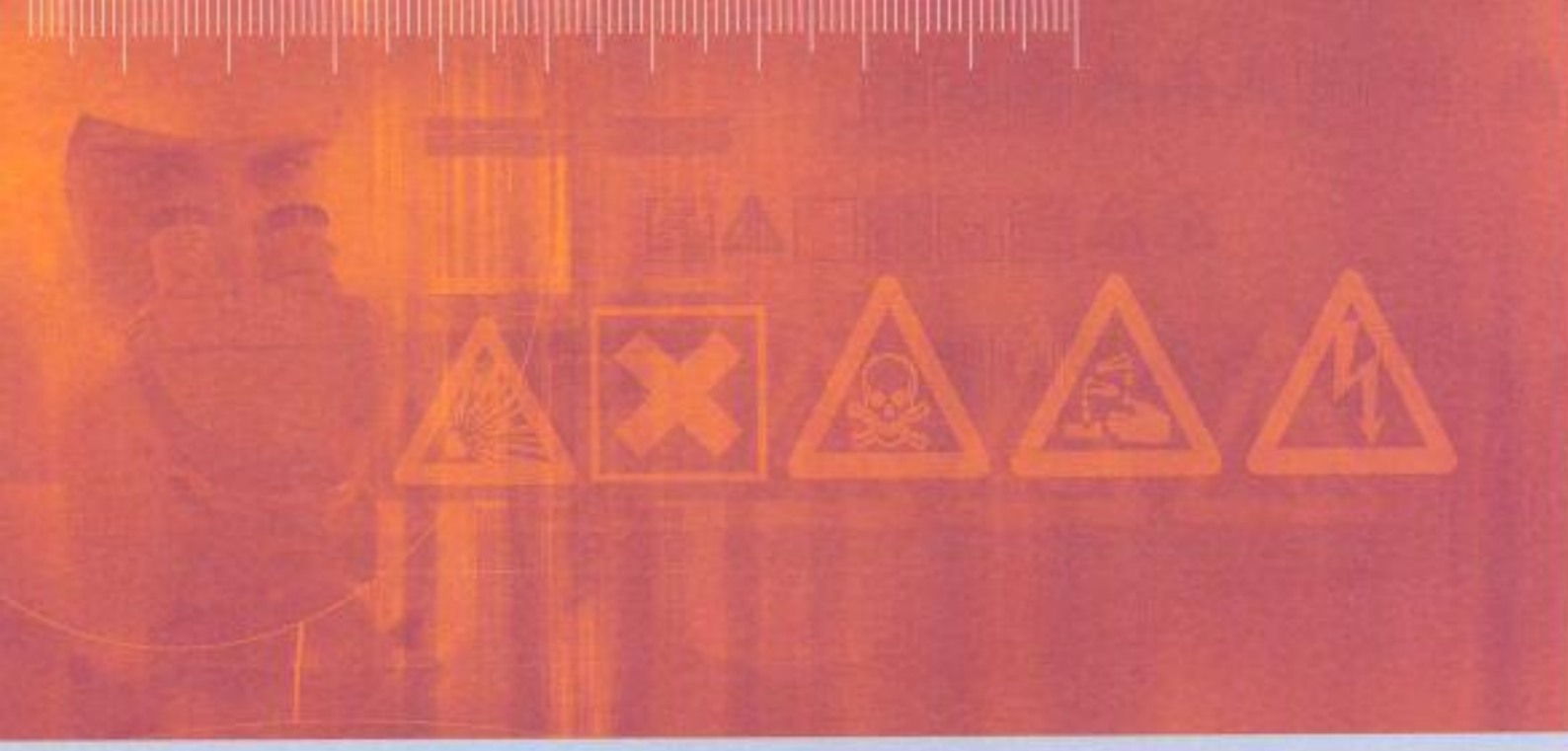


RAPPORT D'ÉTUDE 01/09/2008

N° DRA-08-95403-01561B

Evaluation des performances des Barrières Techniques de Sécurité (DCE DRA-73)

Evaluation des Barrières Techniques de Sécurité - Ω 10

INERIS

Evaluation des performances des Barrières Techniques de Sécurité (DCE DRA-73)

Evaluation des Barrières Techniques de Sécurité - Ω 10

Direction des Risques Accidentels

Unité Evaluation Quantitative des Risques

Client : **MINISTERE DE L'ECOLOGIE, DE L'ENERGIE, DU DEVELOPPEMENT DURABLE ET DE L'AMENAGEMENT DU TERRITOIRE (MEEDDAT)**

Liste des personnes ayant participé à l'étude : Nguyen Thuy LE, Ahmed ADJADJ, Sylvain CHAUMETTE, Sébastien BOUCHET, Valérie DE DIANOUS.

PREAMBULE

Le présent document a été établi :

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

Il s'agit de données et informations en vigueur à la date de l'édition du document, septembre 2008.

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

PAGE DE VALIDATION			
Evaluation des barrières techniques de sécurité			
Rédaction initiale			
Auteurs	**Qualité**	**Date**	**Emargement**
Nguyen Thuy LE et Valérie de DIANOUS	Ingénieur à l'Unité DIAG Ingénieur à l'Unité EQRI	30/09/08 01/09/08	
Dans le cadre de la procédure générale qualité de l'INERIS et en respect du paragraphe 14.2 du manuel qualité, ce document a fait l'objet de relectures et d'un contrôle par des vérificateurs.			
Relecture	**Qualité**	**Date**	**Emargement**
Christophe BOLVIN	Responsable unité EQRI	25/09/08	
Vérification finale	**Qualité**	**Date**	**Emargement**
Marie-Astrid KORDEK	Déléguée Appui à l'Administration	29/09/08	
Approbation	**Qualité**	**Date**	**Emargement**
Sylvain CHAUMETTE	Responsable du Pôle AGIR Direction des Risques Accidentels	29/09/08	

REPERTOIRE DES MODIFICATIONS

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

TABLE DES MATIERES

1 GLOSSAIRE ET DEFINITIONS

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).

Dispositif de sécurité : Elément 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.

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 NF EN 61508 et NF EN 61511.

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.

Principe de 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.....).

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.

Probabilité moyenne de défaillance par heure (PFH) : Pour un système non réparable, elle correspond à la moyenne du taux de défaillance sur un intervalle de temps donné.

Proportion de défaillances en sécurité (SFF – Safe Failure Fraction) : Proportion du taux global des défaillances aléatoires de matériel d'un dispositif qui a comme conséquence une défaillance en sécurité ou une défaillance dangereuse détectée (c'est à dire détectée par un test de diagnostic). On distingue ainsi deux types de défaillances :

- Défaillance en sécurité : Défaillance qui n'a pas la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction.
- Défaillance dangereuse : Défaillance qui a la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction.

Redondance : Existence, dans un composant, de plus d'un moyen pour accomplir une fonction requise (CEI6271-1974)

Système instrumenté de sécurité : combinaison de capteurs, d'unité de traitement et d'actionneurs (équipements de sécurité) ayant pour objectif de remplir une fonction ou sous-fonction de sécurité.

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.

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

EIReDA : European Industry Reliability Data bank

EXERA : Association des Exploitants d'Equipements de mesure, de Régulation et d'Automatisme

LOPA : Layer Of Protection Analysis

NPRD : Nonelectronic Parts Reliability Data

OREDA : Offshore Reliability Data

2 OBJECTIFS ET DOMAINE D'APPLICATION

2.1 CONTEXTE GENERAL

Depuis l'année 2000, le Ministère de l'Ecologie, de l'Energie, du Développement Durable et de l'Aménagement du Territoire (MEEDDAT) finance un programme d'appui technique, intitulé "Formalisation du savoir et des outils dans le domaine des risques majeurs" (DRA35 puis DRA76).
L'objet du premier volet de ce programme est de réaliser un recueil global formalisant l'expertise de l'INERIS dans le domaine des risques accidentels. Ce recueil évolutif sera constitué de différents rapports consacrés aux thèmes suivants :

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

Chacun de ces documents reçoit un identifiant propre du type « Ω-X » afin de faciliter le suivi des différentes versions éventuelles du document.
In fine, ces documents décrivant les méthodes pour l'évaluation et la prévention des risques accidentels, constitueront un recueil des méthodes de travail de l'INERIS dans le domaine des risques accidentels.

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

Cette nouvelle loi introduit au niveau 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 précise "pour être prises en compte dans l'évaluation de la probabilité, des mesures de maîtrise des risques doivent être efficaces, avoir une cinétique de mise en œuvre en adéquation avec celle des 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 justifier les choix de conception des équipements de sécurité mis en place sur leurs installations afin d'atteindre un niveau de risque aussi bas que possible, compte-tenu de l'état des connaissances et des pratiques et de la vulnérabilité de l'environnement de l'installation[2].

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) appelées aussi mesures de maîtrise des risques (MMR) ,
- 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.

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

Le présent document vise à présenter des principes généraux d'évaluation. Le site internet Badoris (http://www.ineris.fr/badoris) fournit des éléments d'évaluation par dispositifs de sécurité.

Seules les barrières techniques de sécurité seront abordées dans ce document. L'INERIS a développé une démarche d'évaluation analogue pour les barrières humaines de sécurité dans le rapport Ω20 « Démarche d'évaluation des Barrières Humaines de Sécurité » [1].

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 NF-EN 61508[2] **(sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité) et NF EN 61511**[3] **(Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur de l'industrie de process), qui sont des références internationales dans le domaine.**

[2] Circulaire du 29 septembre 2005 relative aux critères d'appréciation de la démarche de maîtrise des risques d'accidents susceptibles de survenir dans les établissements dits « SEVESO », visés par l'arrêté du 10 mai 2000 modifié.

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[3].

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.

Cette démarche présente une méthode d'analyse qualitative[4] et semi-quantitative[5] 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 peu disponibles. On se reportera au paragraphe 7.2 pour les limites d'utilisation de l'approche décrite dans ce rapport.

La démarche proposée découle de travaux menés dans le cadre de programmes d'appui technique financés par le Ministère de l'Ecologie, de l'Energie, du Développement Durable et de l'Aménagement du Territoire, à savoir les programmes DRA71, DCE-DRA73 et DRA76.

Ce document intègre certains éléments développés dans le document « Evaluation du niveau de confiance d'un équipement IPS dans une installation » INERIS-DCE-LEEL-AAD/JM-03.

Ce rapport a été rédigé avec l'aide des documents suivants :

- Rapport Ω10 réalisé dans le cadre du DRA-39 – Evaluation des Barrières Techniques de sécurité – N. AYRAULT – février 2005,
- Rapport réalisé dans le cadre du DRA-39 - Guide principal relatif à l'évaluation des Barrières Techniques de Sécurité pour l'inspection des installations classées – S. BOUCHET – juin 2005,
- Méthodologie d'évaluation d'un dispositif de sécurité dans une installation industrielle – A. ADJADJ et F. MASSE - INERIS-DCE-LEEL/75014-01- avril 2006.

---

[3] 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 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 mise en œuvre et évaluées selon les méthodes Omega 10 et 20.

[4] Les normes NF EN 61508 et NF EN 61511 comportent d'autres éléments de nature qualitative, qui peuvent prendre la forme de prescriptions ou d'exigences en terme d'état de l'art).

