0 a été ajoutée) est le suivant :

[4] Un actionneur (moteur ou vanne) d'une fonction de sécurité peut également être utilisé pour le fonctionnement d'un process (par exemple démarrage et arrêt périodique pour un process batch ou un stockage). Ces formes de sollicitation ne sont pas considérées comme des sollicitations de la fonction de sécurité. En revanche, elles seront prises en compte dans la définition de la fréquence de test de la partie concernée de la fonction de sécurité.

Niveau de confiance (NC)	Probabilité moyenne de défaillance à la sollicitation (PFD_{avg})	Fréquence moyenne de défaillance par heure (PFH_{avg})	Réduction du risque (RR)
4	$10^{-5} \leq PFDavg < 10^{-4}$	$10^{-9} \leq PFHavg < 10^{-8}$	10 000 < RR ≤ 100 000
3	$10^{-4} \leq PFDavg < 10^{-3}$	$10^{-8} \leq PFHavg < 10^{-7}$	1 000 < RR ≤ 10 000
2	$10^{-3} \leq PFDavg < 10^{-2}$	$10^{-7} \leq PFHavg < 10^{-6}$	100 < RR ≤ 1 000
1	$10^{-2} \leq PFDavg < 10^{-1}$	$10^{-6} \leq PFHavg < 10^{-5}$	10 < RR ≤ 100
0	$10^{-1} \leq PFDavg < 1$	$10^{-5} \leq PFHavg < 10^{-4}$	1 < RR ≤ 10

Tableau 4 : Correspondance Niveau de confiance – réduction du risque pour des systèmes fonctionnant à la sollicitation

4.5.2 JUSTIFICATION DE LA MÉTHODE

4.5.2.1 LES NORMES IEC 61511 ET IEC 61508 À LA BASE DE LA MÉTHODE

Le NC est issu[5] des SIL (Safety Integrity Level) tels que définis dans les normes de sécurité fonctionnelle (IEC 61511[5] pour les systèmes instrumentés de sécurité pour le secteur des industries de transformation et IEC 61508[4] pour les systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité).

L'INERIS a étendu la notion de NC à tout type de dispositif en se reposant sur l'approche de la norme IEC 61511[5]. Contrairement à la norme IEC 61508[4], qui est une norme qui fixe des exigences pour la conception d'un dispositif de sécurité de technologie électrique et électronique (c'est donc une norme destinée aux fabricants qui maîtrisent la conception, jusqu'au composant), la norme IEC 61511[5] fixe des exigences pour la maîtrise des systèmes instrumentés de sécurité qui assurent des fonctions/barrières de sécurité (c'est donc une norme pour les utilisateurs de dispositifs de sécurité).

La norme IEC 61511[5] concerne les systèmes instrumentés de sécurité qui sont basés sur l'utilisation de capteurs, de systèmes de traitement et d'éléments terminaux, quelle que soit leur technologie et elle est appropriée dans le cadre d'une démarche semi-quantitative.

Dans les normes de sécurité fonctionnelles (IEC 61511[5] et IEC 61508[4]), l'évaluation des facteurs de réduction de risque repose sur deux aspects :

- **L'aspect qualitatif** : l'architecture définit des SIL maximums ;
- **L'aspect quantitatif** : les calculs permettent de déterminer les paramètres liés à l'indisponibilité qui conditionnent également le niveau de SIL.

C'est le SIL minimum issu des deux approches qui doit ensuite être retenu pour le SIL du système.

5 Le NC répond à des attentes d'évaluation simples en vue de la réalisation d'études de dangers. Le SIL selon les normes IEC 61511[5] et 61508[4] est une démarche différente.

L'INERIS retient, dans sa démarche explicitée dans le présent rapport, les aspects qualitatifs[6]. Il est ainsi supposé que les caractéristiques des systèmes (notamment fréquence de test adaptée, taux de défaillance adaptés) permettent d'assurer la contrainte quantitative[7]. Cette hypothèse peut ne pas être valable dans certaines conditions (fréquence de test faible, taux de défaillances élevé …).

4.5.2.2 NON-ÉQUIVALENCE SIL ↔ NC

Les normes couvrent toutes les phases du cycle de vie global des systèmes instrumentés de sécurité (SIS). En conséquence, il serait faux de considérer qu'un NC donné implique un SIL donné. L'allocation de SIL à un dispositif suppose le respect de nombreuses exigences complémentaires.

Au contraire, le SIL d'un dispositif peut conduire à déterminer un NC, sous réserve de la mise en œuvre adéquate du système sur site et que les conditions d'évaluation du SIL par le fournisseur du dispositif soient les mêmes que celles d'utilisation du dispositif sur site et de la prise en compte des contraintes liées au procédé et à l'environnement.

4.5.3 ANALYSE PRÉLIMINAIRE QUALITATIVE POUR LES BIS ET LES DISPOSITIFS ACTIFS

Au-delà des aspects d'allocation de NC à des systèmes de sécurité s'appuyant sur l'architecture des systèmes, il faut au préalable s'assurer qu'un certain nombre de **critères qualitatifs** est assuré : **concept éprouvé**, **sécurité positive**, bonne **maîtrise des mises hors service des barrières**…Il faudra également s'assurer que les systèmes de sécurité font l'objet de **tests périodiques** de fonctionnement et qu'ils sont correctement **maintenus**.

En l'absence de tests périodiques et d'opérations de maintenance, la barrière sera considérée comme non performante (NC0). On se reportera au chapitre 6 pour l'analyse des critères maintenabilité et testabilité.

La prise en compte des autres critères (concept éprouvé, sécurité positive, gestion des mises hors service) est traitée ci-dessous.

4.5.3.1 CONCEPT ÉPROUVÉ

Un dispositif utilisé à des fins de sécurité devra satisfaire au principe de concept éprouvé. Il doit pour cela être reconnu pour l'utilisation envisagée (bon retour d'expérience qualitatif sur des applications similaires).

Le concept éprouvé est un principe à utiliser avec précaution : il faudra s'assurer que la notion de concept éprouvé fait référence à des contextes d'utilisation similaires à ceux du site où le dispositif est mis en œuvre (contexte et historique d'utilisation, maintenance, organisation, etc.).

---

6 Le terme qualitatif s'oppose aux méthodes quantitatives basées sur les calculs de sûreté de fonctionnement.

7 Le NC dépend de la périodicité des tests et de la complétude de ces tests. Une stratégie de tests permettant de maintenir un NC constant dans le temps doit être définie.

Dans la mesure du possible, un dispositif de type nouvelle technologie devra donc être éprouvé *a minima* sur les utilisations en procédé ou en parallèle de dispositifs de concept éprouvé. À défaut, on pourra envisager un suivi et des tests sur le dispositif planifiés avec des fréquences plus importantes que celles définies pour des dispositifs de concept éprouvé.

Pour la justification du facteur de réduction de risques d'un dispositif de sécurité, on s'intéressera à son retour d'expérience quantifié et on parlera, dans ce cas, de dispositif "validé par l'usage" (cf. paragraphe 4.5.4.1).

4.5.3.2 PRINCIPE DE SÉCURITÉ POSITIVE

Quand on parle de sécurité positive, il faut distinguer la notion de sécurité à manque avec celle de sécurité positive.

Un équipement est dit "à sécurité à manque" lorsqu'une perte des alimentations/utilités (fluide moteur, électricité, …) conduit l'équipement à se mettre en situation sécuritaire stable.

Un équipement est dit "à sécurité positive" lorsque les défaillances principales (rupture ligne, perte signal, dérive, court-circuit, blocage… et perte d'alimentations) conduisent l'équipement à se mettre en situation sécuritaire stable. La notion de sécurité positive ("fail safe" en anglais) est donc beaucoup plus large que la notion de sécurité à manque qui ne considère que les défaillances liées à l'alimentation.

Dans ce rapport, un équipement est considéré à sécurité positive si au minimum il est de type "sécurité à manque". De plus, la position de sécurité doit être maintenue dans le temps.

En fonction du contexte, la position de sécurité pourra être différente. Par exemple, pour une vanne, la position de sécurité peut être la position ouverte (cas de vannes montées sur un réseau incendie ou un réseau d'inertage) ou fermée (cas des vannes situées sur des canalisations de transfert de substances dangereuses).

De façon générale, si une BTS n'est pas à sécurité positive alors que cette disposition est pertinente et applicable pour une utilisation en sécurité, des mesures particulières doivent être mises en œuvre pour s'assurer de son fonctionnement.

Il est aussi important de noter que :

1. **le principe de sécurité positive ne s'applique pas à tous les dispositifs** (par exemple : soupape de sécurité, bassin de rétention…).

2. **pour d'autres systèmes, la perte d'énergie conduira inexorablement à la perte de la fonction de sécurité** (par exemple, extracteur dans un local confiné ou système d'extinction incendie). Dans ce cas, on parlera de dispositifs de **sécurité à émission**.

Pour les dispositifs de sécurité à émission, on s'interrogera alors sur la fiabilisation du système d'alimentation et la nécessité de respecter les exigences suivantes :

- la perte d'intégrité de circuit est détectée (par exemple, surveillance de bout de ligne),
- l'intégrité de l'alimentation en énergie est assurée, en utilisant une alimentation auxiliaire (par exemple, groupe diesel, batterie de secours, alimentations sans coupure, capacité tampon d'air comprimé…).

Dans ces conditions, le dispositif pourra potentiellement être retenu comme une barrière (si les autres critères sont satisfaits). Une analyse des causes de perte d'énergie devra être menée, notamment pour s'assurer que l'alimentation de la barrière est maintenue en situation accidentelle et que la perte d'énergie ne conduit pas à la situation accidentelle. Pour un dispositif à émission, l'alimentation devra alors être étudiée comme un sous-système de la barrière avec une évaluation du NC associé (NC1, NC2…).

Concernant le principe de sécurité positive, les questions suivantes pourront être soumises aux personnes participant à l'évaluation de la performance de la barrière :

- Quelle est la position de repli de l'organe d'isolement ? Correspond-elle à une position de sécurité des installations ?
- La technologie des équipements est-elle compatible avec la position de repli (vannes simple-effet ou double-effet, …) ?
- La position de repli ne génère-t-elle pas de situations dangereuses ?
- Quelles mesures sont prises pour assurer l'alimentation en énergie dans le cas d'un dispositif à émission ?

4.5.3.3 MISE HORS SERVICE DE LA BARRIÈRE - GESTION DES SHUNTS / BY-PASS

La mise hors service de la barrière peut intervenir au moins de deux façons :

1. **La mise hors service peut se produire à la suite d'une action volontaire de by-pass.** Ils peuvent être utilisés afin d'inhiber tout ou partie d'une BTS pendant les opérations de tests, de maintenance ou en cas de défaillance. Ils doivent alors satisfaire les exigences suivantes :

- Une procédure d'utilisation des by-pass doit être définie et doit intégrer les modalités de remise en service des BTS.

  La procédure précise les modes opératoires, la fonction des personnes, la coordination et la communication de l'information des différents acteurs (qui active, qui garde la liste des matériels by-passés), la pose, la dépose, la remise en fonctionnement, les mesures compensatoires si nécessaire, les éventuelles restrictions sur les activités alentours, la procédure ou le dispositif prévu qui informe de l'état du système. La vérification du bon enlèvement de l'inhibition fait également partie des procédures de vérifications des opérations de maintenance (procédure de réception, procédure de remise en service).

- En plus des procédures, il est recommandé que les exploitants utilisent les moyens suivants pour éviter que l'inhibition reste en place :
    - l'établissement d'une liste des by-pass en possession de l'exploitant stipulant leur état,
    - l'utilisation d'un moyen de signalisation visuelle qui indique qu'une BTS est inhibée.

2. **La barrière peut faire l'objet d'interventions intempestives** conduisant à une perte de ses performances. Des dispositions doivent être prises par l'exploitant pour assurer l'intégrité de la barrière. Elle doit être protégée contre tout risque d'intervention qui peut la mettre en état hors service (par la modification des configurations, par une simple erreur de manipulation…).

On recherchera de manière qualitative à s'assurer que des mesures sont prises pour éviter des interventions intempestives ou pour gérer les périodes de by-pass. Les questions suivantes permettent de vérifier ces principes :

- Peut-on accéder et manœuvrer facilement la barrière ? Peut-on modifier la configuration de la barrière ?
- Les personnes intervenant sur la barrière sont-elles aptes à le faire ?
- Existe-il un système de verrouillage de la barrière (clé, code d'accès, …) ?
- Quelles procédures sont mises en œuvre pour gérer les shunts ?
- Comment s'assure-t-on de la remise en service de la barrière après un shunt ?

4.5.4 PRINCIPE D'ALLOCATION DES NC

4.5.4.1 DÉTERMINATION DES NC DES BIS ET DISPOSITIFS ACTIFS

L'évaluation semi-quantitative proposée permet d'attribuer un NC aux BIS à partir de leur architecture. Il s'appuie sur le tableau suivant extrait de la norme IEC 61511-1[9]. Il définit des contraintes d'architecture minimales pour une fonction instrumentée de sécurité en fonction du SIL et du mode de fonctionnement. Il s'agit d'exigences minimales applicables dans des conditions spécifiques telles que définies dans la norme.

