ALLOCATION DE NIVEAU D'INTÉGRITÉ DE SÉCURITÉ (SIL) REQUIS CONFORMEMENT A LA NORME CEI 61511

Lanternier B. [1], Adjadj A.[1]

[1]Institut Nationale de l'Environnement Industriel et des Risques, DCE/LEEL
Verneuil en Halatte – France
brice.lanternier@ineris.fr ; ahmed.adjadj@ineris.fr

ABSTRACT

The IEC 61511 standard concerns functional safety for safety instrumented systems (SIS) application in Process Industries. The standard requires to carry out process hazard and risk assessment in order to deduce SIS specifications. Two main concepts, which are fundamental according to the application, are underlined: safety lifecycle and safety integrity levels. This article mostly deals with the safety integrity levels (SIL) and with their allocation, depending on the SIS considered. This international standard describes various quantitative and qualitative methodologies for SIL allocation. The choice between these methods will depend on various criteria as illustrated in this paper. The paper makes a brief description of three spread methods in the Process Industries. The selected criteria for each method are presented. Advantages and disadvantages of these various methods are indicated. In order to illustrate the methodology of a SIL allocation, a case study on a storage unit of ammonia is presented.

RÉSUMÉ

La norme CEI 61511 s'intéresse à la sécurité fonctionnelle dans l'application des systèmes instrumentés de sécurité aux industries de production par processus. Elle exige dans ce cadre de conduire une évaluation de danger et de risque des processus pour permettre d'en déduire des spécifications pour les SIS. Deux concepts fondamentaux sont mis en avant : le cycle de vie de sécurité et les niveaux d'intégrité de sécurité ou SIL (Safety Integrity Level). Cet article s'intéresse plus particulièrement au niveaux d'intégrité de sécurité et à leur allocation en fonction du SIS à évaluer. La norme décrit différentes méthodes d'allocation de SIL, qu'elles soient qualitatives ou quantitatives. Aucune méthode n'est à privilégier, le choix d'une technique dépendra de différents critères. Cet article fait ainsi une brève description de trois méthodes répandues dans le secteur des industries de procédés. Nous présentons les critères qui orientent le choix d'une méthode et indiquons les avantages et les inconvénients de ces différentes méthodes. Afin d'expliciter le déroulement d'une démarche d'allocation de SIL, une application sur une unité de stockage d'ammoniac est présentée.

1. INTRODUCTION

Les normes internationales de Sécurité fonctionnelle CEI 61508 [1] et CEI 61511 [2] définissent une démarche d'analyse du niveau d'intégrité d'un système de sécurité. Elles permettent de définir le niveau d'intégrité de sécurité requis (SIL) pour une Fonction Instrumentée de Sécurité suite à une analyse de risque. Ces normes n'imposent pas de règle mais proposent en revanche des méthodes pour l'allocation du SIL. Ces méthodes sont, plus au moins bien adaptées en fonction du niveau de détail des analyses de risques réalisées au préalable ainsi que de la qualité et la quantité des informations disponibles.
Une fois la contribution des systèmes de sécurité autres que les SIS évaluée, la réduction de risque nécessaire pour respecter l'objectif fixé (risque résiduel) est atteint grâce aux Fonctions Instrumentées de Sécurité.
Les données nécessaires pour l'allocation du SIL ne sont pas toujours disponibles ou n'existent pas. Dans ce cas, il faut s'appuyer sur le retour d'expérience de l'exploitant et l'expertise acquise dans des installations similaires.
La norme CEI 61511 décrit plusieurs méthodes d'allocation de SIL. Certaines sont de types qualitatifs (le graphe de risque, la grille de criticité issue de la circulaire du 29 septembre 2005 [3],…) et d'autres sont de type quantitatifs (LOPA : Layer of Protection Analysis [4]). Le choix d'une méthode dépendra de différents critères comme le montre cet article. Une application sur une unité de stockage d'ammoniac est présentée.