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

2.4 ORGANISATION DU DOCUMENT

Le rapport est organisé de la façon suivante :

- Chapitre 1: glossaire et définitions
- Chapitre 2 : objectifs et domaine d'application
- Chapitre 3 : types de barrières techniques de sécurité
- Chapitre 4 : évaluation des barrières techniques de sécurité – dispositifs actifs et systèmes instrumentés de sécurité
- Chapitre 5 : évaluation des dispositifs et barrières passives
- Chapitre 6 : évolution des performances dans le temps (maintenance et tests)
- Chapitre 7 : synthèse de l'évaluation des BTS
- Chapitre 8 : références
- Chapitre 9 : liste des annexes

3 TYPES DE BARRIERES TECHNIQUES DE SECURITE

Les barrières de sécurité (ou mesures de maîtrise des risques) sont de trois types :

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

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

Note : la bonne conception des installations ainsi 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.

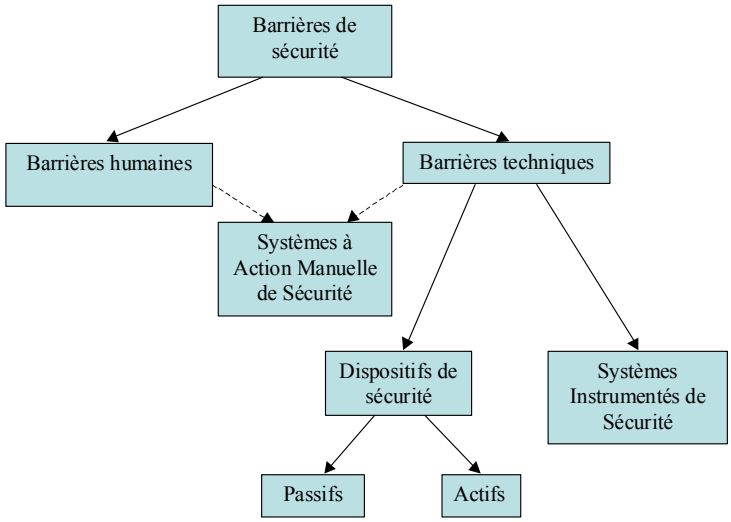


Figure 1 : typologie des Barrières Techniques de Sécurité

3.1 DISPOSITIFS DE SECURITE

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. Ils peuvent nécessiter une source d'énergie externe pour fonctionner.

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[6] dans sa globalité. Il faut une action humaine et/ou une source d'énergie externe (cf. § 3.2 - SIS) 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	Toit flottant de bacs
Double clapet de rupture	Murs coupe-feu sans ouverture
Clapet excès de débit	Talus de réservoirs
Events de respiration de bacs avec ressorts	Events de respiration de bacs sans ressort
	Arrête-flamme
	Ignifugeage
	Disque de rupture
	Cuvette de rétention
	Ecrans de protection mécanique ou thermique
	Réducteur de débit sans ressort

Tableau 1 : : exemples de dispositifs actifs et passifs

3.2 SYSTEMES INSTRUMENTES DE SECURITE (SIS)

Les systèmes instrumentés de sécurité sont des combinaisons de capteurs, d'unité de traitement et d'actionneurs (équipements de sécurité) ayant pour objectif de remplir une fonction ou sous-fonction de sécurité[7]. Un S.I.S. nécessite une énergie extérieure pour initier ses composants et mener à bien sa fonction de sécurité.

La figure page suivante montre une représentation schématique générique d'un SIS.

[6] Cf. glossaire § 1

[7] Une fonction de sécurité peut se décomposer en plusieurs sous-fonctions de sécurité liées.

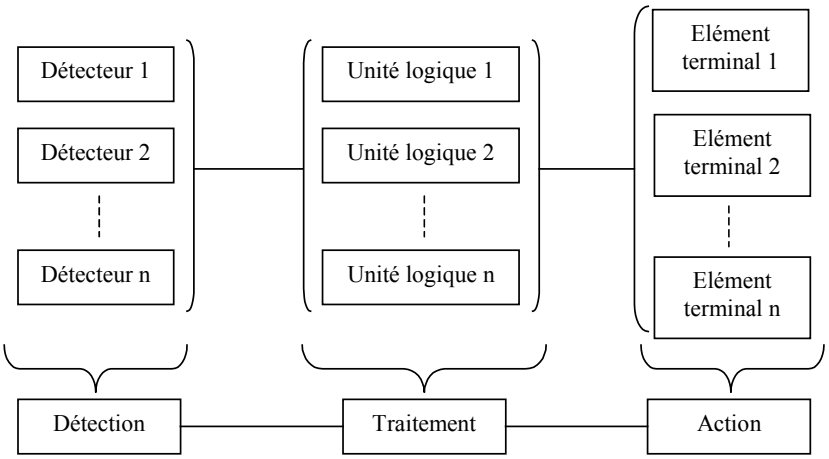


Figure 2 : schéma générique d'un SIS

Dans ce schéma, trois sous-fonctions composent un SIS : il s'agit des sous-fonctions « détection », « traitement de l'information» et « action ».

3.2.1 SOUS-FONCTION DE SECURITE "DETECTION"

Cette sous-fonction de sécurité peut être assurée par différents détecteurs de paramètres (pression, température, débit, concentration…). Ils sont traités ici de façon générique.

Un **détecteur** de paramètre 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. Le capteur ne fait pas intervenir de microprocesseurs.
- 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 ou un signal de type binaire 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 un SIS.

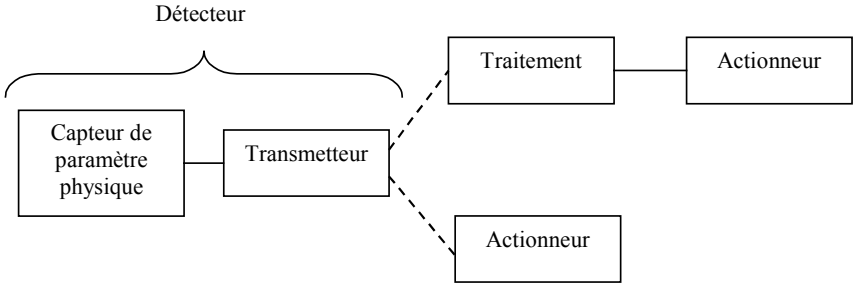


Figure 3 : architecture depuis le capteur jusqu'à l'actionneur

3.2.2 SOUS-FONCTION DE SECURITE "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 **unités de traitement** peuvent être classées en deux catégories selon leur technologie :

- Les technologies câblées, à base de composants logiques élémentaires (relais), liés entre eux électriquement (ou de manière pneumatique ou hydraulique).
- Les technologies programmées, à base de centrales d'acquisition ou d'alarmes, d'automates programmables (API) dont certains peuvent être dédiés à la sécurité (APIdS), de calculateurs industriels ou de cartes électroniques à microprocesseurs et/ou à logique programmable.

Le choix d'une technologie 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.

3.2.3 SOUS-FONCTION DE SECURITE "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 partiellement ou totalement par le SIS réside d'une part dans la détection du phénomène dangereux et d'autre part dans la mise en position finale de sécurité de ces éléments (ouvert/fermé, arrêt/démarrage). Le SIS pourra assurer la fonction totalement (détection, traitement, action finale) ou partiellement (le SIS assure par exemple la fonction de détection et de traitement jusqu'à une alarme, l'action finale peut ensuite être réalisée par une action humaine).

3.2.4 COMMUNICATIONS ENTRE LES ELEMENTS D'UN SIS

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 hertzienne), de fibres optiques (bus de terrain) ou de tuyauteries (transmissions pneumatique ou hydraulique).

3.3 SYSTEME A ACTION MANUELLE DE SECURITE

Les systèmes 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 un système à action manuelle de sécurité.

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 [1] relatif à la démarche d'évaluation des Barrières humaines de Sécurité.

4 EVALUATION DES BARRIERES TECHNIQUES DE SECURITE – DISPOSITIFS ACTIFS ET SYSTEMES INSTRUMENTES DE SECURITE

4.1 RAPPEL SUCCINCT DE L'APPROCHE BARRIERE

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 des phénomènes dangereux est listé.

Pour être retenues dans l'évaluation des probabilités d'occurrence des phénomènes dangereux, les barrières de sécurité doivent 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, si la barrière de sécurité peut être retenue pour le scénario étudié, puis à attribuer un facteur de réduction de risque aux barrières de sécurité retenues. 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 dont les intensités seront liées aux performances des barrières.

4.2 IDENTIFICATION DES BARRIERES TECHNIQUES DE SECURITE : CRITERES MINIMAUX

Avant d'étudier en détail les performances des Barrières Techniques de Sécurité (BTS), il faut en premier lieu s'assurer du respect des critères minimaux. Ces critères sont les suivants :

- **indépendance** : 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.

  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.

- **utilisation pour la sécurité** : a minima, le descriptif technique de la BTS doit préciser qu'elle est conçue pour une utilisation en sécurité. Elle doit présenter un certain nombre de caractéristiques (par exemple : conception simple, robustesse).

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 CRITERE EFFICACITE.

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.

Dans beaucoup de situations, 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 au fonctionnement du rideau d'eau 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 au fonctionnement de la vanne 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 associé au fonctionnement de la barrière. Ainsi :

- Un temps de fermeture d'une vanne de 30 secondes conduira ainsi à un rejet dangereux.
- 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 :

- 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 ;
- établir les scénarios de référence vis-à-vis desquels la barrière a été dimensionnée ;
- 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...), 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 ADAPTE :

L'équipement est dit satisfaire au principe de dimensionnement adapté lorsqu'il est conçu sur la base de normes et standards reconnus et lorsque le dimensionnement est réalisé sur la base de conditions de fonctionnement adaptées au site. Son dimensionnement doit également tenir compte des événements redoutés à maîtriser et doit répondre à un cahier des charges spécifique.

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 :

- Existe-t-il des notes de calcul, des études spécifiques sur le dimensionnement de la BTS ?
- 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, notamment pour les colonnes d'abattage, les cuvettes de rétention…
- Des essais ont-ils été réalisés (in situ, en laboratoire) ?

- Quel est le retour d'expérience sur l'utilisation de ce dispositif ?
- 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 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 ?
- Existe-t-il des normes ou des standards professionnels concernant cette barrière?

4.3.2 PRINCIPE DE RESISTANCE AUX CONTRAINTES SPECIFIQUES :

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 (produit, exploitation, environnement…) en situation normale et en situation dégradée du fait de l'accident ?
- 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 ?

4.3.3 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.

On note que le positionnement et l'accessibilité de la barrière interviennent également dans la réalisation des opérations de maintenance, de contrôle, de tests, d'étalonnage…qui ont une influence sur ses performances.

4.4 CRITERE TEMPS DE REPONSE

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 de l'information à la ou les barrières de sécurité devant remplir la fonction 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. Mais 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 précautions en comparant les conditions de détermination des temps de réponse avec les conditions réelles d'utilisation. D'autre part, il est à noter que, comme le montrent les résultats statistiques d'une étude de l'EXERA[8] (cf annexe A), il faut être prudent avec les performances annoncées des dispositifs de sécurité par les fabricants. En effet, selon les essais que l'EXERA a menés sur 107 matériels en 5 ans, seulement un sur deux répondait globalement à l'ensemble des spécifications annoncées.

Ainsi, hormis un solide retour d'expérience, les 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 ou du fait de l'industriel, 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 significativement 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.