SIL	Exigence minimale de tolérance aux anomalies matérielles[8]
1 (pour tous les modes)	0
2 (pour le mode à faible sollicitation)	0
2 (pour le mode continu et forte sollicitation)	1
3 (pour tous les modes)	1
4 (pour tous les modes)	2

Tableau 5 : Exigences minimales de tolérance aux anomalies matérielles selon le SIL

[8] La tolérance aux anomalies matérielles correspond au niveau de redondance. Si le retour d'expérience et la capacité de diagnostic le justifient, les normes IEC 61508 et 61511 permettent une tolérance par rapport à cette exigence de redondance.

Dans le cadre de l'approche présentée dans ce rapport, seul le mode de fonctionnement à la sollicitation est considéré.

L'allocation du NC à une BIS ou un dispositif actif est présentée dans les tableaux 6 et 7 suivants où les paramètres qui interviennent sont :

- **La tolérance aux anomalies matérielles** qui s'assimile à la présence ou non de redondance. Une fonction de sécurité (réalisée par une BTS) sera considérée comme "tolérante à une anomalie" lorsque le dysfonctionnement d'un des éléments la composant ne perturbera pas sa réalisation. La redondance d'éléments la composant est un moyen de répondre à cette exigence. Si on raisonne au niveau du composant, on recherchera les redondances internes. Au niveau des éléments de la barrière, on pourra rechercher les redondances externes (par exemple 2 détecteurs de gaz couvrant une même zone, deux soupapes permettant d'assurer chacune la prévention de l'éclatement d'un réservoir). La tolérance aux anomalies matérielles sera estimée à partir de l'étude de l'architecture du système et reliée à un scénario bien identifié.

- **La notion de "validé par l'usage'' pour un dispositif** qui est basée sur un retour d'expérience quantifié permettant de valider son facteur de réduction de risques. Il faudra que le dispositif soit utilisé depuis plusieurs années sur des sites industriels et que son retour d'expérience soit bon. La qualité du retour d'expérience[9] sera évaluée en s'appuyant sur :
  - le retour d'expérience de l'utilisateur (exploitant, service maintenance, inspection…), voire du fournisseur. Un suivi des barrières doit être réalisé permettant de prouver les performances (efficacité, temps de réponse, niveau de confiance) sur une période adéquate,
  - les standards ou normes indiqués par les syndicats professionnels ou les réglementations nationales et/ou internationales,
  - l'accidentologie sur des installations similaires (retour d'expérience des accidents, des incidents et des presqu'accidents).

Un dispositif est considéré "validé par l'usage" pour un NC donné si les conditions suivantes sont respectées :

- La démonstration de la performance du dispositif basé sur son REX correspond à une utilisation pour la/les mêmes fonctions et est réalisée dans des conditions similaires ;
- L'évaluation du NC atteint par le dispositif repose sur l'exploitation de son REX en prenant en compte :
  - le nombre de dispositifs observés,
  - la durée de fonctionnement cumulée,
  - les événements constatés (sollicitations, déclenchements intempestifs, défaillances…) ;
- Seul le concepteur peut modifier le fonctionnement intrinsèque du dispositif.

9 Une analyse quantitative des données de retour d'expérience (avec la borne supérieure de l'intervalle de confiance unilatéral à 70%) peut justifier la tenue des exigences quantitatives du NC visé.

- **La fréquence de sollicitation du dispositif** où deux modes de sollicitation sont considérés, tels que définis dans la norme IEC 61511-1[9] :
  - mode à faible sollicitation : la fréquence des sollicitations n'est pas supérieure à une par an,
  - mode à sollicitation élevée : la fréquence des sollicitations est supérieure à une par an.

Il est rappelé que la sollicitation d'une fonction de sécurité correspond à une mise en sécurité du process (automatique ou manuelle) dans le cadre d'un scénario accidentel ou incidentel. Les autres types d'activations de la fonction de sécurité (fonctionnement normal du process, test et déclenchement intempestif) ne sont pas considérés comme une sollicitation et ne sont donc pas pris en compte dans la fréquence de sollicitation.

Dans cette nouvelle version de l'Omega 10 une approche plus industrielle et pragmatique a été retenue pour définir le mode à forte sollicitation. Une fonction instrumentée de sécurité (SIF) sollicitée plusieurs fois par an devrait dans le cas général être considérée à forte sollicitation. Cependant, dans le cas d'une fréquence de sollicitations maximale de 3 par an, le mode de fonctionnement à faible sollicitation peut être accepté si la fréquence de test de la barrière est adaptée, avec une fréquence au moins aussi élevée que la fréquence de sollicitation prévue.[10]

Cette considération est acceptable si a minima les deux conditions suivantes sont respectées :

1. la fréquence de sollicitations maximale acceptable est de 3 par an ;
2. la maîtrise du scénario d'accident repose sur une ou plusieurs autres barrières de sécurité indépendantes en aval de la SIF ainsi sollicitée.

- **Le comportement sur défaut du dispositif** où est considérée la capacité de diagnostic et de traitement des défaillances du dispositif. Deux situations sont considérées :
  1. dispositif avec capacité de diagnostic capable de détecter / diagnostiquer une défaillance le concernant (un court-circuit, une dérive par exemple) et renvoyer a minima une alarme (par exemple capteurs analogiques ou numériques avec autodiagnostic (Cf. paragraphe 3.3.4) ;
  2. dispositif sans capacité de diagnostic qui n'est pas capable de détecter / diagnostiquer une défaillance le concernant, comme les capteurs binaires.

Un dispositif est considéré avec capacité de diagnostic dans la mesure où sa couverture de diagnostic (DC)[11] est supérieure à 60%.

[10] Il est rappelé, dans ce cas, que les sollicitations ne sont pas à considérer comme des tests ceux-ci devant être réalisés par ailleurs.

[11] DC : Diagnostic Coverage

La couverture du diagnostic d'un composant ou d'un sous-système est le rapport du taux des défaillances détectées au taux des défaillances totales du composant ou du sous-système détectées par les auto diagnostics. La couverture du diagnostic ne prend pas en compte les défaillances détectées lors des tests périodiques.

Rappel : Dans cette nouvelle version de l'OMEGA 10, la notion de proportion de défaillances sûres (SFF) a été supprimée. Ce critère est remplacé par le critère capacité de diagnostic.

- **La nature du dispositif** selon qu'il soit un élément d'une BIS ou un dispositif actif. Pour une BIS, les éléments considérés sont les capteurs, les systèmes de traitement programmables ou non programmables et les actionneurs. Les systèmes de traitement programmables d'une BIS correspondent aux automates programmables et les non programmables correspondent aux relais.

En fonction des paramètres définis précédemment, l'INERIS propose les approches suivantes (basées sur la norme IEC 61511-1[9]) pour la définition du NC.

1. Pour les **systèmes de traitement programmables** d'une BIS, le NC potentiel est présenté dans le paragraphe 4.5.4.2.

2. Pour les **autres systèmes (dispositifs actifs, capteurs, actionneurs et systèmes de traitement non programmables),** on distingue deux cas selon qu'ils soient ou non « validés par l'usage » :

   - **Systèmes non validés par l'usage :**
     a) Pour les **dispositifs actifs**, le NC potentiel est attribué selon le tableau suivant :

Caractéristiques de la barrière		**Tolérance aux anomalies matérielles**		
		0	**1**	**2**
Dispositif non validé par l'usage	**Faible sollicitation**	NC 1	NC 2	NC 3
	Forte sollicitation	NC 1	NC1	NC 2 par défaut voire NC 3

Tableau 6 : NC pour les dispositifs actifs non validés par l'usage

     b) **Pour les capteurs, actionneurs et systèmes de traitement non programmables,** le NC potentiel est attribué selon le tableau suivant :

Caractéristiques de la barrière		**Tolérance aux anomalies matérielles**		
		0	**1**	**2**
Sans capacité de diagnostic	**Faible sollicitation**	NC 1	NC 2	NC 3
	Forte sollicitation	NC 1	NC 1	NC 2 par défaut voire NC 3
Avec capacité de diagnostic	**Faible sollicitation**	NC 1 par défaut voire NC 2	NC 2 par défaut voire NC 3	NC 3
	Forte sollicitation	NC 1	NC 2	NC 3

Tableau 7 : NC pour les capteurs, actionneurs et systèmes de traitement non programmables non validés par l'usage

- **Systèmes validés par l'usage :**
  a) Pour les **dispositifs actifs**, le NC potentiel est attribué selon le tableau suivant :

Caractéristiques de la barrière		Tolérance aux anomalies matérielles		
		0	**1**	**2**
Dispositif validé par l'usage	**Faible sollicitation**	NC 2	NC 3	NC3
	Forte sollicitation	NC1	NC2	NC3

Tableau 8 : NC pour les dispositifs actifs validés par l'usage

b) **Pour les capteurs, actionneurs et systèmes de traitement non programmables**, le NC potentiel est attribué selon le tableau suivant :

Caractéristiques de la barrière		Tolérance aux anomalies matérielles		
		0	**1**	**2**
Sans capacité de diagnostic	**Faible sollicitation**	NC 2	NC 3	NC 3
	Forte sollicitation	NC 1	NC 2	NC 3
Avec capacité de diagnostic	**Faible sollicitation**	NC 2	NC 3	NC 3
	Forte sollicitation	NC 1 par défaut voire NC 2	NC 2 par défaut voire NC 3	NC 3

Tableau 9 : NC pour les capteurs, actionneurs et systèmes de traitement non programmables validés par l'usage

Rappel :

1. Pour attribuer un NC, le dispositif doit répondre aux critères qualitatifs (concept éprouvé, sécurité positive…).

2. Pour les éléments ''validés par l'usage'', le NC potentiel doit être justifié par un REX quantifié.

3. Dans le cas d'un dispositif à émission, l'alimentation en énergie doit être étudiée comme un sous-système avec attribution d'un NC. Celle-ci peut nécessiter la mise en œuvre d'une alimentation secourue fiabilisée, répondant aux contraintes d'indépendance, d'architecture et de maintenance compatibles avec le NC visé et disposant d'une autonomie suffisante pour la durée de la sollicitation. Cela signifie que dans ce cas les utilités et communications doivent être évaluées au même titre que les sous-systèmes détection, traitement et action.

4. Pour la définition du NC d'une BIS, il est important de s'assurer que les composants (matériel et logiciel) sont protégés contre les modifications.

4.5.4.2 NC DES SYSTÈMES DE TRAITEMENT PROGRAMMABLES D'UNE BIS

Pour le traitement d'une BIS réalisée par un automate programmable, la définition du NC dépendra du type d'automate : standard (API) ou de sécurité (APS).

- Pour un traitement assuré par un automate programmable standard :

  Ce type d'automate est utilisé pour faire à la fois de la conduite et de la sécurité (SNCC, …), les fonctions de sécurité assurées dans la partie sécurité peuvent être valorisées en tant que MMRIC avec un NC 1 tel que précisé dans le guide MMRI[6].

- Pour un traitement assuré par un automate programmable de sécurité, le NC correspondra au SIL associé.

Pour la transmission d'informations entre les différents éléments d'une BIS par l'intermédiaire d'un réseau de terrain, il est nécessaire que celui-ci soit un réseau de terrain dit de sécurité capable de répondre à des exigences de niveau SIL (1, 2 ou 3). Dans le cas contraire, un NC de 1 maxi pourra être retenu si une évaluation a montré que le risque d'altération du traitement des informations et de retard dans leur traitement n'a pas d'impact sur la performance attendue de la BIS.

De façon générale pour les systèmes de traitement de BIS, lorsqu'un niveau de confiance strictement supérieur à 1 est recherché :

- L'utilisation d'un APS répondant aux exigences de la norme IEC 61508[4] doit être retenue. Leurs cartes processeurs, mémoire et alimentation peuvent être redondantes et ils disposent de fonctions d'autodiagnostic. Leur position de repli en sécurité est connue en cas de défaut.
- L'utilisation de modules/relais éprouvés par l'usage ou répondant aux exigences de la norme IEC 61508[4] (ou autres standards tels que les normes IEC 61511[5], EN ISO 13849[10] et EN 954-1[11]) doit être retenue.

4.5.4.3 APPLICATION DES TABLEAUX – CAS PARTICULIERS

Pour le cas de dispositifs complexes et « non validés par l'usage » (analyseur de gaz, système de détection de fuite par mesures distribuées de température, …) un NC 1 peut être valorisé sur la base d'un suivi particulier en exploitation via des vérifications régulières (par exemple par la mise en œuvre d'un processus de qualification).

4.5.5 ÉVALUATION DES NC DES BARRIÈRES À PARTIR D'ÉLÉMENTS UNITAIRES – CAS DES DISPOSITIFS ACTIFS ET BIS

Dans la pratique, le NC de chacun des éléments unitaires constituant la barrière de sécurité est évalué séparément au cas par cas selon le scénario étudié en utilisant les tableaux présentés au paragraphe 4.5.4.1.

Puis on réalise les agrégations des NC des différents sous-systèmes selon les règles présentées ci-après.

4.5.5.2 ÉVALUATION DES NC UNITAIRES

Règle n°1 : SIL d'un sous-système -> NC

Si une BTS ou un élément de BTS répond aux exigences de la norme IEC 61508[4] (certificat, rapport d'évaluation, …) et possède donc un SIL, alors le NC retenu équivaut au SIL, **à la condition que l'exploitant suive les prescriptions du manuel utilisateur (ou safety manuel) fourni (installation, raccordement, configuration, maintenance…) et prenne en compte les contraintes liées au procédé et à l'environnement.**

Règle n°2 : NC unitaire maxi 3

Même en présence de redondance, l'attribution d'un NC de 4 à une BIS (ou à une sous-fonction) unique n'est pas réaliste actuellement car il supposerait des contraintes importantes.