2. METHODE DE DETERMINATION DES SIL REQUIS

2.1 Introduction

Pour toute installation industrielle, il est nécessaire de définir les situations dangereuses, puis de prendre les mesures nécessaires afin :

- d'éliminer ou réduire les risques dans la mesure du possible (intégration de la sécurité à la conception et à la construction), ce qui implique de les identifier et de les évaluer en termes de conséquences sur les personnes et l'environnement, au niveau du site et de ces alentours,
- de prendre les mesures de sécurité nécessaires vis-à-vis des risques ne pouvant être éliminés, par des systèmes de prévention et de protection (dont les fonctions instrumentées de sécurité),
- d' informer les utilisateurs des risques résiduels dus à l'efficacité incomplète des mesures de protection adoptées (indiquer si une formation particulière est requise et signaler s'il est nécessaire de prévoir un équipement de protection individuelle).

Pour identifier les fonctions instrumentées de sécurité et définir leur SIL, il est nécessaire que les risques soient préalablement identifiés, ainsi que leurs conséquences sur les personnes et l'environnement. Les données suivantes sont donc indispensables :

- description des procédés et des installations,
- recensement des matières et produits utilisés,
- historiques des incidents et accidents répertoriés,
- identification et caractérisation des potentiels de dangers et estimation de leurs effets,
- analyses de risque réalisées.

Ces données ne sont pas toujours explicitement formulées et recensées au niveau de la documentation de l'entreprise. Par conséquent, il est nécessaire de réaliser un travail visant soit à améliorer la documentation soit à rechercher les informations indispensables notamment d'identifier les risques potentiels et les barrières de sécurité existantes. Pour ce faire, un audit de l'installation peut être envisagé afin de recenser les documents existants, de rassembler les éléments nécessaires à la définition du SIL et d'identifier les analyses complémentaires à mener.
La norme CEI 61511 décrit différentes méthodes de détermination de SIL. Nous avons choisi de revenir plus en détails sur quelques unes afin de comprendre les différentes philosophies mises en œuvre. Parmi celles-ci, on citera les méthodes qualitatives que sont « le graphe de risque » et la « grille de criticité » et la méthode quantitative « LOPA » (Layer of Protection Analysis).

2.2 Le Graphe de risques

Le graphe de risque consiste à hiérarchiser les niveaux de sécurité à partir de quatre paramètres liés à la conséquence du risque sur le personnel ou l'environnement (C), à la fréquence d'exposition au risque (F), à la possibilité d'éviter le danger (P) et à la probabilité d'occurrence du danger (W) tels que présenté sur la figure 2.2-1.