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.

[8] EXERA: Association des Exploitants d'Equipements de Mesure, de Régulation et d'Automatisme

4.5 NIVEAU DE CONFIANCE

4.5.1 FACTEUR DE REDUCTION DE RISQUES

- **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}.

Dans une approche semi-quantifiée, si l'évènement initiateur a une fréquence de $10^{-X/an}$ et que le niveau de confiance de la barrière est NC correspondant de manière conservatrice à un facteur de réduction de risques de 10^{NC}, la fréquence d'occurrence de l'évènement est alors de $10^{-(X+NC)}$.

A 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**.

Il peut exister un deuxième événement correspondant au bon fonctionnement de la barrière avec des intensités d'effet plus faibles (par exemple barrières de limitation, soupapes) mais avec une probabilité légèrement inférieure à celle de l'événement initiateur (mais ayant la même classe de probabilité).

Le principe d'allocation d'un NC à une BTS est explicité au paragraphe 4.5.4.

Mais une analyse qualitative de la BTS préalable est nécessaire. Les éléments faisant l'objet de l'analyse sont précisés au paragraphe 4.5.3.

- **Principe de la méthode d'allocation des NC et extrapolation aux autres barrières**

Les tableaux des normes NF EN 61508 et NF EN 61511 permettent d'attribuer un NC pour les **systèmes instrumentés de sécurité**. Ainsi, le type de systèmes définit, en fonction de l'architecture et de la proportion de défaillances en sécurité (SFF), le NC attendu. Puis le NC est ensuite directement corrélé avec le facteur de réduction de risques.

L'INERIS a étendu ces principes aux **dispositifs actifs** (soupapes par exemple). Pour les **dispositifs passifs**, l'évaluation du NC repose sur des principes différents qui sont détaillés chapitre 5.

- **Lien avec les paramètres des normes NF EN 61508 et NF EN61511**

La norme NF EN 61511-1 présente des tableaux faisant le lien entre les diverses caractéristiques des systèmes (SIL, PFD_{avg} ou PFH).

Ils font apparaître deux types de systèmes :

- **Ceux fonctionnant à la sollicitation** : une fonction de sécurité a un mode de fonctionnement de type à la sollicitation (au sens de la norme) "lorsqu'une action spécifiée (par exemple une fermeture de vanne) est effectuée en réponse aux conditions du processus ou à d'autres sollicitations."

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

- **Ceux fonctionnant en mode continu** : une fonction de sécurité a un mode de fonctionnement en mode continu (au sens de la norme) "lorsqu'en cas de défaillance de la fonction instrumentée de sécurité, un danger potentiel apparaît, sans autre défaillance, sauf si une action est entreprise pour le prévenir."

  Le SIL est alors relié au PFH du système.

On s'intéresse dans le cadre de ce rapport aux systèmes fonctionnant à la sollicitation, pour lesquels on cherche à évaluer des facteurs de réduction de risques.

Le tableau issu de la norme NF EN 61511-1 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 :

Niveau de confiance (NC)	Probabilité moyenne de défaillance à la sollicitation (PFD_{avg})	Réduction du risque (RR)
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	$10\,000 < RR \leq 100\,000$
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	$1\,000 < RR \leq 10\,000$
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	$100 < RR \leq 1\,000$
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	$10 < RR \leq 100$
0	$10^{-1} \leq PFDavg < 1$	$1 < RR \leq 10$

Tableau 2 : correspondance Niveau de confiance – réduction du risque pour des systèmes fonctionnant à la sollicitation

4.5.2 JUSTIFICATION DE LA METHODE

- **Les normes NF EN 61508 et NF EN 61511 à la base de la méthode**

Le NC est issu[9] des SIL (Safety Integrity Level) tels que définis dans les normes NF EN 61508 (pour les systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité) et NF EN 61511 (pour les systèmes instrumentés de sécurité pour le secteur des industries de transformation).

L'INERIS a étendu la notion de NC à tout type de dispositif.

On note que la norme NF EN 61511 relative aux systèmes instrumentés de sécurité concerne les systèmes instrumentés de sécurité qui sont basés sur l'utilisation d'une technologie électrique / électronique / électronique programmable. Cependant, il est précisé dans la norme qu'elle concerne également les capteurs et les éléments terminaux des SIS, quelle que soit leur technologie.

Dans les normes NF EN 61508 et 61511, 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 de fiabilité permettent de déterminer les paramètres liés à la fiabilité (Probabilité moyenne de défaillance PFD_{avg} et taux de défaillance instantané PFH) 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.

L'INERIS retient, dans sa démarche explicitée dans le présent rapport, les aspects qualitatifs[10]. Il est ainsi supposé que les caractéristiques des systèmes (données relatives à la fiabilité) permettent d'assurer la contrainte quantitative[11]. Cette hypothèse peut ne pas être valable dans certaines conditions (fréquence de tests faible, SFF très élevée pouvant conduire dans un 1er temps à un SIL élevé par la contrainte architecturale, taux de défaillances dangereuses élevé).

- **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 a 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 de la certification du dispositif soient les mêmes que celles d'utilisation du dispositif sur site.

---

[9] Le NC répond à des attentes d'évaluation simples en vue de la réalisation d'études de dangers. La certification du niveau SIL selon la norme NF EN 61508 est une démarche différente.

[10] Le terme qualitatif s'oppose aux méthodes quantitatives basées sur les calculs de fiabilité.

[11] 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.

4.5.3 ANALYSE PRELIMINAIRE QUALITATIVE POUR LES SIS 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 EPROUVE

Un dispositif utilisé à des fins de sécurité devra satisfaire au principe de concept éprouvé. Il faudra donc qu'il réponde pour cela aux exigences suivantes:

- soit l'équipement a subit des tests de qualification pour un usage précis correspondant au contexte de mise en place sur site. Ces tests sont réalisés par l'utilisateur ou par d'autres organismes compétents.
- soit il est utilisé depuis plusieurs années sur des sites industriels et le retour d'expérience est bon. La qualité du retour d'expérience 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.
  - l'accidentologie sur des installations similaires (retour d'expérience des accidents, des incidents et des presqu'accidents),
  - les standards ou normes indiqués par les syndicats professionnels ou les réglementations nationales et/ou internationales.

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. A défaut, on pourra envisager des tests sur le dispositif planifiés avec des fréquences plus importantes que celles définies pour des dispositifs de concept éprouvé. Un suivi rigoureux des performances devra être réalisé.

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, taux de sollicitation, etc).

4.5.3.2 PRINCIPE DE SECURITE POSITIVE

Dans ce rapport, un équipement est défini à **sécurité positive** lorsqu'une perte du fluide moteur ou des utilités (réseau pneumatique ou hydraulique), conduit l'équipement à se mettre en situation sécuritaire stable ; la position de sécurité doit être maintenue dans le temps. Ce principe est également connu sous le nom de sécurité à manque.

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).

Si une BTS n'est pas à sécurité positive alors que cette disposition est pertinente et applicable pour une utilisation en sécurité, elle ne sera pas retenue.

Le principe de sécurité positive ne s'applique pas à tous les dispositifs (par exemple, la soupape de sécurité).

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). On s'interrogera alors sur la fiabilisation de l'alimentation électrique et la nécessité dans les cas extrêmes d'avoir recours à des secours d'alimentation de type groupe Diesel, batteries….

Pour certains dispositifs tels que les détecteurs, les vannes disposées sur des procédés ne tolérant pas d'arrêt, des sous-systèmes redondants, le principe pourra être assoupli[12] dans le sens où une coupure ou un court-circuit de la ligne d'alimentation et/ou de communication pourra ne pas déclencher automatiquement la mise en sécurité des installations mais devra, dans ce cas, entraîner une **alarme** (dans les délais compatibles avec la sécurité) **suivie d'une action humaine dans des délais compatibles avec la sécurité**. En cas de perte de fluide moteur ou des utilités, le maintien en position de la vanne pourra être retenu. On cherchera là encore dans ses situations à privilégier la qualité de l'alimentation électrique ou des utilités.

Concernant ce principe, 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 ?

---

[12] On notera que la norme NF EN 61511 exige effectivement que le mode de défaillance dominant d'un sous-système autre qu'une unité logique à électronique programmable soit **à un état de sécurité ou que les défaillances dangereuses soient détectées** (et suivies de l'action adéquate) pour attribuer un NC 1 à un tel sous-système en absence de redondance.

4.5.3.3 MISE HORS SERVICE DE LA BARRIERE - GESTION DES SHUNTS

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

- **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…).
- **La mise hors service peut se produire à la suite d'une action volontaire de by-pass**. Des by-pass des systèmes de sécurité sont en effet possibles sur les sites pour différentes raisons :
  - la réalisation de certains essais : si le procédé ne tolère pas de fermeture de vanne, un by-pass de l'électrovanne sera réalisé pour éviter la fermeture de la vanne ; le démarrage de groupes Diesel pourra se faire en choisissant une position "manuelle" pour le démarrage des groupes…
  - la marche dégradée en cas de défaillance d'un dispositif : si un détecteur est défaillant, il sera déconnecté de la boucle de sécurité le temps de réaliser les interventions nécessaires à sa réparation…

  Le by-pass des équipements de sécurité devra se faire en respectant des procédures de marche dégradée définies sur le site, en mettant en place des moyens compensatoires et des mesures permettant de limiter et contrôler le temps de mise en place du by-pass.

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 facilement 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

- **Détermination des NC des SIS**

L'évaluation semi-quantitative proposée par l'INERIS qui permet d'attribuer un NC aux SIS à partir de leur architecture s'appuie sur les tableaux des normes NF EN 61508-2 et NF EN 61511. Ces tableaux définissent des contraintes d'architecture pour les différents sous-systèmes relatifs à la sécurité.

Plusieurs paramètres interviennent :

- **<u>la proportion de défaillances en sécurité (SFF pour Safe Failure Fraction)</u>** est le rapport de la somme du taux de défaillances sûres et du taux de défaillances dangereuses détectées sur la somme des taux de défaillances du système. L'estimation de ce paramètre est difficile à réaliser; elle nécessite des études spécifiques telles que l'AMDE ainsi que des données de fiabilité. De ce fait, **par défaut, et sauf cas particuliers (données précises, présence d'un watchdog**[13] **sur un système programmable), l'INERIS considère alors dans ses évaluations que la proportion de défaillance en sécurité est inférieure à 60 %**[14]. Si des études spécifiques attestent des proportions de défaillance en sécurité plus élevées que celles retenues par défaut, alors elles peuvent être utilisées pour la détermination du SFF.

On a : $$SFF = \frac{\sum \lambda_T - \sum \lambda_{DU}}{\sum \lambda_T}$$

Avec : λ_T : Taux de défaillances total

λ_{DU} : Taux de défaillances dangereuses non détectées

- <u>La tolérance aux anomalies matérielles</u> 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 du système instrumenté, 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.

---

13 **"Watchdog"** *(Chien de garde)* **ou autocontrôle :** les automates de sécurité surveillent en permanence le cycle de traitement des informations et l'exécution des tâches, et interviennent si le temps d'un cycle n'est pas conforme à celui déterminé par l'utilisateur. Ceci permet d'assurer la stabilité du système, en évitant des cycles processeur trop longs correspondant à un état de blocage.