Comme le précise la norme IEC 61511-1[9] : "Les applications, qui nécessitent l'utilisation d'une fonction instrumentée de sécurité unique du niveau 4 d'intégrité de sécurité, sont rares dans l'industrie des processus. Ces applications doivent être évitées, lorsque cela est raisonnablement possible, en raison de la difficulté d'atteindre et de maintenir de tels niveaux élevés de performance tout au long du cycle de vie. ".

Cependant, la norme IEC 61511[5] n'interdit pas le NC4. Dans le cas où un NC4 est valorisé pour une BTS, une analyse particulière devra être réalisée et des justifications devront être apportées[12].

Le NC maxi que l'on peut valoriser pour une sous-fonction d'une BIS, conformément à l'approche présentée dans ce rapport, est NC 3.

Règle n°3 : dispositifs actifs

Pour des systèmes composés de dispositifs de sécurité actifs, la détermination du niveau de confiance se fait directement à partir du tableau 9 du paragraphe 4.5.4.1.

4.5.5.3 ÉVALUATION DES BIS OU SYSTÈMES COMPLETS

Pour des BIS composées de différents sous-systèmes, les règles suivantes seront appliquées, en plus des règles précédentes.

Règle n°4 : éléments en parallèle d'une BIS ou d'un dispositif actif

Lorsque les composants ou sous-systèmes sont en parallèle, on ne réalise pas d'addition des NC des différents composants ou sous-systèmes mais on utilise les tableaux définis au paragraphe 4.5.4.1.

L'évaluation du NC de la fonction sera complétée d'une analyse sur les modes communs de défaillance (Cf. paragraphe 4.7).

[12] À titre indicatif : pas de logiciel, tolérance aux défaillances matérielles au minium de 2, …

Règle n°5 : éléments en série

Pour des sous-systèmes en série (cas des parties détection, traitement et action d'une barrière instrumentée de sécurité), le NC du système est le minimal des NC des différents sous-systèmes.

Si un nombre important de dispositifs avec le même NC se trouvaient en série (ce qui est peu probable), le NC du système devrait être réduit de 1, à moins qu'une analyse quantitative ne démontre que le NC est maintenu.

4.5.5.4 EXEMPLE D'ÉVALUATION

Un exemple d'illustration de l'application des règles n°4 et n°5 est fourni ci-dessous. On suppose une architecture dans laquelle une fonction de sécurité particulière est réalisée soit par la combinaison des sous-systèmes 1, 2 et 3, soit par la combinaison des sous-systèmes 4, 5 et 3, comme illustré sur la figure suivante. Dans ce cas, la combinaison des sous-systèmes 1 et 2 et la combinaison des sous-systèmes 4 et 5 ont la même fonctionnalité en termes de sous-fonctions de sécurité.

Dans cet exemple, la combinaison de sous-systèmes parallèles est basée sur le fait que chaque sous-système réalise la fonction de sécurité prescrite qui le concerne indépendamment[13] de l'autre sous-système (parallèle). La fonction de sécurité sera réalisée :

- en cas d'anomalie du sous-système 1 ou du sous-système 2 (car la combinaison des sous-systèmes 4 et 5 est capable d'assurer la fonction de sécurité indépendamment de 1 et 2),
- ou en cas d'anomalie du sous-système 4 ou du sous-système 5 (car la combinaison des sous-systèmes 1 et 2 est capable d'assurer la fonction de sécurité indépendamment de 4 et 5).

[13] Il est supposé dans cet exemple l'absence de mode commun de défaillance.

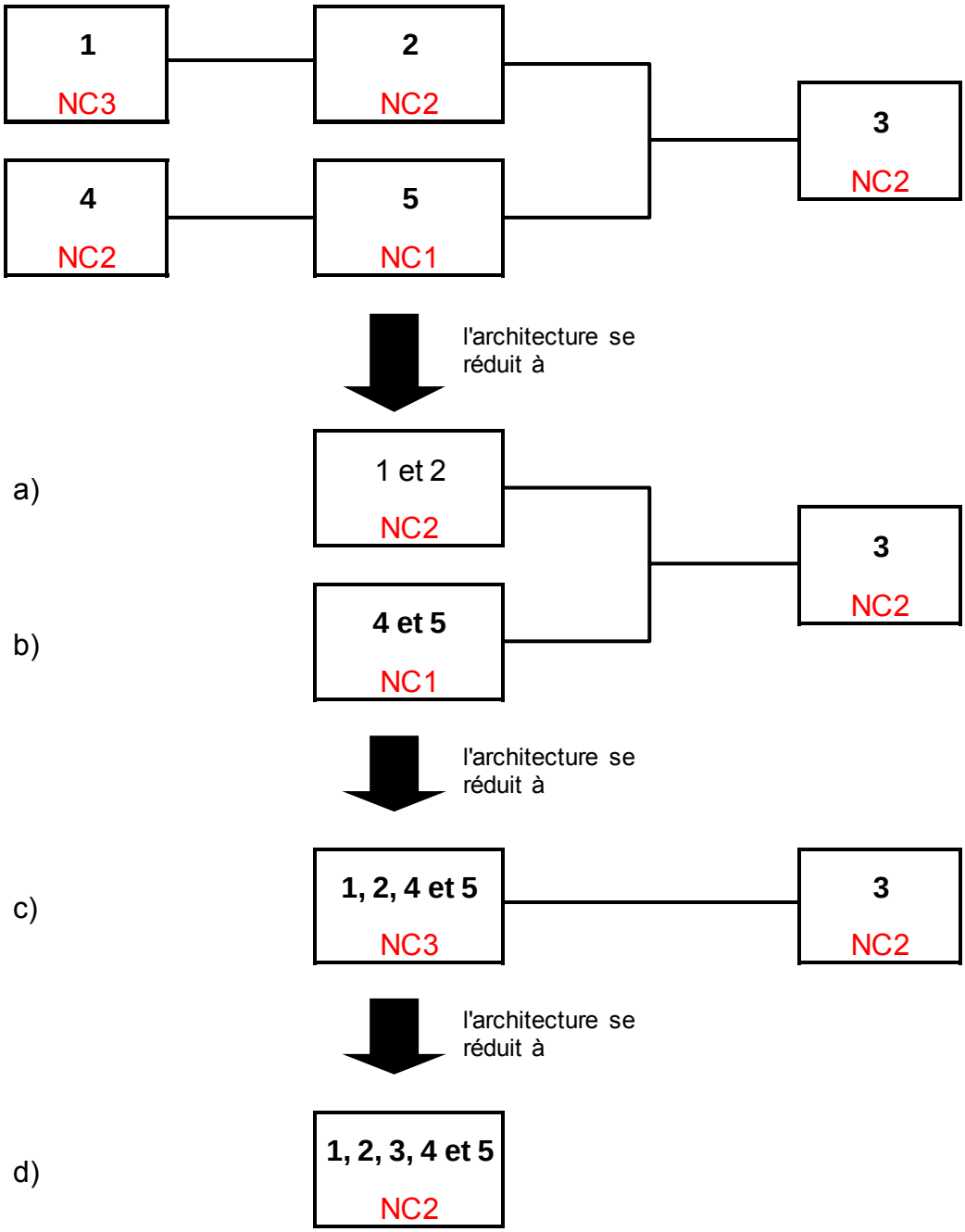


Figure 5 : Exemple d'évaluation du niveau de confiance d'une BIS composée de plusieurs éléments

La détermination du NC du système est détaillée dans les étapes suivantes :

a) en combinant les sous-systèmes 1 et 2 : la tolérance aux anomalies matérielles réalisées par la combinaison des sous-systèmes 1 (de NC 3) et 2 (de NC 2) satisfait aux prescriptions du NC 2 (déterminé par le sous-système 2) ;

b) en combinant les sous-systèmes 4 et 5 : la tolérance aux anomalies matérielles réalisées par la combinaison des sous-systèmes 4 (de NC 2) et 5 (de NC 1) satisfait aux prescriptions du NC 1 (déterminé par le sous-système 5) ;

c) en outre, en associant la combinaison des sous-systèmes 1 et 2 avec la combinaison des sous-systèmes 4 et 5 : le niveau de confiance du système, correspondant à la combinaison des sous-systèmes 1, 2, 4 et 5 est déterminée en retenant la combinaison de sous-systèmes qui a le NC le plus élevé et en analysant l'effet de l'autre combinaison de sous-systèmes sur la tolérance aux anomalies matérielles.

   Ainsi, dans notre exemple, la combinaison des sous-systèmes 1 et 2 a un NC de 2 tandis que la combinaison de 4 et 5 a un NC de 1. Cependant, en cas d'anomalie de la combinaison de 1 et 2, la fonction de sécurité pourrait être assurée par la combinaison de 4 et 5. De ce fait, le NC du système correspondant à la combinaison de 1, 2, 4 et 5 est 3.

d) la démarche pour identifier le NC du système constitué par la combinaison des sous-systèmes 1, 2, 4, 5 et 3 est identique à celle développée dans le a) et b).

Remarque : la représentation sous forme bloc diagramme, représentant l'architecture des BIS (Cf. Figure 5), permet de bien repérer les redondances. **Une attention particulière doit être portée au traitement des modes communs de défaillance.**

4.6 AGRÉGATION DES PERFORMANCES D'UNE BIS

Les performances des détecteurs, des unités de traitement et des actionneurs sont usuellement analysées séparément (mettant chacun en œuvre une sous-fonction de sécurité). Les résultats sont ensuite agrégés pour obtenir la performance de la BIS.

L'agrégation des différents critères est résumée dans le tableau ci-après.

Efficacité	Elle est égale à l'efficacité la plus faible des 3 sous systèmes $EF_{BIS} = Min\ (EF_{détecteur}, EF_{traitement}, EF_{actionneur})$
Temps de réponse	Il est pris égal à la somme des 3 temps de réponse de chacun des sous système $TR_{BIS} = TR_{détecteur} + TR_{traitement} + TR_{actionneur}$
Niveau de confiance	Il est égal au niveau de confiance le plus faible des 3 sous systèmes $NC_{BIS} = Min\ (NC_{détecteur}, NC_{traitement}, NC_{actionneur})$

Tableau 10 : Principe d'agrégation des performances des sous-fonctions d'une BIS

4.7 AGRÉGATION DES PERFORMANCES DES DIFFÉRENTES FONCTIONS DE SÉCURITÉ

Lorsque plusieurs barrières de sécurité interviennent sur un scénario d'accident, il faut évaluer la réduction de risques globale induite par l'ensemble des barrières de sécurité.

L'analyse des modes communs de défaillance doit être réalisée. **Elle pourra conduire à ne pas additionner les NC des différentes barrières.**

Des règles spécifiques pour l'analyse des modes communs de défaillances sont précisées dans le rapport Ω Agrégation semi-quantitative des probabilités [12].

D'un point de vue pratique, les questions suivantes (liste non exhaustive) peuvent permettre d'évaluer le mode commun de défaillance :

- Existe-t-il des évènements initiateurs pouvant conduire à la défaillance de plusieurs barrières de sécurité (incendie, explosion…) ?
- Les différentes chaînes de sécurité comportent-elles des éléments communs (action par une même personne, relais commun, automate commun, électrovanne commune, vanne commune…) ?
- Les barrières de sécurité sont-elles montées sur des piquages communs, utilisent-elles les mêmes technologies ?

4.8 SOURCES DOCUMENTAIRES

Les sources d'informations consultables pour évaluer la performance d'une barrière technique de sécurité sont :

- les standards et / ou référentiels des syndicats professionnels (Eurochlor, CFBP, UIC, UFIP…),
- la base de données sur les BTS et les rapports de l'INERIS sur les BTS disponibles sur PRIMARISK,
- les documents techniques des fournisseurs et des fabricants.

5 ÉVALUATION DES DISPOSITIFS ET BARRIÈRES PASSIVES

5.1 INTRODUCTION

Un dispositif passif est défini comme une barrière ne mettant en jeu aucun système mécanique pour remplir sa fonction et ne nécessitant ni action humaine (hors intervention de type maintenance), ni action d'une mesure technique, ni source d'énergie externe pour remplir sa fonction.

S'il est associé à des mesures techniques et/ou humaines et que leurs défaillances conduisent à la perte de la fonction de sécurité, le dispositif ne constitue plus une barrière passive.

On retrouve potentiellement dans cette catégorie les cuvettes de rétention, les disques de rupture, les arrête-flammes, les confinements, les murs coupe-feu...

L'objectif de ce paragraphe est de préciser le principe d'évaluation des performances des dispositifs passifs et des barrières mettant en œuvre la mesure potentiellement passive et des mesures techniques et/ou humaines associées.

5.2 ÉVALUATION DES PERFORMANCES DU DISPOSITIF PASSIF (ASSURANT SEUL UNE FONCTION DE SÉCURITÉ)

5.2.1 PRINCIPE D'ÉVALUATION DES DISPOSITIFS PASSIFS

L'évaluation des dispositifs passifs repose globalement sur les mêmes principes que les autres dispositifs.

En résumé, les différentes étapes de l'évaluation sont les suivantes :

1- Vérification que le dispositif est conçu pour une **utilisation en sécurité** et que son fonctionnement n'est pas affecté par la phase accidentelle (**indépendance**) ;
2- Évaluation de **l'efficacité** dans un contexte d'utilisation et pour une durée de fonctionnement donnée ;
3- Évaluation du **temps de réponse** (critère généralement non pertinent pour un dispositif passif) ;
4- Évaluation du **Niveau de Confiance (NC)** du dispositif.