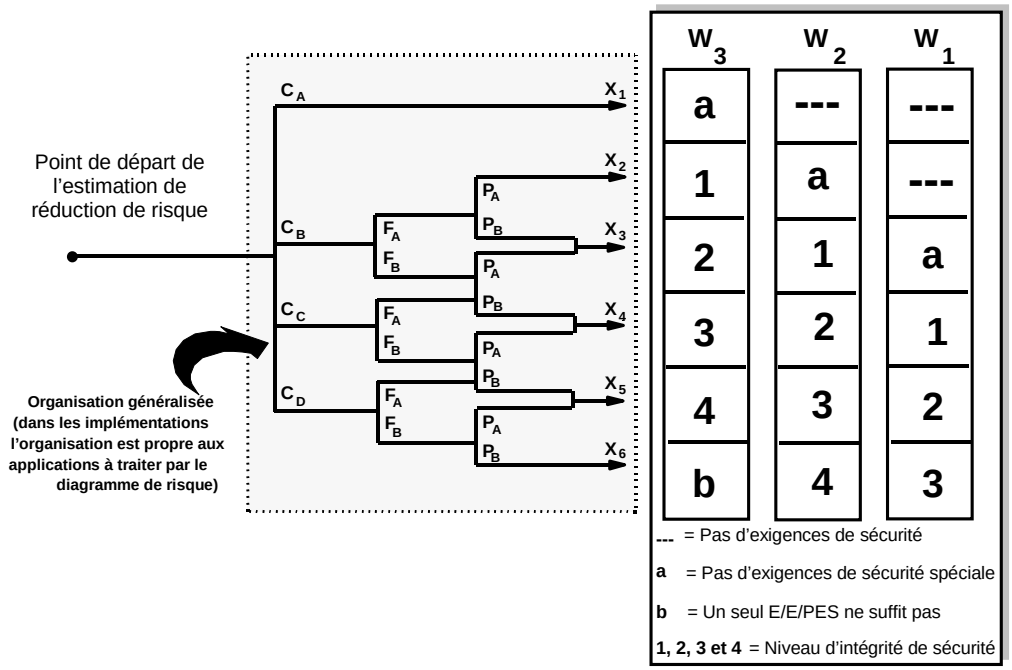

Figure 2.2-1 Graphe de hiérarchisation du risque présenté dans la norme CEI 61511-3

La classification repose sur une hiérarchisation en 6 classes d'exigences graduées de "a" à "b" en passant par SIL1 à SIL 4. La catégorie "a" correspond alors à "aucune exigence particulière de sécurité" tandis que la catégorie "b" correspond à une situation inacceptable (le système instrumenté est insuffisant).

Les niveaux affectés aux paramètres du graphe constituent la base de l'évaluation du risque. Une phase de calibrage ou d'étalonnage du diagramme de risque est nécessaire. Elle permet d'adapter les paramètres en prenant en compte les spécificités de l'entreprise et la réglementation. La difficulté est alors de calibrer le graphe. L'étalonnage des paramètres doit permettre de prendre en compte toutes les situations sans pour autant obtenir une échelle trop large qui ne permettraient pas une précision suffisante. En effet, selon les choix de l'analyste, les résultats peuvent rapidement passer d'un niveau d'intégrité à un autre.

Tableau 2.2-1 : Etalonnage des paramètres du graphe de risque

Paramètres de risque		**Classification**
Conséquences	C_A C_B C_C C_D	Incident mineur Effets reversibles Effets létaux limités au site Effets létaux en dehors du site
Exposition	F_A F_B	Exposition rare dans la zone considérée Exposition fréquente dans la zone considérée
Possibilité d'éviter le danger	P_A P_B	Possible sous certaines conditions Impossible
Taux de sollicitations	W_1 W_2 W_3	Faible probabilité (Accident pouvant se produire) Probabilité moyenne (Accident, déjà observé) Probabilité élevée (Accident fréquent, observé plus d'une fois)

2.3 La Grille de criticité

Cette méthode consiste à positionner les différents scénarios d'accidents (sans prendre en considération les barrières de sécurité) sur une matrice de criticité, puis à déterminer les critères pour passer d'une situation dangereuse à une situation acceptable grâce aux barrières de sécurité mises en place. Les échelles de gravité et de probabilité des événements permettent de classer les différents risques répertoriés sur la grille de criticité. Chaque exploitant doit définir, en fonction des spécificités de son établissement, la grille de criticité qui semble la mieux adaptée. Dans le cas d'un site ICPE (Installation Classée pour la Protection de l'Environnement), l'exploitant peut se reposer sur les échelles de gravité et de probabilité des deux arrêtés datant du 21/09/05 [5][6] et également sur la grille de criticité (*Tableau 2.3-1*) issue de la circulaire d'application [3] de l'arrêté relatif à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des installations classées soumises à autorisation.

Comme il n'est pas possible d'éliminer tous les risques potentiels, il est nécessaire de définir des critères d'acceptabilité en 3 zones :

- une zone de risque élevé inacceptable car trop dangereux et/ou trop fréquent, figurée par le mot «NON»
- une zone de risque intermédiaire, figurée par le sigle «MMR» (Mesures de Maîtrise des Risques), pour lesquels il convient d'ajouter des barrières de sécurité pour réduire le risque,
- une zone de risque accepté, qui ne comporte ni «NON» ni «MMR».