14 Le **taux inférieur à 60%** est la classe de SFF la plus conservatrice retenue dans la norme NF EN 61508-2 (cf page 32).

- Le type de sous-systèmes : **simple ou complexe**.

  De manière simplifiée, l'INERIS retient pour les **systèmes simples** les systèmes **sans microprocesseurs ou logiciels** et pour les **systèmes complexes** ceux **avec microprocesseurs ou logiciels**. Les systèmes dits simples ou complexes sont rattachés respectivement aux systèmes de type A ou B (tels que définis dans la norme NF EN 61508-2) et aux systèmes de type unités logiques de l'électronique programmable ou aux autres sous-systèmes (tels que définis dans la norme NF EN 61511-1).

  On pourra pour plus de détails se reporter à l'annexe C qui établit le lien entre les dénominations de systèmes simples et complexes et les termes employés dans les normes NF EN 61508 et NF EN 61511.

En fonction des trois paramètres définis précédemment, les tableaux de la norme **NF EN 61508-2** présentent donc les **SIL maximums** en fonction des SFF et des tolérances aux anomalies matérielles. Les tableaux issus de la norme (dans lesquels SIL a été remplacé par NC) sont les suivants :

Proportion de défaillances en sécurité (SFF)	Tolérances aux anomalies matérielles		
	0	1	2
< 60%	NC 1	NC 2	NC 3
60% à <90%	NC 2	NC 3	NC 4
90% à <99%	NC 3	NC 4	NC 4
≥99%	NC 3	NC 4	NC 4

Tableau 3 : contraintes architecturales sur les sous-systèmes de type A (simple)

Proportion de défaillances en sécurité (SFF)	Tolérances aux anomalies matérielles		
	0	1	2
< 60%	Non autorisé	NC 1	NC 2
60% à <90%	NC 1	NC 2	NC 3
90% à <99%	NC 2	NC 3	NC 4
≥99%	NC 3	NC 4	NC 4

Tableau 4 : contraintes architecturales sur les sous-systèmes de type B (complexe)

La norme NF EN 61511 propose le même type de tableau que le Tableau 4 pour les systèmes complexes.

Pour les **systèmes simples (exemple de capteurs, éléments terminaux et unités logiques autres qu'électroniques programmables)**, le tableau des tolérances aux anomalies matérielles est à première vue plus simple que celui des types A de la norme 61508, dans la mesure où il ne fait plus mention des SFF. Mais les conditions associées au tableau permettent de traiter les cas supplémentaires.

NC	Tolérance minimale aux anomalies du matériel (voir conditions)
1	0
2	1
3	2
4	Les exigences spéciales s'appliquent – voir la CEI 61508

Tableau 5 : tolérance minimale aux anomalies du matériel (soit nombre d'anomalies matérielles tolérées sans remise en cause de la fonction de sécurité) pour les capteurs, les éléments terminaux et les unités logiques non PE (simples)

Le tableau s'applique sous conditions. Les conditions définies dans le Tableau 5 sont les suivantes :

- Pour que la tolérance aux anomalies de matériel soit celle indiquée dans le tableau, il faut que le mode de défaillance dominant soit à un état de sécurité ou que les défaillances dangereuses soient détectées (et suivies de l'action adéquate), faisant ainsi référence au critère de **sécurité positive** (cf § 4.5.3.2). Sinon, la tolérance aux anomalies de matériel doit être augmentée de 1.
- Au contraire, la tolérance aux anomalies de matériel peut être réduite de 1 si les quatre conditions suivantes sont réunies :
    - S'il peut être prouvé par une utilisation antérieure que le dispositif est apte à être utilisé dans les systèmes instrumentés de sécurité ;
    - Si le dispositif ne permet que le réglage des paramètres relatifs au processus (gamme de mesure…)
    - Si le réglage des paramètres relatif au processus du dispositif est protégé (par mot de passe, cavalier…) ;
    - Si la fonction a une prescription de SIL inférieure à 4.

  Il est précisé d'autre part que si une évaluation est faite selon les normes 61508, la tolérance aux anomalies matérielles peut être celle définie dans les tableaux de la norme 61508-2.

  Par exemple, si on considère un élément terminal unique tel qu'une vanne :

  - le NC de la vanne pourra être pris égal à NC1 si la vanne est à sécurité positive.
  - Le NC pourra être pris égal à 2, même en l'absence de redondance, si la vanne bénéficie d'un retour d'expérience adéquat et que le réglage des paramètres ne peut pas être modifié accidentellement.

4.5.5 EVALUATION DES NC DES SYSTEMES A PARTIR DE DONNEES UNITAIRES – CAS DES DISPOSITIFS ACTIFS ET SIS

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 chapitre 4.5.4.

Puis on réalise les agrégations des NC des différents sous-systèmes selon les règles suivantes proposées par l'INERIS.

4.5.5.1 EVALUATION DES NC UNITAIRES

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

Si une BTS ou un élément de BTS a été certifié suivant la norme NF-EN 61508, et possède donc un SIL, alors le NC retenu équivaut au SIL, **à la condition expresse que l'exploitant suive rigoureusement le cahier des charges fourni (installation, raccordement, configuration, maintenance…)**. Le niveau de confiance d'un équipement certifié SIL3 peut ainsi être de "3". C'est notamment le cas des automates de sécurité qui sont certifiés suivant cette norme, pour une architecture donnée en entrée et en sortie compatible avec le SIL3.

Règle n°2 : NC unitaire maxi 3

Les technologies et connaissances actuelles ne permettent pas d'atteindre un NC de 4 pour un composant de sécurité quel que soit le système, en absence de redondance. En effet pour une tolérance à la défaillance de 0, le NC ne dépasse pas 3, même pour un système de type A (simple).

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 5 paragraphe 4.5.4.

4.5.5.2 EVALUATION DES SIS OU SYSTEMES COMPLETS

Pour des SIS composés de différents sous-systèmes, les règles suivantes seront appliquées.

Note : Les règles ne sont pas définies pour la prise en compte de différentes fonctions instrumentées agissant sur un même scénario d'accident ou pour des fonctions instrumentées de sécurité agissant en parallèle à des dispositifs techniques (actifs et/ou passifs) ou humains.

Règle n°4 : éléments en parallèle d'un SIS : principe d'agrégation et NC3 maxi

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. Un sous-système en parallèle à un autre conduira à une tolérance à la défaillance supplémentaire et permettra d'augmenter le NC du système.

Mais même en présence de redondance, l'attribution d'un NC de 4 à un SIS unique n'est pas réaliste actuellement car il supposerait des contraintes importantes. Comme le précise la norme NF EN 61511-1. "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 de sécurité. Dans les cas où de tels systèmes sont spécifiés, toutes les personnes qui sont impliquées dans le cycle de vie de sécurité devront avoir des niveaux de compétence élevés". **On retient donc un NC maxi de 3.**

L'évaluation du NC de la fonction sera complétée d'une analyse sur les modes communs de défaillance.

Règle n°5 : éléments en série

Pour des sous-systèmes en série (cas des parties détection, traitement et action d'un système instrumenté 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 trouvait en série (ce qui est peu probable), le NC du système devrait être réduit de 1.

4.5.5.3 EXEMPLE D'EVALUATION

Un exemple d'illustration de l'application des règles n°4 et n°5 est fourni ci-dessous. Il est directement issu de la norme NF EN 61508-2 : les SIL ont simplement été remplacés par les NC.

On suppose une architecture dans laquelle une fonction de sécurité particulière est réalisée soit par une combinaison des sous-systèmes 1, 2 et 3, soit par une combinaison des sous-systèmes 4, 5 et 3, comme illustré sur la figure 4. Les éléments sont du type A (simple) ou du type B (complexe). 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 et contribuent indépendamment à fournir des données au sous-système 3.

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**[15] 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).

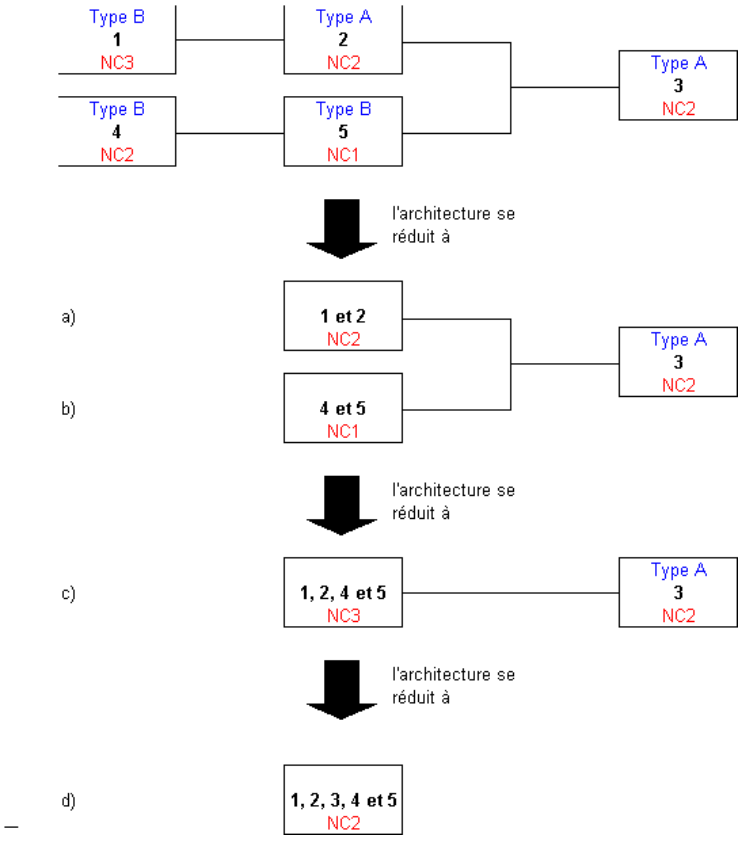


Figure 4 : Exemple d'évaluation du niveau de confiance d'un SIS composé de plusieurs éléments

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 et la proportion de défaillance en sécurité 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) ;

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

b) en combinant les sous-systèmes 4 et 5 : la tolérance aux anomalies matérielles et la proportion de défaillances en sécurité 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. Pour tenir compte de cet effet, la tolérance aux anomalies du sous-système (1, 2) est augmentée de 1. Or d'après le Tableau 4, en augmentant de 1 la tolérance aux anomalies du système, on augmente également de 1 le NC du système. 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 d'architecture des SIS permet de bien repérer les redondances. **Une attention particulière doit être portée au traitement des modes communs de défaillance.**

4.6 AGREGATION DES PERFORMANCES DU SIS

Les performances des détecteurs, des unités de traitements 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 du SIS. 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 $EF_{sis} = Min (EF_{détecteur} , EF_{traitement} , EF_{actionneur})$
Temps de réponse	Il est pris égal à la somme des 3 temps de réponse de chacun des sous système $TR_{sis} = TR_{détecteur} + TR_{traitement} + TR_{actionneur}$
Niveau de confiance	Il est égal au niveau de confiance le plus faible des 3 sous systèmes $NC_{sis} = Min (NC_{détecteur} , NC_{traitement} , NC_{actionneur})$

Tableau 6 : principe d'agrégation des performances des sous-fonctions d'un SIS

4.7 AGREGATION DES PERFORMANCES DES DIFFERENTES FONCTIONS DE SECURITE

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.**

Les questions suivantes (liste non exhaustive) permettent d'évaluer le mode commun de défaillance :

- Existe-t-il des évènements initiateurs pouvant conduire à la défaillance de plusieurs barrières de sécurité (chute d'avion, séisme…mais aussi 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 BADORIS (http://www.ineris.fr/badoris),
- les documents techniques des fournisseurs et des fabricants,
- des rapports de l'INERIS :
    - *Synthèse des résultats de la campagne d'évaluation des détecteurs de gaz ammoniac - INERIS AWa-SBo-2004-46059 -nh3 – août 2004*
    - *évaluation des détecteurs de gaz chlore fixes - INERIS-DRA/PREV-76114-DRA61-op b Cl2-NLp-Sbo – octobre 2006*
    - *Rapport sur les colonnes d'abattage – N. AYRAULT – mai 2004*
    - *Rapport sur les rideaux d'eau – S. BOUCHET – juin 2000*
    - *Rapport sur les explosimètres à long chemin optique – V. DEBUY – février 2003*

5 EVALUATION DES DISPOSITIFS ET BARRIERES PASSIVES

5.1 INTRODUCTION

Un dispositif passif est défini (cf § 3.1) comme un dispositif 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.