Mais l'évaluation du NC s'appuie sur une démarche différente de celle mise en œuvre pour les autres dispositifs techniques (dispositifs actifs et barrières instrumentés de sécurité).

Les évaluations des différents paramètres sont précisées dans les paragraphes suivants.

5.2.2 EFFICACITÉ

Comme pour les autres dispositifs**, l'efficacité d'un dispositif passif doit être évaluée dans son contexte d'utilisation et pendant une durée donnée de fonctionnement.** Par exemple la propriété coupe-feu d'un mur sera maintenue pour une durée limitée.
L'évaluation de l'efficacité repose en premier lieu sur les principes de **dimensionnement adapté** et de **résistance aux contraintes spécifiques**. D'autres paramètres, comme **le positionnement (cf. § 4.3.3)** pour la définition des différents termes)**,** peuvent également, selon la barrière étudiée, influencer l'efficacité. L'efficacité est évaluée notamment pour un scénario d'accident précis (rupture brutale de bac, incendie de cellules d'aérosols…). L'efficacité doit être notamment analysée pour des causes bien spécifiques.

Note : lorsque le dispositif est associé à des mesures techniques et/ou humaines pour assurer la fonction de sécurité, l'efficacité de la fonction peut être compromise par la défaillance des mesures associées (cf. § 5.3).

L'efficacité peut également être dégradée dans le temps, si bien que la barrière de sécurité peut ne plus remplir sa fonction de façon optimale. À défaut de tests qui sont généralement non réalisables sur les barrières passives, des contrôles doivent être mis en œuvre permettant de vérifier des paramètres (tels que l'état général, l'étanchéité) qui traduisent finalement le bon fonctionnement de la barrière.

5.2.3 TEMPS DE RÉPONSE

Ce critère n'est pas pertinent pour les dispositifs passifs.

5.2.4 NIVEAU DE CONFIANCE

5.2.4.1 FACTEUR DE RÉDUCTION DE RISQUES

Comme pour les autres barrières (dispositifs actifs, barrières instrumentées de sécurité, barrières humaines et BAMS), le NC est associé à un facteur de réduction de risques.

De manière générale, une barrière passive donne lieu dans l'étude de dangers à deux situations dangereuses :

- le cas avec fonctionnement de la barrière (intensité réduite, probabilité non réduite du facteur de réduction de risque de la barrière) ;
- le cas avec défaillance de la barrière (intensité maximale, probabilité réduite du facteur de réduction de risque de la barrière).

Cependant en pratique dans les études de dangers, la défaillance de certaines barrières passives n'est pas retenue. Des exemples sont présentés au paragraphe 5.6. **La non prise en compte de la défaillance de la barrière équivaudrait à considérer que la barrière passive a un NC infini, vision qui ne doit être retenue qu'au cas par cas.**

5.2.4.2 ÉVALUATION DU NC D'UN DISPOSITIF PASSIF

Bien que la barrière passive soit généralement considérée comme "extrêmement fiable", il n'existe pas, à ce jour et à notre connaissance, de données disponibles qui permettent de quantifier leur probabilité de défaillance (pas de REX formalisé sur le fonctionnement des barrières passives, bases de données génériques ne précisant pas suffisamment les contextes d'utilisation).

L'ouvrage Layer Of Protection Analysis présentant la méthode LOPA[13] fournit des exemples de probabilité de défaillance sur sollicitation (PFD) de dispositifs de sécurité passifs que l'on trouve dans la littérature et dans l'industrie et propose de retenir une PFD. Mais les NC déterminés dans le LOPA[13] sont des valeurs moyennes dont l'origine des données n'est pas clairement exprimée, ce qui les rend difficilement exploitables car difficilement justifiables, en comparaison de la situation étudiée. Le tableau suivant présente ces informations.

Dispositif passif	PFD (littérature et industrie)	PFD retenu dans l'ouvrage LOPA
Cuvette de rétention	10^{-2} à 10^{-3}	10^{-2}
Système de drainage souterrain	10^{-2} à 10^{-3}	10^{-2}
Event ouvert	10^{-2} à 10^{-3}	10^{-2}
Ignifugeage	10^{-2} à 10^{-3}	10^{-2}
Mur résistant à la surpression / Bunker	10^{-2} à 10^{-3}	10^{-3}
Arrête Flamme	10^{-1} à 10^{-3}	10^{-2}
Disque de rupture	10^{-1} à 10^{-5}	10^{-2}

Tableau 11 : PFD de dispositifs extraits de l'ouvrage présentant la méthode LOPA[13]

Pour prendre en considération le fait que ce type de barrière est relativement fiable mais pour ne pas faire reposer toute la sécurité sur une seule barrière, il est proposé de retenir par défaut un NC2 sur les dispositifs passifs. De plus, ceci permet d'intégrer les hypothétiques défaillances dans le cycle de vie du dispositif (conception, fabrication, installation sur site, défauts intrinsèques, maintenance…).

Cependant, des mesures complémentaires peuvent être mises en place qui permettent de mieux détecter d'éventuelles défaillances ou de réduire les possibilités de défaillance de la barrière au moment où elle sera sollicitée. **Dans le cas de l'existence de ces mesures, il est proposé d'augmenter au cas par cas le NC à 3**.

Par exemple :

- des contrôles spécifiques internes (par l'industriel, sur la base d'une procédure de contrôle) et/ou externes (par des assureurs, par un organisme expert…) peuvent être mis en place à différents stades de la mise en œuvre de la barrière,
- accréditations des entreprises réalisant les installations,

- suivi de standards de conception, de fabrication, d'installation ou de construction,
- gestion des modifications selon des procédures.

A contrario, le NC de la barrière peut être réduit. Il est en effet nécessaire d'analyser pour chaque barrière les défaillances possibles ; une probabilité d'occurrence élevée sur une cause de défaillance **pourra conduire à réduire le NC à moins de 2.**

5.3 PRINCIPE D'ÉVALUATION DES BARRIÈRES DE SÉCURITÉ "PASSIVES"

Deux situations se présentent :

- **Lorsque le dispositif passif constitue à lui seul une barrière de sécurité** (exemple du mur coupe-feu sans ouvertures dans le mur ou du disque de rupture échappant directement à l'atmosphère), l'évaluation repose simplement sur les principes définis plus haut.
- **Lorsque la mesure potentiellement passive est associée à des mesures techniques et/ou humaines pour assurer une fonction de sécurité** (par exemple fonction de limitation de la propagation d'un incendie assurée par un mur coupe-feu et des portes coupe-feu, fonction de réduction des effets au sol assurée par un confinement et un extracteur), **l'évaluation de la barrière doit prendre en compte l'évaluation des mesures associées** (en utilisant par exemple les méthodes développées dans ce rapport et dans l'Oméga 20[3]).

Les deux situations suivantes sont possibles :

- **Lorsque la défaillance des mesures associées conduit à la perte totale de la fonction de sécurité,** l'évaluation des performances est faite en intégrant dans la performance de la barrière les performances des éléments associés. On ne considère alors que deux situations : fonctionnement ou défaillance de la fonction de sécurité. Les paramètres (efficacité, NC…) sont alors évalués pour la fonction de sécurité.
- **Lorsque la défaillance des mesures associées conduit à une perte partielle**[14] **de la fonction de sécurité**, l'évaluation des performances peut également être faite comme précédemment en ne considérant alors que les deux situations : fonctionnement ou défaillance de la fonction de sécurité.

  Mais il peut aussi être retenu de réaliser l'évaluation de la barrière en dissociant les différents éléments constitutifs et en les évaluant séparément.

[14] La perte partielle de la fonction de sécurité signifie qu'une fonction de sécurité reste assurée par la partie "passive" de la barrière. Par exemple une enceinte de confinement assure une réduction des effets de dispersion au sol même en cas de défaillance du système d'extraction.

Cette approche est certes plus complexe dans sa présentation car elle fait apparaître plus d'évènements associés respectivement au fonctionnement ou à la défaillance de chacun des composants de la barrière de sécurité. Les paramètres (efficacité, Niveau de Confiance…) sont alors évalués pour chaque fonction associée à chaque composant de la barrière.

Cependant cette approche présente deux avantages notables qui peuvent justifier son utilisation :

- Elle permet de faire apparaître clairement les événements associés à la défaillance du dispositif passif, ce qui permet de vérifier les conditions d'applicabilité (aspect mesure passive) du « filtre probabilité » défini dans la circulaire du 10 mai 2010[14].
- Elle permet de faire apparaître des évènements d'intensités et de probabilités graduées. La probabilité d'occurrence de chaque événement est évaluée respectivement à partir de la probabilité de défaillance du dispositif passif et à partir des probabilités de défaillance des mesures associées.

5.4 EXEMPLE ET REPRÉSENTATION EN ARBRES D'ÉVÈNEMENTS

On envisage les trois situations suivantes :

- Le dispositif assure seul la fonction de sécurité (pas de mesures techniques et/ou humaines associées).
- La défaillance d'une mesure technique et/ou humaine conduit à la perte totale de la fonction de sécurité liée à la barrière passive.
- La défaillance d'une mesure technique et/ou humaine conduit à une perte partielle de la fonction de sécurité liée au dispositif passif.

5.4.1 CAS DU DISPOSITIF PASSIF

On considère l'exemple d'un disque de rupture, supposé monté directement sur le réacteur qu'il protège de la surpression. L'arbre d'évènements est le suivant :

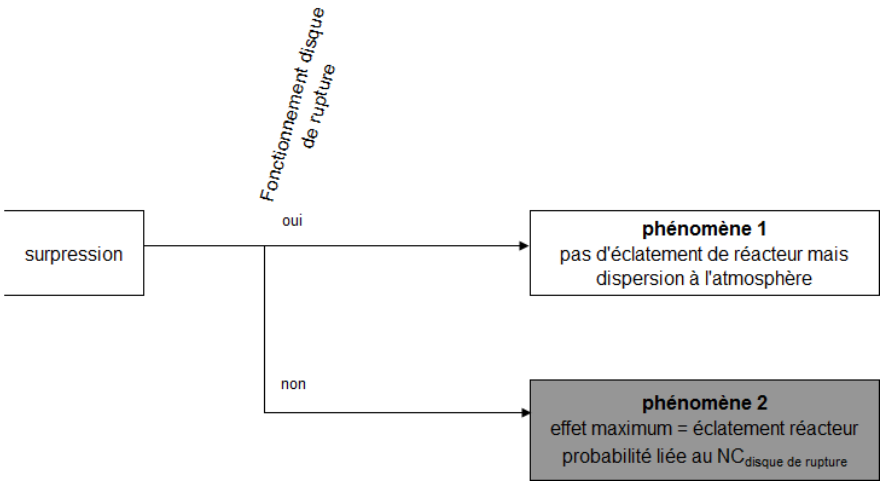


Figure 6 : Exemple d'arbre d'évènements - disque de rupture

5.4.2 CAS DE LA PERTE TOTALE DE LA FONCTION DE SÉCURITÉ

Si la défaillance des mesures techniques et/ou humaines associées à la mesure potentiellement passive conduit à la perte totale de la fonction de sécurité liée à la barrière passive, l'arbre d'évènements conduit à deux évènements : fonctionnement ou défaillance de la fonction de sécurité. Les performances (efficacité, NC…) sont évaluées en tenant compte des performances de chaque composant de la barrière.

Ainsi, pour des murs coupe-feu équipés de portes de grande surface, l'arbre d'évènements (sur la période inférieure au degré coupe-feu du mur) est le suivant :

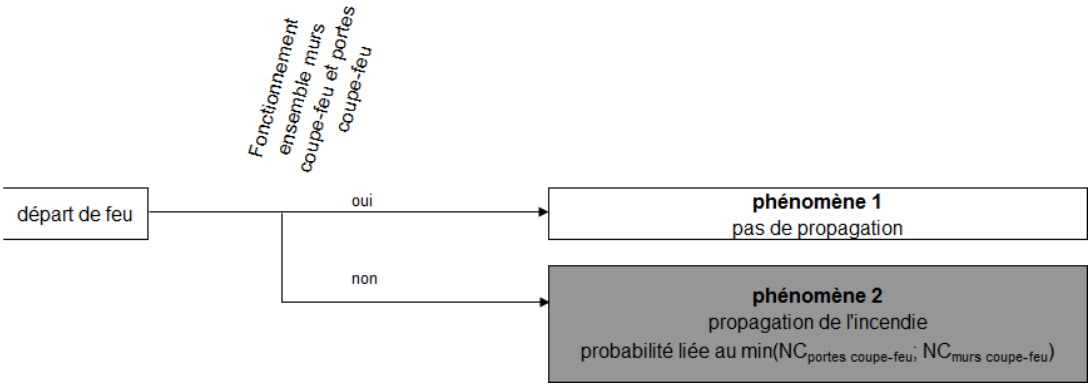
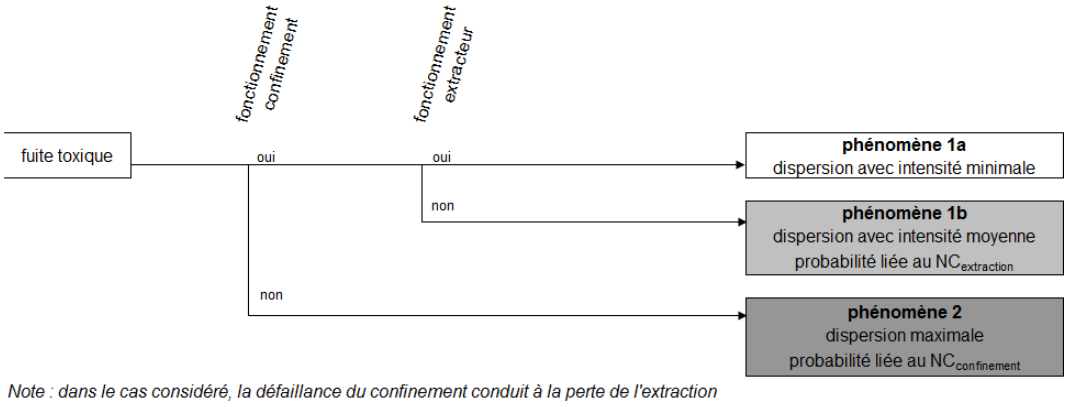


Figure 7 : Exemple d'arbre d'évènements – murs coupe-feu avec portes coupe-feu

Note : les figures font apparaître le paramètre NC. Celui-ci peut se traduire en pratique par une probabilité d'occurrence d'évènement.