Tableau 2.3-1 : Grille d'analyse de la justification des mesures de maîtrise du risque

Probabilité / **Gravité**	E	D	C	B	A
Désastreux	Non partiel / MMR2*	NON 1	NON 2	NON 3	NON 4
Catastrophique	MMR 1	MMR 2*	NON 1	NON 2	NON 3
Important	MMR 1	MMR 1	MMR 2*	NON 1	NON 2
Sérieux			MMR 1	MMR 2	NON 1
Modéré					MMR 1

Si les effets et/ou la probabilité estimée conduisent à un positionnement de l'accident en dehors des zones de risques "accepté", il est nécessaire de rajouter d'autres barrières de sécurité. Dans le cadre de la norme CEI 61511, les barrières de sécurité complémentaires seront des fonctions instrumentées de sécurité (FIS). Ces FIS devront conduire à ce qu'aucun risque "inacceptable" ne subsiste. Une barrière instrumentée de sécurité agit généralement sur la fréquence de l'événement redouté, elle n'intervient pas sur la dangerosité de l'accident. Ainsi, la barrière tend à décaler vers la gauche la probabilité d'occurrence de l'accident. Ramené aux niveaux d'un SIL, le décalage d'une case vers la gauche correspond à SIL 1 (réduction du risque d'un facteur 10), de 2 cases à SIL 2 et ainsi de suite. Cette règle implique que la discrétisation en probabilité soit d'une décade par classe.

Cette approche est simple à mettre en œuvre et le positionnement des scénarios d'accident est aisé. Elle est utilisable sur des technologies opérationnelles depuis une période représentative et ne peut s'appliquer à des procédés nouveaux sans retour d'expérience. A l'instar du graphe de risques, cette méthode trouve sa difficulté dans le calibrage de la matrice.

2.4 LOPA (Layer Of Protection Analysis)

Contrairement aux techniques d'évaluation des risques purement qualitatives, l'analyse des couches de protection permet d'estimer la fréquence d'un événement redouté. Cette méthode intègre les couches de protection de l'entreprise, tant organisationnelles1 que techniques. Les dimensions organisationnelles, prises en compte dans ce cadre, n'ont pas vocation à être exhaustives [7]. La méthode LOPA évalue la réduction du risque en analysant la contribution des différentes couches (des caractéristiques intrinsèques du process jusqu'aux mesures de secours) en cas d'accident. Elle est utilisée pour déterminer quel SIL est assigné à chaque FIS et elle permet de déterminer combien de couches de protection sont nécessaires pour ramener le risque à un niveau tolérable. L'objectif est de calculer le risque résiduel exprimé en fréquence d'accident par an, ce qui impose de quantifier les fréquences d'occurrence des événements initiateurs et les probabilités de défaillances de chaque couche.
L'analyse comprend les étapes suivantes:

- La définition de l'impact de l'événement redouté (gravité);
- La détermination et l'énumération de tous les événements initiateurs;
- La détermination et l'énumération de toutes les couches de protection qui empêchent la propagation de l'événement initiateur conduisant à l'événement redouté;
- La détermination de la fréquence des événements initiateurs, basée sur des données de REX et/ou de jugement d'experts;
- La détermination de l'efficacité des couches de protection en probabilité de défaillance sur demande, basée sur des données de REX et/ou de technologie;
- Le calcul de la fréquence de l'événement redouté.