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

- Lorsqu'un de ces équipements (cuvette de rétention, disques de rupture…) assure seul une fonction de sécurité (indépendamment de toute mesure technique ou humaine), il constitue un dispositif de sécurité passif. C'est une barrière (ou mesure de maîtrise des risques) passive.
- Mais s'il est associé à des mesures techniques et/ou humaines et que leur défaillance conduit à la perte de la fonction de sécurité, la barrière ne constitue plus une barrière passive.

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.

5.2 EVALUATION DES PERFORMANCES DU DISPOSITIF PASSIF (ASSURANT SEUL UNE FONCTION DE SECURITE)

5.2.1 PRINCIPE D'EVALUATION 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- Evaluation de **l'efficacité** dans un contexte d'utilisation et pour une durée de fonctionnement donnée ;

3- Evaluation du **temps de réponse** (critère généralement non pertinent pour un dispositif passif) ;

4- Evaluation du **Niveau de Confiance (NC)** du dispositif.

Mais contrairement aux autres dispositifs techniques (dispositifs actifs et systèmes instrumentés de sécurité), l'évaluation du NC ne s'appuie pas sur des normes de sûreté de fonctionnement.

Les évaluations des différents paramètres sont précisées paragraphes suivants.

5.2.2 EFFICACITE

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 chapitre 4.3 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 (séisme, chute d'avion).

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. A 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) qui traduisent finalement le bon fonctionnement de la barrière (cf § 5.2.4).

5.2.3 TEMPS DE REPONSE

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

5.2.4 NIVEAU DE CONFIANCE

5.2.4.1 FACTEUR DE REDUCTION DE RISQUES

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

De manière conservatrice, on retient que le NC est associé à une réduction de risques de 10^{NC}, qui correspond à la défaillance de la barrière (cf § 4.5.1).

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).

La non prise en compte de ce dernier cas équivaudrait à considérer que la barrière passive a un NC infini, vision qui n'est pas retenue par l'INERIS (cf §5.2.4.2).

5.2.4.2 EVALUATION 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).

Seul, à notre connaissance, l'ouvrage Layer Of Protection Analysis présentant la méthode LOPA 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 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 7 : PFD de dispositifs extraits de l'ouvrage présentant la méthode LOPA

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[16], nous proposons 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, défaillance intrinsèque, maintenance…).

[16] *Cette vision est en accord avec la philosophie de la norme NF EN 61508 relative aux systèmes instrumentés de sécurité dans laquelle la notion d'architecture (et de redondance éventuelle de systèmes) et celle de contrainte quantitative sont complémentaires.*

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, nous proposons 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.

Au contraire, 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'EVALUATION DES BARRIERES DE SECURITE "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 [1]).

  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[17] 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.

  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 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.
  - ✓ 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 3 octobre 2005[18].

Note : toute fonction de sécurité intègre une part humaine, ne serait-ce que dans les opérations de conception, montage, maintenance, etc. Lorsque l'action humaine est intégrée dans le cycle de vie de la barrière (montage de disque de rupture, vidange de cuvette de rétention…), elle ne remet pas en cause le caractère passif de la barrière. On considère alors que la barrière est passive ; l'action humaine est intégrée dans les performances de la barrière. En revanche, lorsque l'action humaine est une action complémentaire pour le fonctionnement de la barrière (fermeture manuelle de porte dans un mur coupe-feu…), elle remet en cause le caractère passif de la barrière.

---

[17] *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.*

[18] *Circulaire du 3 octobre 2005 relative à la mise en œuvre des plans de prévention des risques technologiques*

5.4 EXEMPLE ET REPRESENTATION EN ARBRES D'EVENEMENTS

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 :

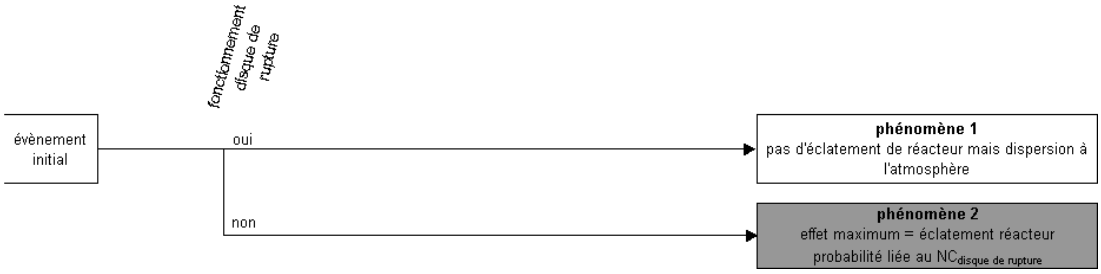


Figure 5 : Exemple d'arbre d'évènements - disque de rupture

- Un autre exemple est la cuvette de rétention (hors rétention avec vidange gravitaire). Une action manuelle de vidange régulière est nécessaire pour assurer l'efficacité de la barrière, mais cette action humaine est intégrée dans les opérations de maintenance et ne remet pas en cause le caractère passif de la cuvette.

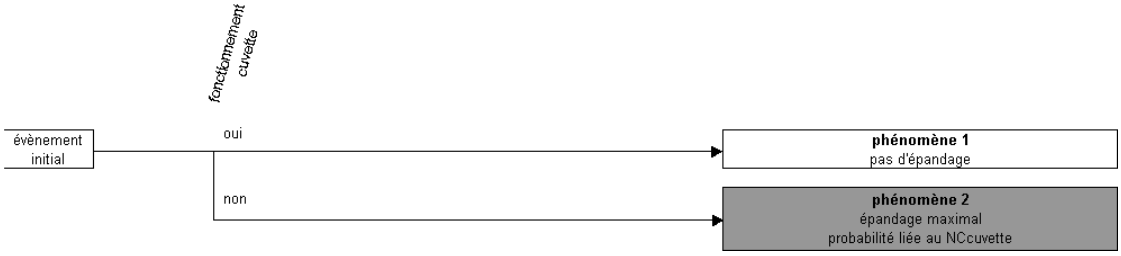


Figure 6 : Exemple d'arbre d'évènements – cuvette de rétention

5.4.2 CAS DE LA PERTE TOTALE DE LA FONCTION DE SECURITE

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 équipé de portes, l'arbre d'évènements (sur la période inférieure au degré coupe-feu du mur) est le suivant :

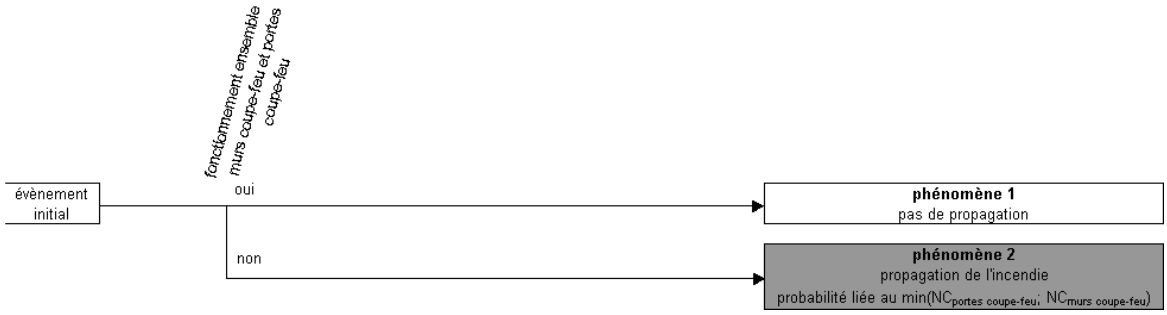


Figure 7 : Exemple d'arbre d'évènements – murs coupe-feu avec portes coupe-feu

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 SECURITE

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 deux façons.

- Une représentation de type simplifiée est toujours envisageable mais elle est réductrice car elle ne fait pas apparaître les phénomènes de probabilités et d'intensités graduées. Ainsi, pour un confinement équipé d'un extracteur, l'arbre d'évènements simplifié est le suivant :

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

Note : l'intensité maximale correspond à l'absence de confinement.

- Mais la représentation détaillée suivante peut également être adoptée.

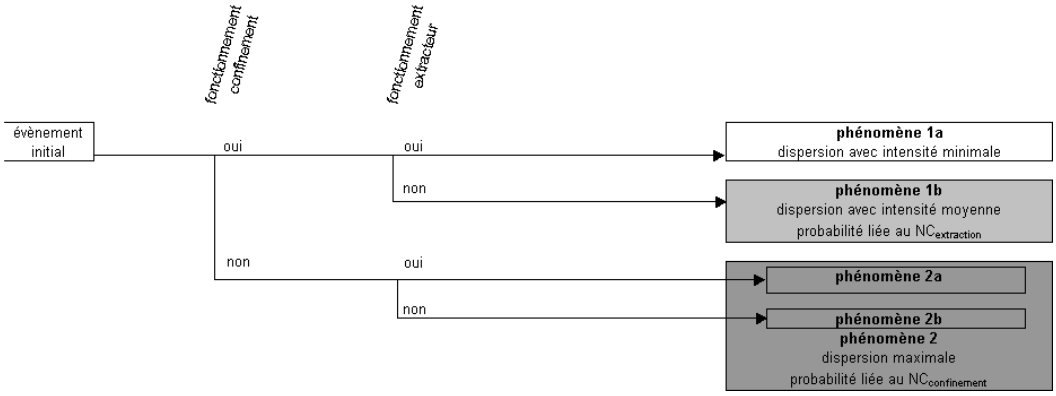


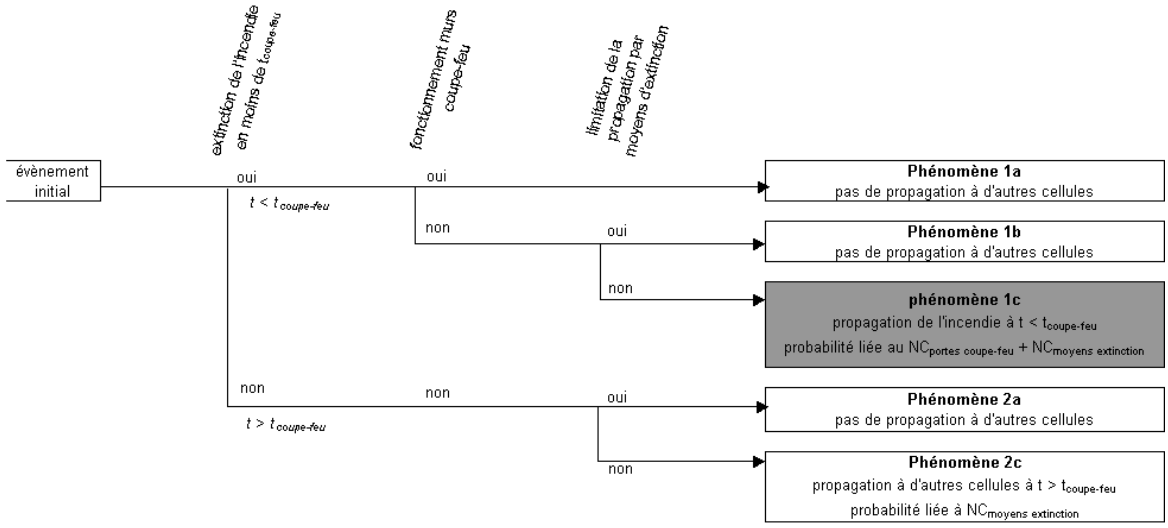
Figure 9 : Exemple d'arbre d'événements détaillé pour un confinement