5.4.3 CAS DE LA PERTE PARTIELLE DE LA FONCTION DE SÉCURITÉ

Si la défaillance des mesures techniques et/ou humaines associées à la mesure passive conduit à la perte partielle de la fonction de sécurité, il est possible de représenter l'arbre d'évènements de la façon suivante :



Note : dans le cas considéré, la défaillance du confinement conduit à la perte de l'extraction

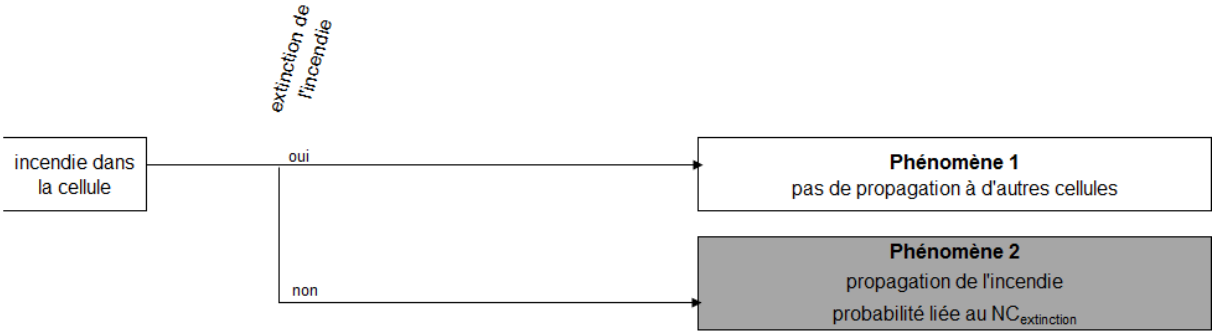
Figure 8 : Exemple d'arbre d'événements détaillé pour un confinement

5.5 CAS PARTICULIER DU DISPOSITIF PASSIF PERDANT SON EFFICACITÉ APRÈS UN CERTAIN DÉLAI

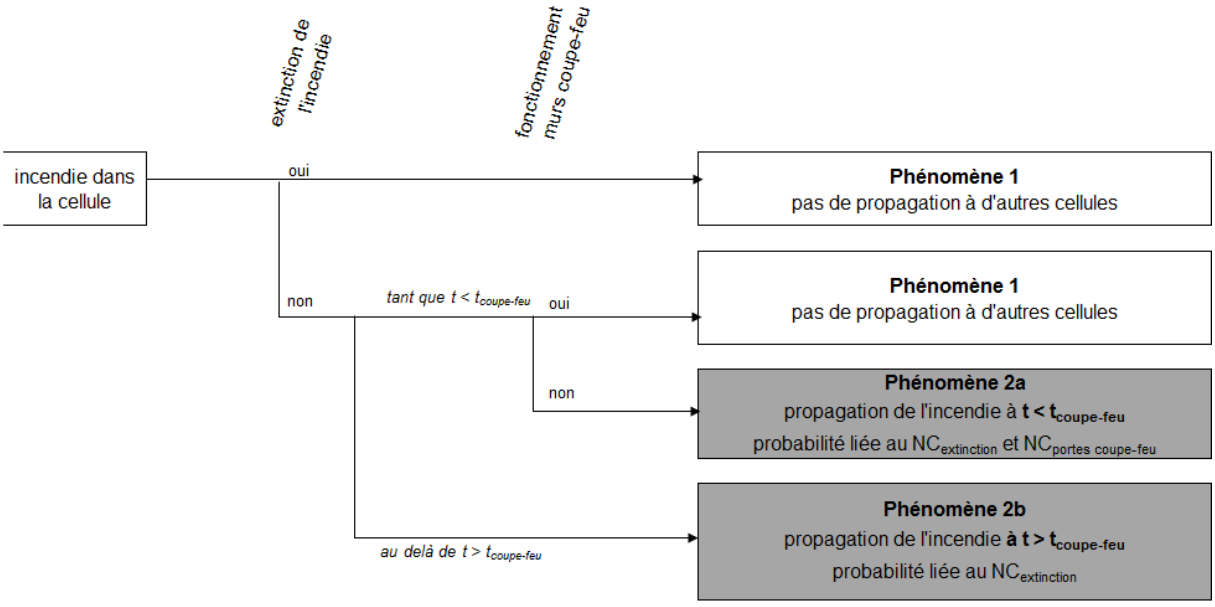
L'efficacité d'une barrière passive peut être dégradée au-delà d'un temps donné : au-delà de ce temps, la barrière passive n'intervient plus pour la réduction du risque. Elle pourrait donc ne pas être considérée dans l'arbre d'évènements. Cependant, il peut être intéressant de mettre en évidence la dynamique du scenario et de faire apparaitre des phénomènes avec des **cinétiques différentes** sur lesquels le rôle de la barrière passive apparait.

Par exemple : si des murs coupe-feu autour d'une cellule de stockage sont dimensionnés pour limiter la propagation d'un incendie pendant une durée $t_{coupe-feu}$ et que la capacité en combustibles dans la cellule peut conduire à un feu de durée supérieure à $t_{coupe-feu}$, le mur coupe-feu ne sera pas performant au-delà de $t_{coupe-feu}$. Deux représentations sont possibles prenant ou pas en compte l'aspect dynamique. La figure ci-dessous illustre ces deux possibilités :

Représentation simplifiée sans considération de l'aspect dynamique :



Représentation faisant apparaitre des phénomènes avec des cinétiques différentes :



note : de manière simplifiée, il est retenu sur la figure que le mur est "simple" (pas d'ouvertures dans les murs)
note : en pratique, dans les entrepôts, une barrière d'intervention peut être prise en compte pour prolonger la durée de tenue du mur.

Figure 9 : Exemples de représentation avec un incendie durant au-delà de la durée de tenue du mur

5.6 EXCEPTIONS À LA PRISE EN COMPTE DE LA DÉFAILLANCE DES BARRIÈRES PASSIVES DANS LES ÉTUDES DE DANGERS FRANÇAISES

Les exemples ci-dessous font apparaitre deux manières de faire :

- Comme expliqué précédemment, le phénomène dangereux associé à la défaillance de la barrière passive doit théoriquement apparaitre dans l'EDD ; il est alors modélisé (sous réserve de ne pas être écarté par application des filtres probabilité) et sa probabilité est évaluée en tenant compte de la probabilité de défaillance de la barrière passive (donc de son NC).
- Pour certaines barrières passives, la défaillance n'est pas considérée : le phénomène dangereux associé à la défaillance de la barrière passive n'est pas représenté dans l'EDD. Il est considéré d'office que la barrière fonctionne.

Des exemples sont présentés dans les paragraphes suivants.

5.6.1 TALUS DE RÉSERVOIRS GPL

La mise en œuvre d'un talus (ou technique mise en œuvre équivalente) conduit à ne pas retenir le phénomène de ruine (BLEVE et/ou rupture par projections / surpression) dans les EDD. Cette approche a été validée par le GT sectoriel GPL animé par le ministère de l'écologie et se traduit dans la circulaire du 10 mai 2010[14].

5.6.2 CUVETTE DE RÉTENTION

L'approche usuelle retenue dans les EDD pour tout type de substance est de ne pas envisager la défaillance de la cuvette avec épandage au-delà de la cuvette (à cause de sa défaillance). D'office, on modélise les effets d'un rejet dans la cuvette sans envisager que la substance peut se répandre en dehors de la cuvette. Si le déversement en dehors de la cuvette peut se produire pour d'autres raisons, il doit être étudié mais on n'est pas alors dans la logique de défaillance de la cuvette (il peut s'agir par exemple de fuites de tuyauteries situées dans la zone au-delà de la cuvette), d'un dimensionnement inadapté de la cuvette, de la cuvette remplie d'eau…

5.6.3 MUR COUPE-FEU

Dans le cas des entrepôts, un mur coupe-feu n'est pas considéré comme défaillant tant que la durée de l'incendie n'excède pas la durée de tenue du mur. On n'envisage donc pas de propagation et les évaluations des effets tiennent compte de la présence des murs.

Si l'incendie dure plus longtemps que la durée de tenue du mur, alors la propagation de l'incendie est envisagée en tenant compte de la barrière « intervention ». La propagation de l'incendie est liée à la défaillance de la barrière « intervention » et non celle du mur.

Dans la mesure où l'efficacité de la barrière intervention est démontrée, il n'y a pas de propagation. Cette approche a été validée par le GT sectoriel Entrepôt animé par le ministère de l'écologie.

5.6.4 BARRIÈRES DANS LES SILOS

Trois types de barrières passives ou mesures constructives sont identifiés usuellement dans les silos. Les pratiques, validées par le GT sectoriel silo et reprises dans le guide silos[15], sont de ne pas considérer leur défaillance :

- **Découplage** : ces barrières sont considérées bien dimensionnées (prescription de l'arrêté d'autorisation) et toujours retenues comme non défaillantes avec suppression des phénomènes d'explosions secondaires associés ;
- **Events ou surfaces soufflables** (version non normée de l'évent) : ce sont également des barrières ou mesures constructives qui sont considérées comme non défaillantes avec réduction des effets d'explosion des phénomènes d'explosion ;

  Note : cette approche se retrouve aussi dans d'autres secteurs (explosion de locaux tels que chaufferies, locaux avec unités de distillation, salles des machines de réfrigération ammoniac…).
- **Grille de réception** : celles-ci sont dimensionnées pour éviter l'introduction d'éléments de grande taille dans la manutention ; on ne les considère pas défaillantes.

6 ÉVOLUTION DES PERFORMANCES DANS LE TEMPS (MAINTENANCE ET TESTS)

La performance des BTS se dégrade dans le temps. Le maintien des performances dans le temps doit être assuré par la mise en œuvre d'une **maintenance et d'une inspection adaptées**, et en réalisant des **tests périodiques**[15] de fonctionnement.

En cas de modifications (sur les barrières ou sur le procédé), il faut s'assurer par une bonne **gestion des modifications** que les performances des barrières ne sont pas dégradées.

6.1 TESTABILITÉ

Pour vérifier si les performances d'une barrière de sécurité se maintiennent dans le temps, il faut tester cette dernière, c'est à dire qu'il faut simuler la situation de danger et vérifier si la fonction de sécurité pour laquelle elle a été mise en place est bien réalisée.

Le test doit concerner toute la barrière de sécurité et pas seulement un élément de la barrière. Ainsi lorsqu'on teste par exemple un détecteur, il faut veiller à tester non seulement le détecteur en lui-même (calibrage, seuils d'alarme, …), mais également ses asservissements (fermeture de vannes de sécurité, déclenchement d'une alarme, arrêt de pompes, …).

Les tests permettent d'avoir un retour sur la dérive des équipements et donc sur la maintenance à mettre en place.

La périodicité des tests et de la maintenance pourra varier et sera adaptée en fonction des résultats des tests réalisés par l'industriel dans le contexte d'utilisation. Elle peut être également définie à partir du calcul de la probabilité de défaillance de la BTS. Pour les BIS, elle peut être définie à l'aide de la méthode présentée en annexe du guide DT93[7] de l'UIC et de l'UFIP.

Dans tous les cas (sauf tests destructifs), tous les éléments d'une barrière de sécurité (soit la fonction de sécurité dans sa globalité) doivent faire l'objet d'un test par du personnel qualifié avant la mise en service de l'installation ainsi qu'avant chaque redémarrage.

Un test complet de la barrière doit être réalisé de préférence. Si le test complet n'est pas possible, des tests par partie peuvent être réalisés. Dans ce cas, il faudra s'assurer que l'ensemble des tests réalisés couvre bien l'intégralité de la performance de la BTS.

[15] On notera cependant que les barrières passives ne font généralement pas l'objet de tests périodiques mais font l'objet d'inspections.

Les questions formulées ci-dessous peuvent servir de support à l'étude de ce paramètre :

- La conception du dispositif de sécurité permet-elle de le tester périodiquement ?
- Peut-on le tester en ligne (en fonctionnement normal) lors de l'arrêt annuel (voire plus dans certaines industries) ?
- Y a-t-il des procédures de tests (validité, périodicité, archivage…) ?
- Comment sont testées les fonctionnalités de la barrière technique de sécurité ?
- Le dispositif intègre-t-il une fonction d'autotest ?
- Comment est déterminée la périodicité des tests ?