L'analyse des couches de protection est une manière efficace de déterminer le niveau d'intégrité de sécurité (SIL) exigé pour les fonctions instrumentées de sécurité (FIS).
Dans l'exemple du tableau 2.4-1, un SIL 3 est requis pour l'événement redouté "Défaillance boîte froide" et un SIL 1 pour "Défaut vapeur HP". La fonction "Mise en sécurité du réacteur par dérive de la température" sera SIL 3 (valeur maximale).
La méthode LOPA ne s'applique que pour le fonctionnement à la demande (le système de sécurité n'est sollicité qu'en présence d'un événement initiateur de la situation dangereuse qui lui est indépendante) et elle n'est pas adaptée au mode continu (une défaillance du système de sécurité est un événement initiateur de la situation dangereuse). Cette méthode a l'avantage de ne pas avoir d'étalonnage à réaliser puisque les valeurs d'entrées sont quantifiées. Le problème se posera cependant sur ces valeurs qui ne sont pas communément admises et qui diffèrent en fonction des sites, des situations, des environnements, des retours d'expériences, etc.

1 La méthode LOPA impose de passer du mode "descriptif " des aspects organisationnels à une "qualification" en vue de manier les données "quantifiables" et "qualifiables" afin d'estimer la fréquence d'un événement redouté.

Tableau 2.4-1 : Exemple de tableau LOPA

Danger combattu : Eclatement du réacteur							
FIS : Mise en sécurité du réacteur sur dérive de la température (emballement thermique)							
Objectif de Sécurité	**Evénement initiateur**		**Couches de protection**				**Fréquence résultante**
			BPCS (Conduite régulation)	**FIS**	**Dispositif d'atténuation (soupape)**	**Dispositif de protection**	
Fréq./an	**Désignation**	**Fréq./ an**	**PFDavg**	**PFDavg**	**PFDavg**	**PFDavg**	
10^{-5}	Défaillance boîte froide (Présence de polluant)	10^{-1}	10^{-1}	**10^{-3} (SIL 3)**	1	1	10^{-5}
10^{-5}	Défaut vapeur HP (Gaz trop chaud)	10^{-2}	10^{-1}	**10^{-1} (SIL 1)**	10^{-1}		10^{-5}
10^{-5}	**…**						

3. APPLICATION INDUSTRIELLE

3.1 Description de l'installation

L'installation est un réseau de refroidissement à l'ammoniac (figure 3.1-1). Le système de refroidissement permet de répondre à la demande de froid des réacteurs. Pour absorber la chaleur produite dans les réacteurs, on envoie de l'ammoniac qui s'évapore au contact de la chaleur. La ligne d'alimentation en ammoniac liquide provenant de la cuve passe par un séparateur et elle se sépare en 2 lignes parallèles. Le séparateur permet de refroidir l'ammoniac liquide avant de l'envoyer aux réacteurs. Il est destiné également à séparer l'ammoniac liquide de l'ammoniac gazeux, provenant de la ligne de retour, pour empêcher la présence de liquide à l'aspiration des compresseurs. Les compresseurs aspirent l'ammoniac gazeux du séparateur et le refoulent vers un condenseur évaporatif. Leur but est de comprimer l'ammoniac gazeux à une pression permettant de le liquéfier par le condenseur évaporatif. Le condenseur évaporatif a pour but de liquéfier l'ammoniac gazeux et pour objectif de maintenir un pression de 11 bars sur la cuve. Une tour de refroidissement permet de refroidir l'eau industrielle alimentant le condenseur évaporatif.
Le système de refroidissement est équipé de vanne d'isolement permettant d'isoler certains tronçons en cas de fuite. Il est également équipé de soupapes de sécurité pour le protéger contre les surpressions.