5.5 CAS PARTICULIER DU DISPOSITIF PASSIF PERDANT SON EFFICACITE APRES UN CERTAIN DELAI

L'efficacité d'une barrière passive peut être dégradée au-delà d'un temps donné : le facteur de réduction de risques est alors lié au NC de la barrière passive mais aussi au NC de la fonction permettant de ne pas atteindre le délai au bout duquel la barrière passive perd ses performances. Différents phénomènes dangereux peuvent être associés, mais il est à noter que **les cinétiques sont alors différentes.**

Par exemple : si des murs coupe-feu (supposés non percés de portes) autour d'une cellule de stockage sont dimensionnés pour limiter la propagation d 'un incendie pendant une durée $t_{coupe\text{-}feu}$ et que la capacité en combustibles peut conduire à un feu de durée supérieure à $t_{coupe\text{-}feu}$, c'est la barrière d'extinction de l'incendie (mesure technique et/ou humaine) qui conditionne la bonne réalisation de la fonction de sécurité que doit assurer le mur coupe-feu. ***Les phénomènes identifiés ont des cinétiques différentes****. La barrière d'extinction intervient dans un premier temps pour limiter la durée de l'incendie. Au-delà de la durée de tenue du mur, elle intervient aussi pour limiter la propagation de l'incendie ; mais ce n'est plus le mur qui assure cette fonction.*

La figure page suivante illustre ces différentes configurations. De manière simplifiée, il est retenu sur la figure que le mur est "simple" (pas d'ouvertures dans les murs) :



note : les barrières identifiées (extinction en moins de $t_{coupe-feu}$ et limitation de la propagation par moyens d'extinction) ne sont pas nécessairement indépendantes.

Figure 10 : Exemple d'arbre d'évènements pour un mur coupe-feu sans ouverture

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

La performance des BTS se dégrade dans le temps lorsque aucune maintenance n'est mise en place. 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**[19] 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 MAINTENANCE

Les barrières techniques de sécurité doivent faire l'objet d'une maintenance préventive destinée à garantir le maintien des performances dans le temps. Ces opérations pourront prendre la forme d'opérations d'entretien (si elles consistent juste à graisser ou à revisser certains boulons) ou d'opérations plus lourdes de maintenance pouvant conduire à une indisponibilité de la barrière (s'il faut démonter entièrement la barrière pour tout nettoyer voire pour changer certaines pièces).

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.

Le groupe de travail 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…).

---

[19] On notera cependant que les barrières passives ne font généralement pas l'objet de tests périodiques

6.2 TESTABILITE

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 capteur de gaz (ou de flamme), il faut veiller à tester non seulement le capteur 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.

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 complet par du personnel qualifié avant la mise en service de l'installation ainsi qu'avant chaque redémarrage.

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.

6.3 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.

Une bonne gestion des modifications doit être réalisée afin de garantir le maintien des performances d'une barrière dans le temps.

On devra alors vérifier que les modifications font l'objet de procédures spécifiques et conduisent à une analyse du fonctionnement des barrières.

7 SYNTHESE DE L'EVALUATION DES BTS

7.1 RAPPEL DES ETAPES DE L'EVALUATION

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- Evaluation 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- Evaluation 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 significativement 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- Evaluation 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 des normes NF EN 61508 et NF EN 61511 relatives aux SIS. L'évaluation a été étendue aux dispositifs actifs.

Des données précises de fiabilité peuvent être nécessaires pour affiner l'évaluation des NC. A défaut, on retient des NC sur la base du type de systèmes : pour des dispositifs sans redondance (pas de tolérance aux anomalies), on a NC 1 pour un système simple (sans microprocesseur) et NC 0 pour un système complexe (avec microprocesseur).

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[20] 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 § 5.2.4.

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'un SIS complet pouvant regrouper plusieurs barrières de sécurité en utilisant notamment les tableaux issus de la norme et les règles présentés au §4.5.5.2;
- évaluer le facteur de réduction de risques induit par l'ensemble des fonctions de sécurité (regroupant éventuellement SIS, dispositifs actifs, dispositifs passifs et/u barrières humaines) agissant sur un scénario d'accident. Le présent document ne présente pas de règles d'agrégation dans ce cas.

Ces évaluations doivent prendre en compte l'architecture et la présence de mode commun de défaillance.

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

7.2 RAPPEL DES OBJECTIFS ET DES LIMITES DE LA METHODE

Il est important de préciser que la démarche présentée dans ce rapport pour évaluer le niveau de confiance ne se substitue pas aux normes NF-EN 61508[2] (sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité) et NF EN 61511[3] (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.

Cette démarche présente une méthode d'analyse qualitative ou semi-quantitative[21] adaptée pour l'évaluation d'une classe de probabilité. Elle s'affranchit des approches quantitatives plus lourdes à mettre en œuvre. **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, SFF très élevée pouvant conduire dans un 1er temps à un SIL élevée par la contrainte architecturale, 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**. Ainsi, un système simple, sans redondance, avec un SFF < 60%, dont les calculs de fiabilité déterminaient une PFD_{avg} de 10^{-4}, aurait quand même un SIL 1 défini par son architecture.

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.

---

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

8 RÉFÉRENCES

[1] Ω20 "Démarche d'évaluation des Barrières humaines de Sécurité" : INERIS pour le Ministère de l'Ecologie et du Développement durable. Rapport disponible sur le site Internet de l'INERIS http://www.ineris.fr

[2] NF EN 61508 "Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité"

[3] NF EN 61511 "Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur de l'industrie de process"

[4] Rapport réalisé dans le cadre du DRA-39 - Guide principal relatif à l'évaluation des Barrières Techniques de Sécurité pour l'inspection des installations classées – S. BOUCHET – juin 2005,

[5] Méthodologie d'évaluation d'un dispositif de sécurité dans une installation industrielle – A. ADJADJ et F. MASSE - INERIS-DCE-LEEL/75014-01- avril 2006.

[6] LOPA : Layer of Protection Analysis.

[7] NF EN ISO 13849-1 (ex NF-EN 954-1) : Sécurité des machines – Partie des systèmes de commande relatives à la sécurité – Partie 1 : principes généraux de conception – Février 2007

9 LISTE DES ANNEXES

Repère	Désignation précise	Nb/N°pages
A	Système Instrumenté de Sécurité	4
B	Etude statistique de l'EXERA	1
C	NC des Systèmes simples ou complexes	2
D	Exemples d'évaluation de sous-systèmes	10

ANNEXE A

Système Instrumenté de Sécurité

Composition d'un S.I.S.

1- Composition minimale d'un SIS :

Les SIS sont constitués de différents éléments unitaires reliés entre eux par des moyens de transmissions. Au minimum, on retrouve en série un capteur, une unité de traitement et un actionneur qui vient commander un élément terminal (cf.

Figure 11).

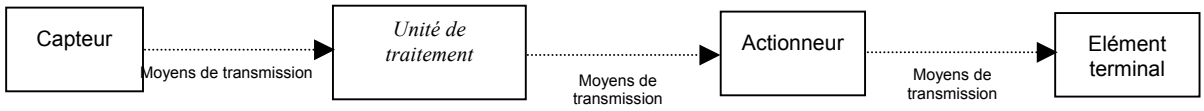


Figure 11 : Schéma d'un SIS simple

2- Composition d'un SIS 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 SIS le montage en parallèle de plusieurs actionneurs et d'éléments terminaux (cf.

Figure 12).

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

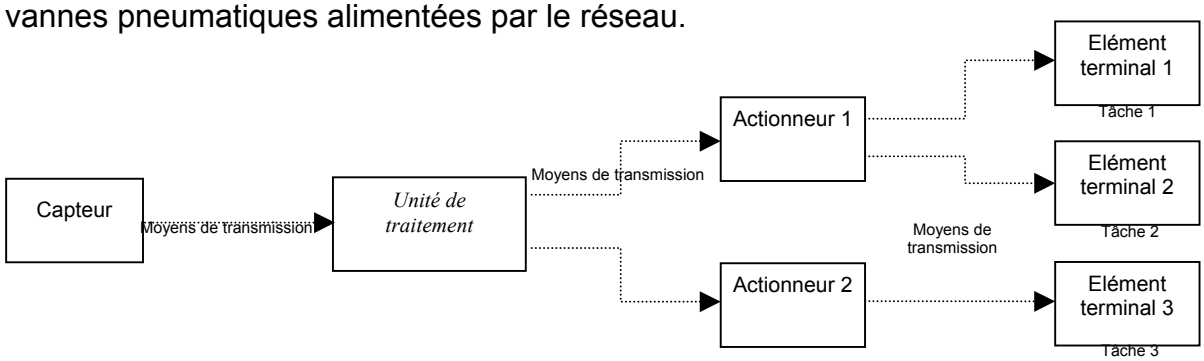


Figure 12: Schéma d'un SIS effectuant plusieurs tâches

Beaucoup moins fréquemment, on trouve 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 13). 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).

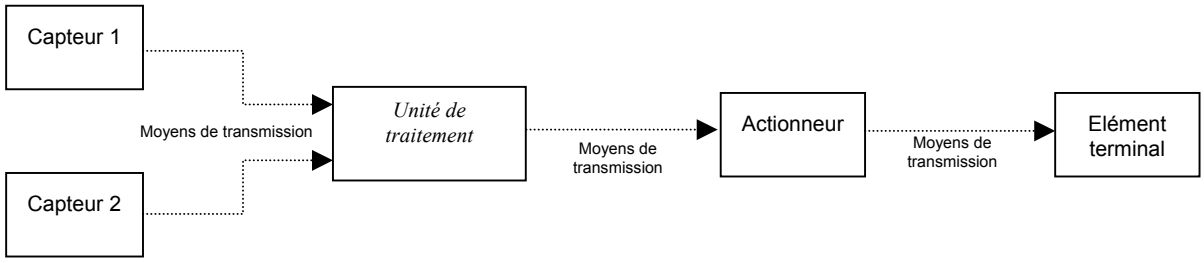


Figure 13 : Schéma d'un SIS recevant plusieurs informations

3- Redondance au sein d'un S.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). A 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 constituants une barrière de sécurité peuvent être redondés : capteurs, unité de traitement, actionneurs, éléments terminaux et même les moyens de transmission.