Dans le cadre des tests, les dispositifs nécessitant un étalonnage régulier feront l'objet de procédures d'étalonnage écrites.

On note que comme pour les opérations de maintenance, les essais peuvent être une source de défaillance. Il convient donc d'apporter la plus grande rigueur à la gestion de ces tests afin d'éviter qu'ils ne puissent conduire à une dégradation de la sécurité.

6.2 MAINTENANCE

Les barrières techniques de sécurité doivent faire l'objet d'une maintenance destinée à garantir le maintien des performances dans le temps. Ces opérations pourront prendre la forme d'opérations d'entretien ou d'opérations plus lourdes de maintenance.

La périodicité de la maintenance sera fonction :

- des données des constructeurs,
- du retour d'expérience de l'Industriel, donc de l'utilisation de la BTS dans ses conditions réelles de fonctionnement,
- des agressions liées à l'environnement naturel (atmosphère saline, humidité…),
- des agressions liées au procédé (température, pression…), au produit (corrosif…), à la localisation du dispositif…,
- des résultats des vérifications et des tests,
- etc.

L'industriel doit pouvoir prouver que la maintenance est effectuée sur chaque BTS étudiée et justifier sa périodicité.

On note cependant que la maintenance peut également être une source de défaillance et des mesures doivent être prises pour les prévenir (marches dégradées, gestion des by-pass…).

6.4 GESTION DES MODIFICATIONS

Des modifications du procédé et/ou du contexte d'utilisation peuvent être réalisées dans la vie d'une installation. Celles-ci peuvent conduire à dégrader les performances des barrières de sécurité ou les rendre inadaptées.

Une gestion des modifications doit être réalisée afin de garantir l'adaptation et le maintien des performances d'une barrière dans les nouvelles configurations.

On devra alors vérifier que les modifications font l'objet de procédures spécifiques (en particulier une analyse d'impact) qui conduisent à la vérification du bon fonctionnement des barrières.

7 SYNTHÈSE DE L'ÉVALUATION DES BTS

7.1 RAPPEL DES ÉTAPES DE L'ÉVALUATION

L'évaluation qualitative ou semi-quantitative des performances d'une barrière ou d'un sous-système se fait selon les étapes suivantes :

1 – Vérification Critères minimaux (cf. § 4.2)

La barrière ou sous-**système doit répondre aux critères minimaux suivants** :

- La BTS 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**.
- Spécification du dispositif pour **un usage en sécurité** : le descriptif technique doit justifier son utilisation « sécurité ».

2- Évaluation de l'efficacité (cf. § 4.3)

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**. La performance est évaluée notamment pour un scénario d'accident précis.

L'évaluation de l'efficacité repose en premier lieu sur les principes de **dimensionnement adapté** et de **résistance aux contraintes spécifiques**. D'autres paramètres, comme le **positionnement**, peuvent également, selon la barrière étudiée, influencer l'efficacité.

3- Évaluation du temps de réponse (cf. § 4.4)

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 inférieur à la cinétique**. Le temps nécessaire pour que le flux de danger atteigne ou sollicite le capteur (temps entre la défaillance du procédé et la sollicitation de la barrière) doit être pris en compte et ajouté au temps de réponse pour comparaison avec la cinétique du phénomène.

4- Évaluation niveau de confiance (cf. § 4.5)

Le NC permet de déterminer un facteur de réduction de risques induit par les barrières selon la correspondance suivante : pour un système de niveau de confiance NC la **réduction de risques est de manière conservative 10^{NC}** : L'évaluation du NC s'effectue de manière semi-quantitative ou qualitative à partir de la norme IEC 61511[5] relative aux SIS. L'évaluation a été étendue aux dispositifs actifs.

Mais au préalable, des critères qualitatifs doivent être pris en compte : **concept éprouvé**, **sécurité positive**, bonne **maîtrise des mises hors service des barrières**…Il faudra également s'assurer que les systèmes de sécurité font l'objet de

tests périodiques de fonctionnement et qu'ils sont correctement **maintenus**. Il faudra également en cas de modification du procédé ou des barrières s'assurer qu'une **bonne gestion des modifications** permet de maintenir les performances des barrières.

En l'absence de tests périodiques[16] et d'opérations de maintenance, la barrière sera considérée comme non performante (NC0). On se reportera au chapitre 6 pour l'analyse des critères maintenabilité et testabilité.

La prise en compte des autres critères (concept éprouvé, sécurité positive, gestion des mises hors service) est traitée de manière qualitative et nécessite une réflexion adaptée au contexte.

Les principes d'évaluation du NC des **dispositifs passifs** sont précisés **au § 5.2**.

5- Agrégation des systèmes et des fonctions de sécurité (cf. § 4.5.5, § 4.6, § 4.7)

Les performances (efficacité, temps de réponse et NC) d'un dispositif ou d'un sous-système ayant été évaluées, il faudra ensuite évaluer :

- les performances d'une BIS complète pouvant regrouper plusieurs éléments de sécurité en utilisant notamment les tableaux issus de la norme et les règles présentées au § 4.5.4.1,
- le facteur de réduction de risques induit par l'ensemble des fonctions de sécurité (regroupant éventuellement BIS, dispositifs actifs, dispositifs passifs et/ou barrières humaines) agissant sur un scénario d'accident. Le présent document ne traite pas de ces aspects qui sont abordés dans le rapport Ω Probabilités [12].

Ces évaluations doivent prendre en compte l'architecture et la présence de modes communs de défaillance.

7.2 RAPPEL DES OBJECTIFS ET DES LIMITES DE LA MÉTHODE

Il est important de préciser que la démarche présentée dans ce rapport pour évaluer le niveau de confiance ne se substitue pas aux normes IEC 61508[4] et IEC 61511[5] qui sont des références internationales dans le domaine.

L'objectif de la démarche décrite dans ce rapport est avant tout de fournir une méthode relativement simple pour évaluer la performance des barrières techniques de sécurité, applicable en groupe de travail, notamment lors de la réalisation d'analyse des risques.

Cette démarche présente une méthode d'analyse qualitative ou semi-quantitative[17] adaptée pour l'évaluation d'une classe de probabilité. Elle s'affranchit des approches quantitatives plus lourdes à mettre en œuvre.

[16] sauf pour les barrières passives qui ne font généralement pas l'objet de tests périodiques

[17] Le terme qualitatif ou semi-quantitatif s'oppose aux méthodes quantitatives basées sur les calculs de fiabilité

Il est ainsi supposé que les caractéristiques des systèmes (données relatives à la fiabilité) permettent d'assurer la contrainte quantitative. Il est supposé implicitement que les contraintes quantitatives sont assurées par la mise en œuvre des dispositifs éprouvés (avec taux de défaillance adaptés) faisant l'objet de maintenance et de tests adaptés.

Cette hypothèse peut ne pas être valable dans certaines conditions (fréquence de tests faible, taux de défaillances dangereuses élevé). Dans ces conditions, des calculs de fiabilité peuvent venir compléter l'approche qualitative ou semi-quantitative.

Si les deux approches sont développées, rappelons que le NC obtenu **sera le minimum des deux valeurs déterminées par les contraintes d'architecture et par les calculs de fiabilité**.

Les performances des installations de procédés assurant une fonction de sécurité (colonne d'abattage par exemple) ne peuvent pas être évaluées en mettant en œuvre directement la méthode OMEGA 10. Il est alors nécessaire de réaliser, en plus de l'analyse des risques associés à ces installations, une analyse des dysfonctionnements amenant ces installations à être indisponibles et à intégrer cette analyse sous forme d'une porte ET dans le nœud papillon. Il est à noter que pour que ces installations aient une meilleure disponibilité, des barrières de sécurité peuvent être mises en œuvre et évaluées selon les méthodes Omega 10 et 20.

7.3 APPLICATION AUX DISPOSITIFS DE TOUT TYPE

Les principes généraux d'évaluation qualitative restent applicables à tous les types de dispositifs (actifs, passifs, systèmes instrumentés).

Le questionnement qualitatif sur l'efficacité, le temps de réponse et le NC permettent de valider les performances et de détecter d'éventuelles faiblesses sur les barrières afin de les corriger.

Le facteur de réduction de risques évalué à partir du NC sera retenu pour les systèmes fonctionnant à la sollicitation.

8 RÉFÉRENCES

1. Loi n° 2003-699 du 30 juillet 2003 relative à la prévention des risques technologiques et naturels et à la réparation des dommages
2. Arrêté du 29/09/05 relatif à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des installations classées soumises à autorisation
3. Ω20 "Démarche d'évaluation des Barrières humaines de Sécurité" : INERIS pour le Ministère de l'Écologie et du Développement durable. Rapport disponible sur le site Internet de l'INERIS http://www.ineris.fr
4. IEC 61508 "Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité" – avril 2010
5. IEC 61511 "Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur de l'industrie de process" – février 2016
6. Guide du 2 octobre 2013 : Guide relatif aux Mesures de Maîtrise des Risques instrumentées (MMRI)
7. DT 93, juillet 2011 : Guide méthodologique pour la gestion et la maitrise du vieillissement des Mesures de Maîtrise des Risques Instrumentées (MMRI)
8. ISO 7498 "Information processing systems -- Open Systems Interconnection -- Basic Reference Model" – October 1984
9. IEC 61511-1 "Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur de l'industrie de process - Partie 1 : cadre, définitions, exigences pour le système, le matériel et le logiciel" – février 2016
10. EN ISO 13849 "Sécurité des machines – Partie des systèmes de commande relatives à la sécurité – Partie 1 : principes généraux de conception" – février 2007
11. EN 954-1 "Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1 : principes généraux de conception" – février 1997, ANNULÉE le 01/09/2012
12. Agrégation semi-quantitative des probabilités dans les études de dangers des installations classées –Ω Probabilités, DRA-14-141478-10997A du 20/10/2015
13. Layer of Protection Analysis – Simplified process risk assessment, Center for Chemical Process Safety of the American Institute of Chemical engineers, 2001
14. Circulaire du 10 mai 2010 récapitulant les règles méthodologiques applicables aux études de dangers, à l'appréciation de la démarche de réduction du risque à la source et aux plans de prévention des risques technologiques (PPRT) dans les installations classées en application de la loi du 30 juillet 2003
15. Guide de l'état de l'art sur les silos pour l'application de l'arrêté ministériel relatif aux risques présentés par les silos et les installations de stockage de céréales, de grains, de produits alimentaires ou de tout autre produit organique dégageant des poussières inflammables, Version 3 de 2008

9 LISTE DES ANNEXES

Repère	Désignation	Nombre de pages
Annexe A	Barrière Instrumentée de Sécurité	4
Annexe B	Exemples d'évaluation de sous-systèmes	10

Annexe A

Barrière Instrumentée de Sécurité

COMPOSITION D'UNE B.I.S.

Pour rappel une BIS est définie de la façon suivante dans ce rapport :

« chaîne de traitement comprenant une prise d'information (capteur, détecteur…), un système de traitement (automate, calculateur, relais…) et une action (actionneur avec ou sans intervention d'un opérateur) et des moyens de communication (analogiques, numériques, Tout Ou Rien) pour réaliser une fonction de sécurité. »

Cette définition nous précise qu'une BIS a pour mission de réaliser une fonction de sécurité (plus précisément une fonction instrumentée de sécurité - SIF).

Il faut également préciser qu'une fonction instrumentée de sécurité peut être réalisée par une ou plusieurs BIS.

1- Composition minimale d'une BIS :

Les BIS sont constituées de différents éléments unitaires reliés entre eux par des moyens de transmission. Au minimum, on retrouve en série un capteur, une unité de traitement et un actionneur qui vient commander un élément terminal (Cf. Figure 11).

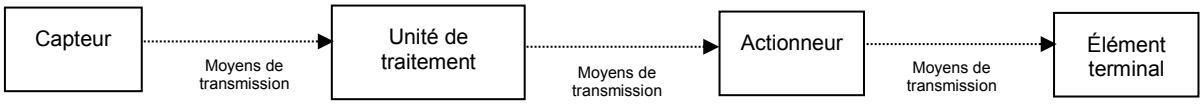


Figure 10 : Schéma d'une BIS simple

2- Composition d'une BIS en fonction des tâches à accomplir :

Une barrière de sécurité a pour finalité, en cas de sollicitation, d'accomplir un certain nombre de fonctions (isoler une capacité, arrêter les flux de produits, …) qui elles-mêmes peuvent se décomposer en tâches (fermeture de plusieurs vannes, arrêt de plusieurs machines, …). C'est dans l'optique d'accomplir toutes les tâches que l'on trouve fréquemment au sein des BIS le montage en parallèle de plusieurs actionneurs et d'éléments terminaux (cf. Figure 12).

À noter qu'un unique actionneur peut commander plusieurs éléments terminaux. Par exemple, une électrovanne trois voies située sur un réseau d'air instrument peut, par mise à l'atmosphère de ce réseau, commander la fermeture de toutes les vannes pneumatiques alimentées par le réseau.