La figure 6 donne un exemple d'un SIS complexe, les redondances étant indiquées en rouge.

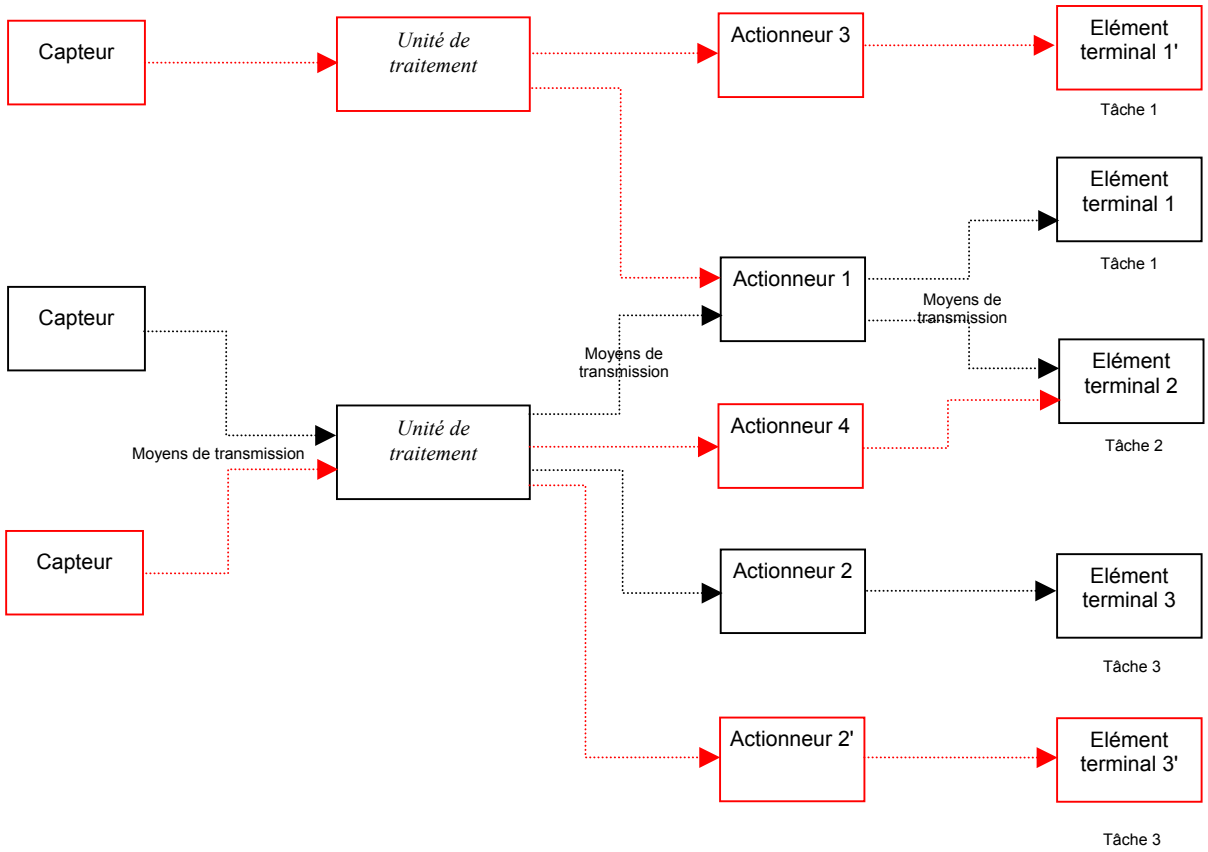


Figure 14 : Schéma d'un SIS complexe avec redondances

A noter que l'on peut distinguer plusieurs types de redondance[22] :

- **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.

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 avant que celle-ci ne 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" car elle permet un bon compromis sécurité – disponibilité des outils de production.

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

ANNEXE B

Etude statistique de l'EXERA

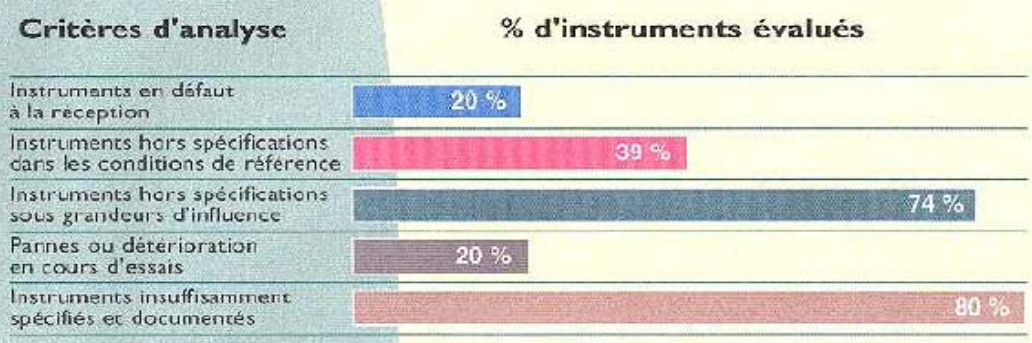
EI
WIB
EXERA

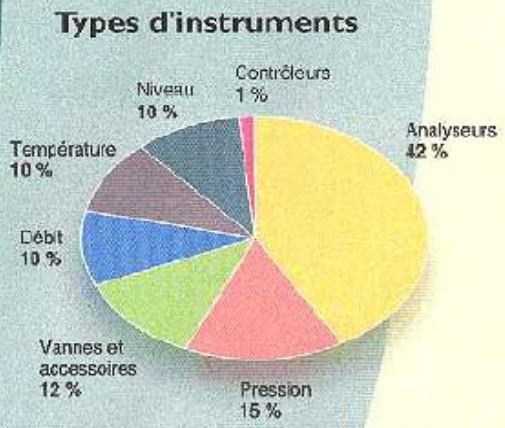
International Instrument User's Associations

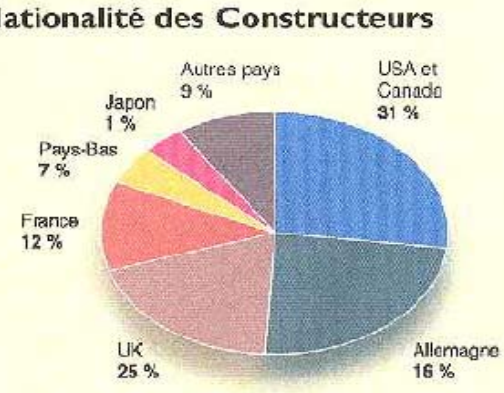
Evaluations

Des statistiques qui interpellent
(107 matériels testés sur cinq ans)

Globalement 1 produit sur 2 répond à l'ensemble des spécifications annoncées







La contribution des associations d'utilisateurs à la qualité des produits :
des modifications sont apportées, par les constructeurs, après évaluation, sur 29 % des produits.

ANNEXE C

NC des systèmes simples ou complexes

La présente annexe détaille le lien entre systèmes simples et complexes et les termes définis dans les normes, à savoir systèmes de type A ou B (terminologie NF EN 61508) ou unités logiques programmables (PE) et autres sous-systèmes.

1- Correspondance entre le vocabulaire des normes et celui de l'INERIS

De manière simplifiée, l'INERIS retient pour les **systèmes simples** les systèmes **sans microprocesseurs ou logiciels** et pour les **systèmes complexes** ceux **avec microprocesseurs ou logiciels**.

Les systèmes dits **simples ou complexes** sont rattachées respectivement aux systèmes de **type A ou B** (tels que définis dans la norme NF EN 61508-2) et aux systèmes de **type unités logiques de l'électronique programmable ou aux autres sous-systèmes** (tels que définis dans la norme NF EN 61511-1).

- **La norme NF EN 61508** considère qu'un système est du **type A** (qualifié de **simple** par l'INERIS) si tous les composants nécessaires à la réalisation de la fonction de sécurité satisfont les conditions suivantes :
  - Les modes de défaillance sont bien définis ;
  - Le comportement du sous-système dans les conditions d'anomalie peut être entièrement déterminé ;
  - Il existe des données de défaillance, obtenues à partir de retour d'expérience sur le terrain, suffisamment fiables pour appuyer des taux de défaillance annoncés relatifs à des défaillances dangereuses détectées ou non détectées.

  Les systèmes ne répondant pas aux conditions de systèmes du type A sont par défaut des systèmes de type B.

  Or, les défaillances des systèmes à base de microprocesseurs ne sont pas bien connues, si bien que ces systèmes ont été rattachés à des systèmes de **type B**. Ils ont été qualifiés de type **complexe** par l'INERIS.

  Les autres dispositifs dont les défaillances sont connues sont rattachés **au type A**. Ils ont été qualifiés de type **simple** par l'INERIS.

- La norme **NF EN 61511** distingue deux types de systèmes : les unités logiques de l'Electronique Programmable (PE) et les autres sous-systèmes (par exemple capteurs, éléments terminaux et unités logiques non PE). Les **unités logiques de l'Electronique Programmable (PE)** sont rattachées aux systèmes de type **complexe** et les **autres** sous-systèmes sont rattachés aux systèmes de type **simple**.

2- Similitude de prescriptions entre les types A et systèmes autres que les unités logiques programmables et les types B et les unités logiques programmables

Les tableaux de la norme NF EN 61508-2 présentent les SIL maximums en fonction des SFF et des tolérances aux anomalies matérielles (cf § *4.5.4*) pour les deux types de composants A et B.

Dans une forme un peu différente mais pour des prescriptions similaires à celles des systèmes de type B de la norme NF EN 61508, la norme **NF EN 61511** spécifie des tolérances minimales aux anomalies de matériel en fonction des SIL (NC pour INERIS) pour des **unités logiques de l'électronique programmable (PE) :**

NC	Tolérance minimale aux anomalies du matériel		
	SFF < 60%	SFF 60% à 90%	SFF > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Les exigences spéciales s'appliquent – voir la CEI 61508		

Tableau 8 : tolérance minimale aux anomalies du matériel pour les unités logiques de l'électronique programmable (PE)

Pour les **autres systèmes (capteurs, éléments terminaux et unités logiques non PE)**, le tableau des tolérances aux anomalies matérielles est à première vue plus simple que celui des types A de la norme 61508. Mais les conditions associées au tableau permettent de traiter les cas supplémentaires (cf § 4.5.4).

NC	Tolérance minimale aux anomalies du matériel (voir conditions)
1	0
2	1
3	2
4	Les exigences spéciales s'appliquent – voir la CEI 61508

Tableau 9 : tolérance minimale aux anomalies du matériel pour les capteurs, les éléments terminaux et les unités logiques non PE

ANNEXE D

Exemple d'évaluation de sous-systèmes

Les exemples présentés dans cette annexe sont issus du guide principal relatif à l'évaluation des barrières techniques de sécurité pour l'inspecteur des installations classées [3].

EXEMPLE 1 : DETECTEURS

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. Le capteur ne fait pas intervenir de microprocesseurs. Il est donc assimilable à un système simple (sans microprocesseur).
- 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 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). il peut donc être assimilé soit à un système simple (détecteur analogique) soit à un système complexe (transmetteur numérique). 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 un SIS.

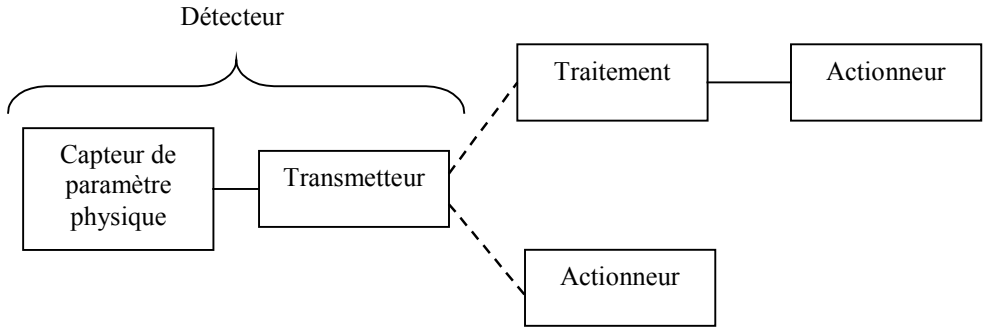


Figure 15 : architecture depuis le capteur jusqu'à l'actionneur

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 du SIS 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	100 %, si le contexte d'utilisation n'a pas d'influence[23] (essais, REX…)
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	1) Détecteur analogique : système simple, architecture monocanal (pas de tolérance aux défaillances) et SFF < 60 % : NC=1 2) Détecteur numérique : système complexe, architecture monocanal (pas de tolérance aux défaillances) • absence de watchdog[24] : SFF < 60 % , NC=0 • présence d'un watchdog : 60 % < SFF < 90 % , NC=1

Tableau 10 : performance des détecteurs de paramètres physiques génériques

Le tableau ci-dessus montre que suivant l'architecture du détecteur, il peut, seul, prétendre à un niveau de confiance ou pas.

Remarque : Lors de l'étude complète d'un SIS, les niveaux de confiance finaux attribués aux relais de sécurité et aux automates programmables dédiés à la sécurité, réalisant la sous-fonction "traitement de l'information", dépendent des architectures en entrée et des architectures en sortie. Les niveaux de confiance annoncés dans ce chapitre sont les niveaux maximum atteignables lorsque les architectures en entrée et en sortie fournies par le constructeur sont respectées, puisque ces éléments sont certifiés pour une architecture en entrée et une architecture en sortie données.

[23] De récents essais sur des détecteurs d'ammoniac fixes ont montré l'influence sur l'efficacité et le temps de réponse de différents contextes d'utilisation (http://badoris.ineris.fr)

[24] watchdog = chien de garde

EXEMPLE 2 : RELAIS ELECTROMECANIQUE

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 à logique câblée.

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.

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

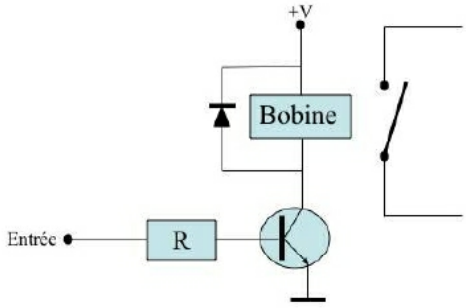


Schéma d'un relais électromécanique

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	Système simple, architecture monocanal (pas de tolérance aux défaillances) et SFF < 60 % NC=1, 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

Remarque : Lors de l'étude complète d'un SIS, les niveaux de confiance finaux attribués aux relais de sécurité et aux automates programmables dédiés à la sécurité, réalisant la sous-fonction "traitement de l'information", dépendent des architectures en entrée et des architectures en sortie. Les niveaux de confiance annoncées dans ce chapitre sont les niveaux maximum atteignables lorsque les architectures en entrée et en sortie fournies par le constructeur sont respectées, puisque ces éléments sont certifiés pour une architecture en entrée et une architecture en sortie données.

EXEMPLE 3 : RELAIS DE SECURITE

Description

Les relais de sécurité sont utilisés dans le domaine de la sécurité machine (protection du travailleur). Ils peuvent également être utilisés pour assurer la sous-fonction "traitement de l'information" d'un SIS mis en œuvre pour la prévention ou la protection d'un accident majeur. Il existe principalement 2 types de relais de sécurité qui reposent sur 2 technologies différentes :

- soit le relais de sécurité est composé par une architecture de relais électromécaniques, dont certains avec des contacts liés, empêchant ainsi un réarmement alors que des contacts resteraient "collés",
- soit le relais de sécurité est un "mini-automate de sécurité", permettant de réaliser des autocontrôles de ses entrées et de ses sorties (transistors MOS). Le fonctionnement des ces relais (notamment les contrôles du bon fonctionnement des sorties par microcoupures) ne permet pas la connexion de n'importe quel actionneur. De manière générale, les actionneurs alimentés par ces relais sont des contacteurs de puissance.

Performance

Les relais de sécurité sont certifiés suivant la norme 13849-1 [7]. Cette norme classe les parties de système de commande relatives à la sécurité en catégorie, 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).

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	• Architecture de relais électromécaniques : système simple, architecture redondante (tolérance aux défaillances) et SFF < 60% voire 60 < SFF < 90 % NC=2 jusqu'à 3, après vérification que la position de repos correspond à l'action de sécurité, du bon dimensionnement par rapport à l'intensité susceptible de le traverser et du respect des architectures en entrée et en sortie fournies par le constructeur • "mini-automate de sécurité" : système complexe, architecture redondante (tolérance aux défaillance) et 60 < SFF < 90 % voire SFF > 90 % NC=2 jusqu'à 3, après vérification que la position de repos correspond à l'action de sécurité, du bon dimensionnement par rapport à l'intensité susceptible de le traverser et du respect des architectures en entrée et en sortie fournies par le constructeur

Remarque : Lors de l'étude complète d'un SIS, les niveaux de confiance finaux attribués aux relais de sécurité et aux automates programmables dédiés à la sécurité, réalisant la sous-fonction "traitement de l'information", dépendent des architectures en entrée et des architectures en sortie. Les niveaux de confiance annoncées dans ce chapitre sont les niveaux maximum atteignables lorsque les architectures en entrée et en sortie fournies par le constructeur sont respectées, puisque ces éléments sont certifiés pour une architecture en entrée et une architecture en sortie données.

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 ; "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 le SFF.

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

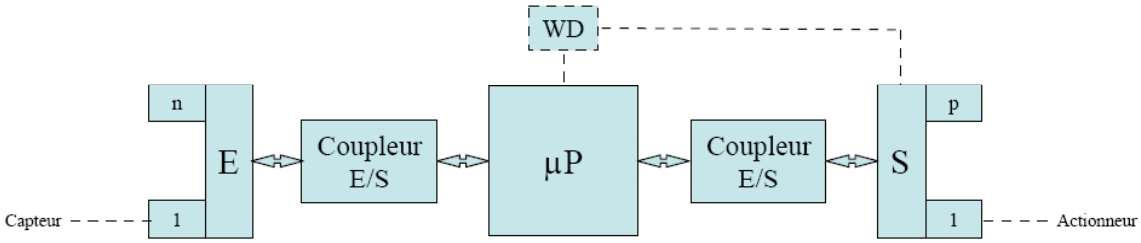


Figure 16 : exemple d'architecture d'un API

Entre les détecteurs et les cartes d'entrée peuvent être installés des convertisseur 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	• API sans watchdog : système complexe, architecture simple (pas de tolérance aux défaillances) et SFF < 60 % NC=0 • API avec watchdog : système complexe, architecture simple (pas de tolérance aux défaillances) et 60 % < SFF < 90 % NC=1

Tableau 11 : performance des API

Remarque : Lors de l'étude complète d'un SIS, les niveaux de confiance finaux attribués aux relais de sécurité et aux automates programmables dédiés à la sécurité, réalisant la sous-fonction "traitement de l'information", dépendent des architectures en entrée et des architectures en sortie. Les niveaux de confiance annoncés dans ce chapitre sont les niveaux maximum atteignables lorsque les architectures en entrée et en sortie fournies par le constructeur sont respectées, puisque ces éléments sont certifiés pour une architecture en entrée et une architecture en sortie données.

EXEMPLE 5 : LES API DEDIES A LA SECURITE (APIDS)

Description

Le fonctionnement des APIdS est globalement identique à celui des API. Un APIdS 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'APIdS (il existe des architectures différentes).

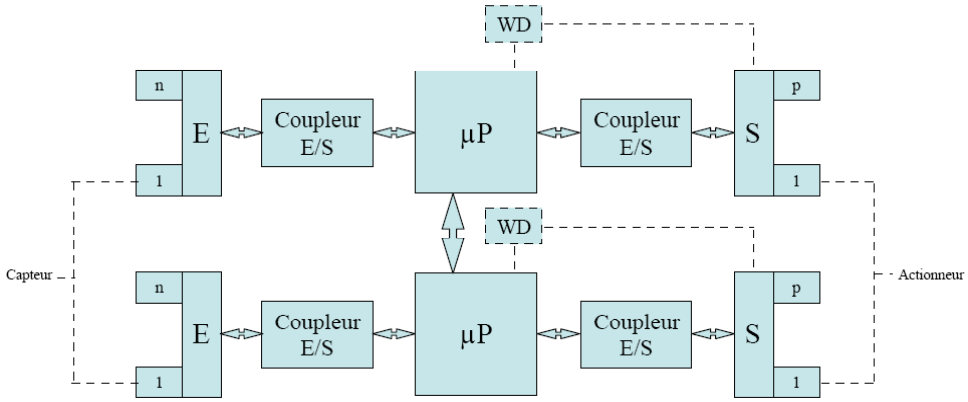


Figure 17 : exemple d'architecture d'un APIdS

Performance

Un automate est déclaré "dédié à la sécurité" lorsqu'il a été certifié suivant la norme NF-EN 61508, 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 APIdS 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 en entrée et en sortie fournies par le constructeur

Tableau 12 : performance des APIdS

Remarque : Lors de l'étude complète d'un SIS, les niveaux de confiance finaux attribués aux relais de sécurité et aux automates programmables dédiés à la sécurité, réalisant la sous-fonction "traitement de l'information", dépendent des architectures en entrée et des architectures en sortie. Les niveaux de confiance annoncés dans ce chapitre sont les niveaux maximum atteignables lorsque les architectures en entrée et en sortie fournies par le constructeur sont respectées, puisque ces éléments sont certifiés pour une architecture en entrée et une architecture en sortie données.

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 ou 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 Système simple, architecture monocanal (pas de tolérance aux défaillances) et SFF < 60 % NC=1, 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 • Démarrage du moteur Tous les éléments constituant sont des systèmes simples, architecture monocanal (pas de tolérance aux défaillances) et SFF < 60 % NC_{sys} = Min ($NC_{contact}$, NC_{moteur} , NC_{pompe}) = 1

Tableau 13 : performance des systèmes "contacteur de puissance, moteur électrique, pompe ou compresseur"

EXEMPLE 7 : LES VANNES MOTORISEES

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 assurée 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	Tous les éléments constitutifs de la vanne motorisée sont des systèmes simples, architecture monocanal (pas de tolérance aux défaillances) et SFF < 60 % $NC_{sys} = Min\ (NC_{corps\_de\_vanne}\ ,\ NC_{moteur}) = 1$

Tableau 14 : performance des vannes motorisées