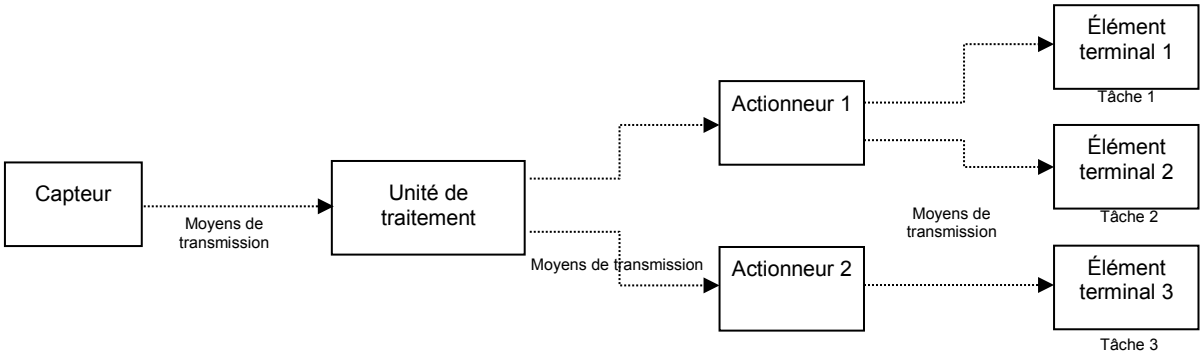


Figure 11: Schéma d'une BIS effectuant plusieurs tâches

On trouve également le montage en parallèle de plusieurs capteurs afin de répondre à un besoin de réception d'informations différentes (pression et température d'un fluide par exemple) par l'unité de traitement pour décider le déclenchement des actions de sécurité (cf. Figure 12). L'unité de traitement gère alors l'arrivée de différentes informations soit par un opérateur logique (par exemple, le déclenchement des actions de sécurité est réalisé si la température est supérieure à 100°C ou si la pression est supérieure à 10 bars), soit par calcul (par exemple, correction de l'information principale reçue par la deuxième information reçue).

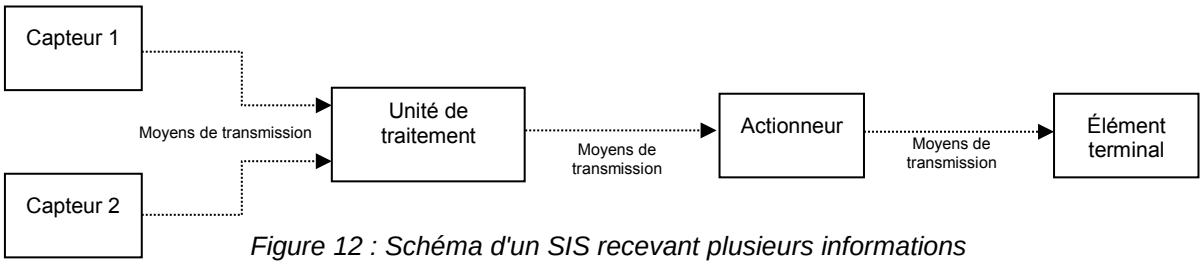


Figure 12 : Schéma d'un SIS recevant plusieurs informations

3- Redondance au sein d'une B.I.S.

Pour améliorer le niveau de confiance d'une barrière de sécurité, il est possible, entre autres, de la doubler totalement (redondance totale), ou de doubler une partie de ses composants (redondance partielle de la barrière de sécurité). À noter que la redondance peut être réalisée avec du matériel identique ou avec du matériel de technologie différente, ce dernier type de redondance permet de limiter les modes communs de défaillance.

Tous les éléments constituant une barrière de sécurité peuvent être redondés : capteurs, unité de traitement, actionneurs, éléments terminaux et même les moyens de transmission.

La figure 13 donne un exemple d'une BIS complexe, les redondances étant indiquées en rouge.

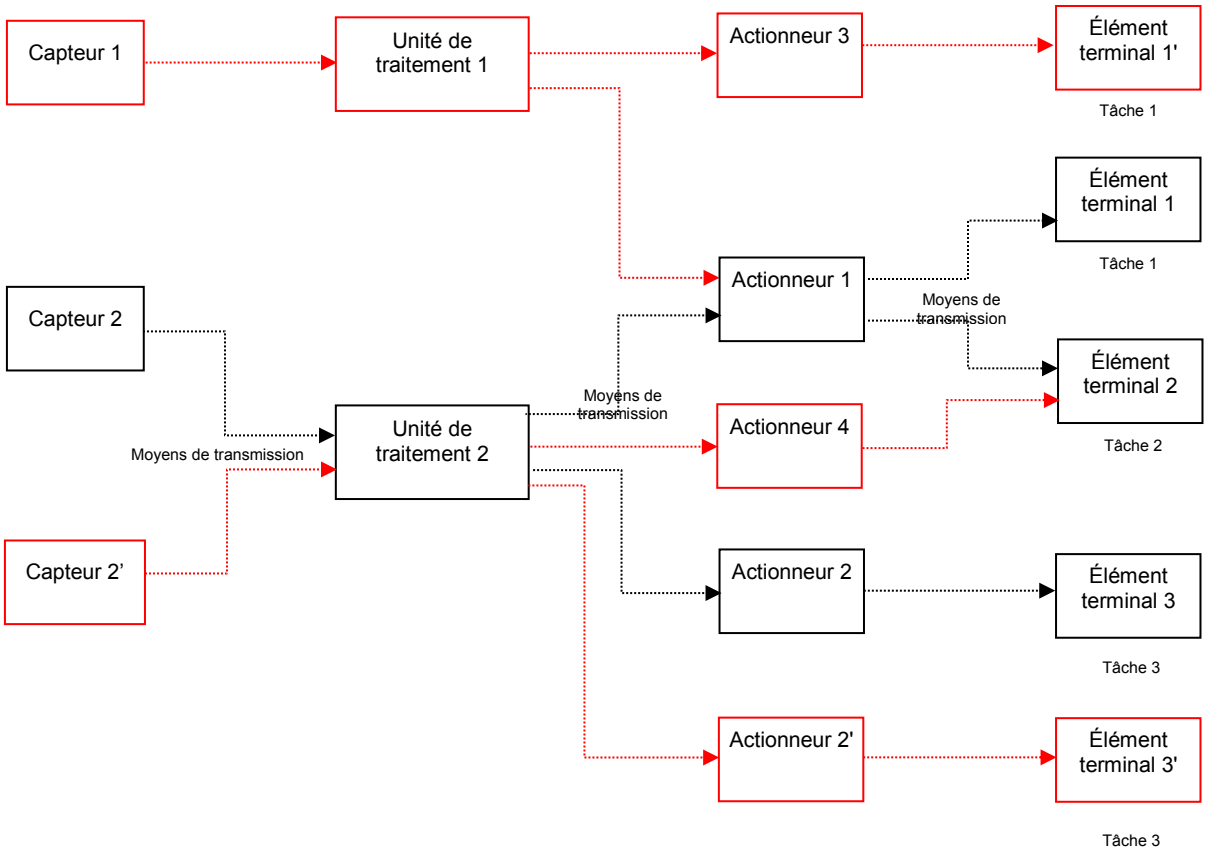


Figure 13 : Schéma d'une BIS complexe avec redondances

À noter que l'on peut distinguer plusieurs types de redondance[18] :

- **la redondance active** qui est une redondance telle que tous les moyens d'accomplir une fonction requise fonctionnent simultanément.
- **la redondance passive** qui est une redondance telle qu'une partie seulement des moyens d'accomplir une fonction requise est en fonctionnement, le reste n'étant utilisé sur sollicitation qu'en cas de défaillance de la partie en fonctionnement.
- **la redondance majoritaire m/n** qui est une redondance telle qu'une fonction n'est assurée que si au moins m des n moyens existants sont en état de fonctionner ou en fonctionnement.

[18] NF X 60-500 – terminologie relative à la fiabilité – Maintenabilité, Disponibilité - octobre 1998

Les architectures les plus souvent rencontrées relatives à ce dernier type de redondance sont les suivantes :

- **1oo1** (m=n=1) : cette architecture comprend un seul élément, et toute défaillance dangereuse de cet élément empêche le traitement correct de tout signal d'alarme valide.
- **1oo2** (m = 1 et n = 2) : cette architecture comprend deux éléments connectés en parallèle de façon que chacun puisse traiter la fonction de sécurité. Tant qu'un élément est opérationnel, la sécurité est garantie.
- **2oo2** (m = 2 et n = 2) : cette architecture comprend deux éléments connectés en parallèle de sorte qu'il est nécessaire que les deux éléments demandent la fonction de sécurité pour que celle-ci survienne. Il faut que les deux éléments soient opérationnels pour assurer la fonction de sécurité. La défaillance dangereuse d'un seul élément empêche le traitement correct de tout signal d'alarme valide.
- **2oo3** (m = 2 et n = 3) : cette architecture comprend trois éléments connectés en parallèle avec un dispositif à logique majoritaire pour les signaux de sortie de telle sorte que l'état de sortie n'est pas modifié lorsqu'un seul élément donne un résultat différent des deux autres éléments. Tant que deux éléments sont opérationnels, la sécurité est garantie. Il faudrait la défaillance dangereuse de deux éléments pour qu'un signal d'alarme valide ne soit pas traité correctement.

  Cette architecture représente aujourd'hui "l'état de l'art" quand il est recherché un bon compromis sécurité – disponibilité des outils de production.

Annexe B

Exemples d'évaluation de sous-systèmes

EXEMPLE 1 : DÉTECTEURS

Description

La fonction de sécurité de "détection" peut être assurée par différents détecteurs de paramètres physiques (pression, température, débit, concentration…). Ils sont traités ici de façon générique.

Un **détecteur** de paramètre physique est généralement constitué de 2 éléments :

- **le capteur** qui est l'élément sensible responsable de la transformation d'une information physique (pression, température, débit, concentration…) en grandeur électrique adaptée au traitement.
- et **le transmetteur** qui assure le conditionnement du signal émis par le capteur pour l'interface utilisateur. Le signal transmis peut être un signal analogique 4-20 mA, un signal numérique ou un signal de type Tout ou Rien (1/0). Dans ce dernier cas, un contact sec (relais) réalise le traitement de l'information. Le transmetteur est soit analogique, soit numérique (système avec microprocesseur ou logique programmable). Le transmetteur, suivant les cas (et ses possibilités), est connecté soit à l'entrée d'une unité de traitement, soit directement à un actionneur.

La figure suivante présente les différentes possibilités de liaisons du détecteur dans une BIS.

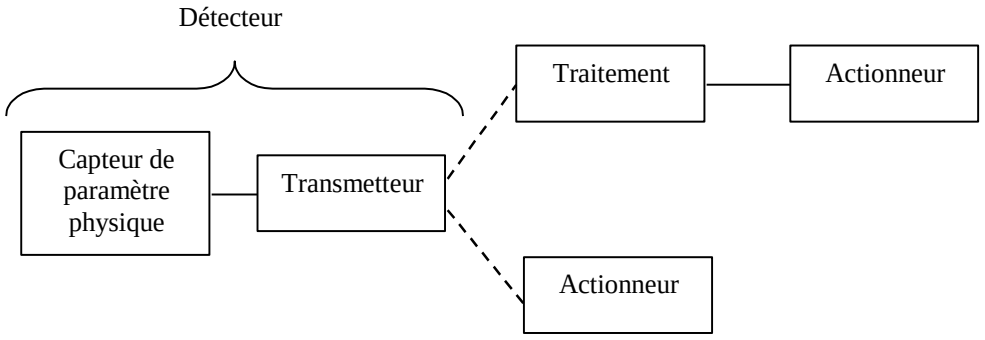


Figure 14 : Architecture depuis le capteur jusqu'à l'actionneur

Performance

Concernant l'efficacité, il est important de vérifier que le détecteur fonctionne bien dans son contexte d'utilisation (température, pression, humidité, vibrations, poussières…). Il faut également s'assurer que le paramètre physique suivi par le détecteur est exploitable pour la sécurité, donc garant de l'efficacité de la BIS dans sa globalité. Ce point rappelle l'importance de l'analyse de risques, dans laquelle sont examinées les cohérences entre dérives éventuelles et mesures de prévention / protection mises en place.

La performance des détecteurs de paramètres physiques génériques est résumée dans le tableau ci-après.

Efficacité	À étudier en fonction de l'analyse de risques
Temps de réponse	Dépendant des technologies et des paramètres mesurés, ainsi que du contexte d'utilisation : de quelques secondes à quelques minutes
Niveau de confiance	Bien que généralement paramétrables, ils sont considérés comme des éléments non programmables. Si dispositif non validé par l'usage : • NC1 dans le mode faible sollicitation • NC1 dans le mode forte sollicitation Si dispositif validé par l'usage : • NC2 dans le mode faible sollicitation • NC1 dans le mode forte sollicitation

Tableau 12 : Performance des détecteurs de paramètres physiques génériques

EXEMPLE 2 : RELAIS ÉLECTROMÉCANIQUE

Description

Schématiquement, un relais est un interrupteur électromécanique qui, excité, ferme ou ouvre un contact généralement de forte section, laissant passer ou isolant un courant. Les relais se retrouvent sur des chaînes de sécurité (les BIS).

L'alimentation de la bobine est obtenue par l'intermédiaire d'un transistor. Le champ magnétique ainsi créé ouvre ou ferme le contact, suivant sa position de repos maintenue par un ressort de rappel.

Pour une utilisation en sécurité, il faut que la position de repos du contact corresponde à l'action de sécurité. Après des cycles répétés, le contact métalliques peut se souder et empêcher l'action de sécurité.

Le schéma suivant illustre la composition d'un relais électromécanique.

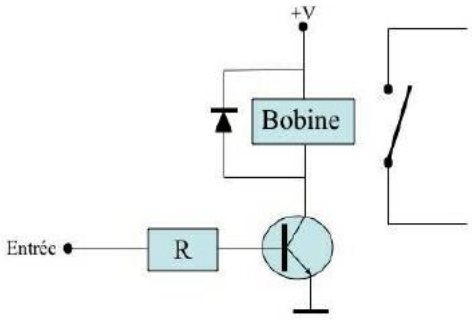


Figure 15 : Schéma d'un relais électromécanique

Performance

La performance des relais électromécaniques est résumée dans le tableau ci-après.

Efficacité	100 %, après vérification du bon dimensionnement par rapport à l'intensité susceptible de le traverser, et si le contexte d'utilisation n'a pas d'influence
Temps de réponse	Quelques dizaines de ms
Niveau de confiance	Ce sont des éléments non programmables. Si dispositif non validé par l'usage : • NC1 dans le mode faible sollicitation • NC1 dans le mode forte sollicitation Si dispositif validé par l'usage : • NC2 dans le mode faible sollicitation • NC1 dans le mode forte sollicitation après vérification que la position de repos correspond à l'action de sécurité et du bon dimensionnement par rapport à l'intensité susceptible de le traverser

EXEMPLE 3 : RELAIS DE SÉCURITÉ

Description

Un relais de sécurité a une conception basée sur la combinaison de contacts en redondance et à guidage forcé pour la commutation de sécurité (avec des contacts liés). Il est également équipé d'un circuit de surveillance pour contrôler et surveiller la position des actionneurs, qui sont commandés par les contacts de sécurité. Il a également la capacité de détecter une défaillance dans le circuit d'entrée telle que la "soudure" d'un contact ou sur l'un des contacts de sécurité du relais de sortie (autocontrôles de ses entrées et de ses sorties). Il permet également d'empêcher un réarmement automatique (redémarrage de l'appareil commandé).

Certains relais de sécurité sont assimilés à un "mini-automate de sécurité".

Performance

Les relais de sécurité sont certifiés suivant les normes IEC 61508[4] et 13849 [10]. Ces normes classent les parties de système de commande relatives à la sécurité en niveaux, de 1 à 4, 4 étant la plus élevée, 1 étant la plus faible. Les exigences permettant d'atteindre ces catégories sont basées principalement sur la sélection des composants et de leur structure (architecture) et sur la capacité à détecter des défaillances.

La performance des relais de sécurité est résumée dans le tableau ci-après.

Efficacité	100 %, après vérification du bon dimensionnement par rapport à l'intensité susceptible de le traverser, et si le contexte d'utilisation n'a pas d'influence
Temps de réponse	Quelques dizaines de ms
Niveau de confiance	Ce sont des éléments certifiés SIL. Bien que généralement paramétrables, ils sont considérés comme des éléments non programmables. NC = SIL après vérification que la position de repos correspond à l'action de sécurité et que les prescriptions de câblage et de configuration du manuel de sécurité sont respectées.

EXEMPLE 4 : LES AUTOMATES PROGRAMMABLES INDUSTRIELS (API)

Description

Un automate programmable industriel est constitué :

- d'une alimentation,
- de cartes d'entrée E (analogiques ou numériques) permettant de recueillir les informations issues des détecteurs,
- d'une unité centrale (dont fait partie le microprocesseur, la mémoire, le watchdog (chien de garde) …) qui traite les informations en entrée pour déterminer les valeurs de sortie, par l'intermédiaire de coupleurs,
- de cartes de sortie S (analogiques ou numériques) permettant de transmettre les valeurs de sortie calculées par le microprocesseur aux actionneurs.

Les API sont pour la plupart équipés d'un watchdog. Le watchdog (WD ou "chien de garde") est un élément indépendant qui surveille le microprocesseur, de façon à éviter les graves conséquences d'un "dérèglement" de celui-ci. Le watchdog permet d'augmenter la capacité de diagnostic.

La figure suivante présente schématiquement un exemple d'architecture d'API.

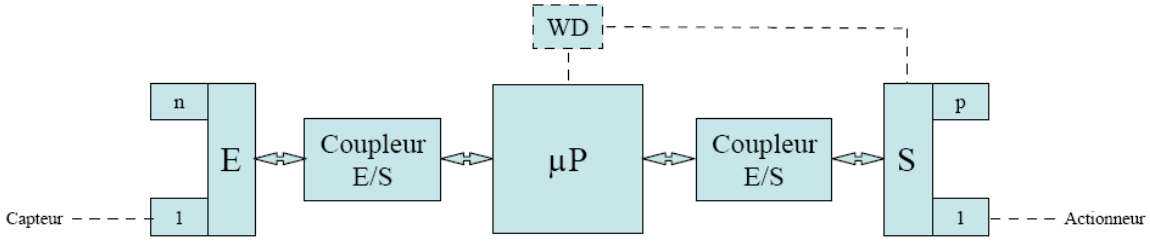


Figure 16 : Exemple d'architecture d'un API

Entre les détecteurs et les cartes d'entrée peuvent être installés des convertisseurs analogique / numérique (CAN) permettant à l'automate d'exploiter les données analogiques délivrées par les détecteurs sur des cartes d'entrée numériques.

Les seuils d'alarme sur les mesures en entrée sont généralement réglés dans l'automate, lorsque ce système de traitement de l'information est utilisé.

Ces automates sont principalement utilisés pour la conduite des process. Cependant, ils peuvent être considérés pour la sécurité, sous certaines conditions.

Performance

La performance des API est résumée dans le tableau ci-après.

Efficacité	100 %, si la validation du programme est cohérente et que le personnel chargé du développement des applications est formé aux principes de sécurité (au sens des automatismes)
Temps de réponse	Caractérisation de l'aspect temporel. Quelques dizaines à quelques centaines de ms
Niveau de confiance	Ce sont des éléments programmables et avec capacité de diagnostic (WD). De façon générale, on retient NC1 quel que soit le mode sollicitation.

Tableau 13 : Performance des API

EXEMPLE 5 : LES AUTOMATES DE SÉCURITÉ (APS)

Description

Le fonctionnement des APS est globalement identique à celui des API. Un APS se différencie d'un API au niveau de son architecture (redondance), qui permet la réalisation d'autotests, avec contrôle de cohérence sur les entrées et les sorties via une communication entre les microprocesseurs. La figure suivante présente schématiquement un exemple d'architecture d'APS (il existe des architectures différentes).

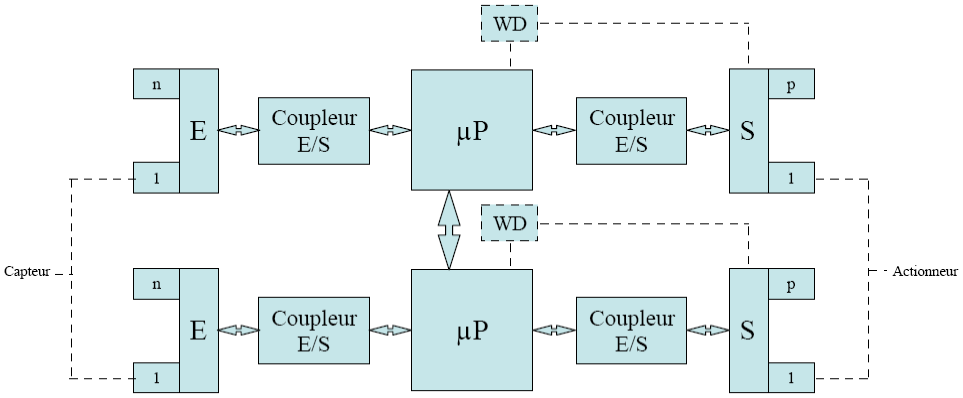


Figure 17 : Exemple d'architecture d'un APS

Performance

Un automate est déclaré "de sécurité" lorsqu'il a été certifié suivant la norme IEC 61508[4], c'est-à-dire qu'il répond aux exigences de la norme pour atteindre un certain niveau d'intégrité de sécurité, plus communément appelé SIL (Safety Integrity Level).

La performance des APS est résumée dans le tableau ci-après.

Efficacité	100 %, si la validation du programme est cohérente et que le personnel chargé du développement des applications est formé aux principes de sécurité (au sens des automatismes)
Temps de réponse	Caractérisation de l'aspect temporel. Quelques dizaines à quelques centaines de ms
Niveau de confiance	NC = SIL, après vérification du respect des architectures, du câblage et de la configuration du manuel de sécurité.

Tableau 14 : Performance des APS

EXEMPLE 6 : LES CONTACTEURS DE PUISSANCE, MOTEURS ELECTRIQUES, POMPES OU COMPRESSEURS

Description

Le système composé par un contacteur de puissance, un moteur électrique et une pompe ou un compresseur est considéré comme un actionneur.

Un contacteur de puissance est assimilable à un relais, permettant la connexion d'éléments nécessitant une puissance électrique importante. Ils sont utilisés, entre autres, pour arrêter ou mettre en fonctionnement des moteurs électriques (compresseur, pompe, …).

Performance

Concernant l'efficacité et le temps de réponse d'un tel système, il faut prendre en compte l'efficacité et le temps de réponse de chacun des 3 éléments constitutifs de ce système.

Dans le cas où la sous-fonction de sécurité a pour but de stopper un écoulement forcé (par pompe ou compresseur) de fluide, le niveau de confiance du système contacteur de puissance, moteur électrique et pompe (ou compresseur) est égal à celui du contacteur de puissance. Si, au contraire, la fonction de sécurité a pour but de créer un écoulement forcé, alors le NC du système est égal au NC le plus faible des différents éléments le constituant.

La performance des systèmes formés par un contacteur de puissance, un moteur électrique et une pompe (ou un compresseur) est résumée dans le tableau ci-après.

Efficacité	L'efficacité du système est variable en fonction des éléments utilisés et du contexte d'utilisation Pour le contacteur de puissance seul, efficacité de 100 %, après vérification du bon dimensionnement par rapport à l'intensité susceptible de le traverser, et si le contexte d'utilisation n'a pas d'influence
Temps de réponse	Variable en fonction des éléments et du contexte d'utilisation : quelques secondes à quelques minutes
Niveau de confiance	➢ Arrêt du moteur : NC système = NC du contacteur de puissance Composant non programmable et sans capacité de diagnostic : Si dispositif non validé par l'usage : • NC1 dans le mode faible sollicitation • NC1 dans le mode forte sollicitation Si dispositif validé par l'usage : • NC2 dans le mode faible sollicitation • NC1 dans le mode forte sollicitation après vérification que la position de repos correspond à l'action de sécurité

	➢ Démarrage du moteur et de la pompe (ou du compresseur, …) Si dispositif non validé par l'usage : NC_{sys} = Min ($NC_{contact}$, NC_{moteur}, NC_{pompe}) = 1 quel que soit le mode avec détection et alarme en cas de perte de l'alimentation électrique ou alimentation de secours Si dispositif validé par l'usage : NC_{sys} = Min ($NC_{contact}$, NC_{moteur}, NC_{pompe}) • NC2 dans le mode faible sollicitation • NC1 dans le mode forte sollicitation avec détection et alarme en cas de perte de l'alimentation électrique ou alimentation de secours

Tableau 15 : Performance des systèmes "contacteur de puissance, moteur électrique, pompe ou compresseur"

EXEMPLE 7 : LES VANNES MOTORISÉES

Description

Une vanne motorisée est composée d'un moteur et d'un corps de vanne muni d'un obturateur.

La motorisation est dans la plupart des cas, soit pneumatique, soit hydraulique (ou une combinaison de ces énergies motrices). Dans le cas d'une vanne de sécurité, le moteur doit être à simple effet, c'est-à-dire que la position de sécurité ("de repos" ; ouverte ou fermée, suivant la sous-fonction de sécurité à remplir) est obtenue avec un ressort de rappel lorsque l'apport d'énergie motrice cesse (sécurité positive). Le maintien de la vanne dans la position de travail ("non sécurité") est assuré par la fourniture de l'énergie motrice en permanence.

Ces vannes peuvent être classées en 2 familles, en fonction du mouvement réalisé par l'obturateur dans le corps de vanne, pour fermer ou permettre l'écoulement du fluide au travers de la vanne :

- vannes à mouvement linéaire,
- vannes à mouvement semi-rotatif de 90°.

Performance

Concernant l'efficacité, le temps de réponse et le niveau de confiance d'une vanne motorisée, il faut étudier la motorisation et le corps de vanne.

La performance des vannes motorisées est résumée dans le tableau ci-après.

Efficacité	• Position de sécurité fermée : 100 %, si le contexte d'utilisation n'a pas d'influence (essais, REX…) et que la vanne, par conception, n'est pas fuyarde en position fermée • Position de sécurité ouverte : 100 %, si le contexte d'utilisation n'a pas d'influence (essais, REX…)
Temps de réponse	Variable en fonction de l'énergie motrice et du contexte d'utilisation : quelques secondes à quelques minutes
Niveau de confiance	Si dispositif non validé par l'usage : • NC1 dans le mode faible sollicitation • NC1 dans le mode forte sollicitation Si dispositif validé par l'usage : • NC2 dans le mode faible sollicitation • NC1 dans le mode forte sollicitation

Tableau 16 : Performance des vannes motorisées

INERIS

maîtriser le risque
pour un développement durable

Institut national de l'environnement industriel et des risques

Parc Technologique Alata
BP 2 - 60550 Verneuil-en-Halatte

Tél. : +33 (0)3 44 55 66 77 - Fax : +33 (0)3 44 55 66 99

E-mail : ineris@ineris.fr - **Internet :** http://www.ineris.fr