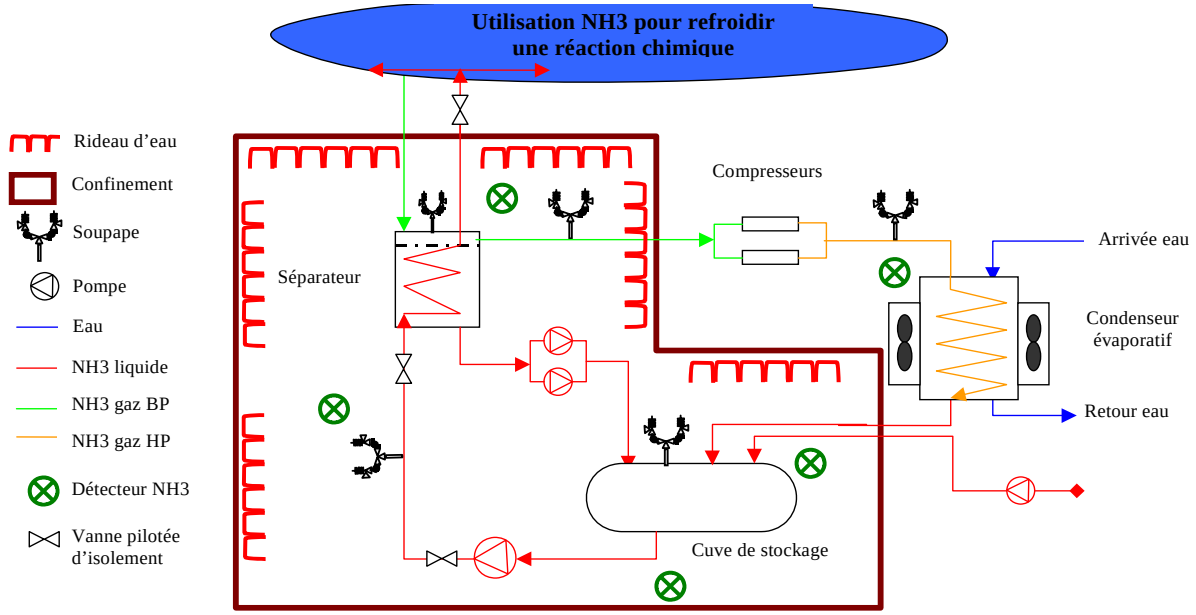

Figure 3.1-1 : Schéma de principe d'un réseau de refroidissement à l'ammoniac

3.2 Eléments permettant de définir les fonctions instrumentées de sécurité

Le but de l'analyse est de définir les FIS de ce système ainsi que leur SIL. Il est donc nécessaire que les risques soient identifiés dans un premier temps (tels que définis dans le paragraphe 2).

3.2.1. Identification des risques par l'examen des installations : Audit

Cette phase est primordiale pour l'étude. Elle représente une phase de prise de connaissance très importante, car de sa justesse dépend la validité de l'étude réalisée. L'examen des installations a permis d'identifier les produits et les équipements mis en œuvre dans ce système ainsi que les spécificités de l'environnement afin de déterminer les potentiels de dangers. Il permet également de prendre en compte les documents existants et les études de sécurité déjà réalisées.
L'examen a identifié les points suivants :

- Risque de perte de confinement de l'ammoniac par rupture mécanique ou soulèvement de soupape définie dans une étude de risque inhérent au site
- Dans le cas des scénarios majorants, les distances d'effet létal sont limitées au site industriel
- Une fiche d'accident relate un cas de rejet d'ammoniac gazeux par soulèvement de soupape
- Les systèmes instrumentés assurent à la fois des fonctions de conduite et de sécurité
- Aucune information sur les événements initiateurs et leurs fréquences d'occurrence, ainsi que sur les probabilités de défaillances des barrières de sécurité n'est disponible.

Ces données étant insuffisantes pour identifier les FIS et de définir leur SIL, il est donc nécessaire de compléter ces données par le retour d'expérience et les avis d'experts.

3.2.2 Identification des risque par le retour d'expérience en accidentologie

Une recherche d'accidents sur la base de données d'accidentologie ARIA du Bureau d'Analyse des Risques et Pollutions Industrielles (BARPI) du service de l'Environnement Industriel à la Direction de la Prévention des Pollutions et des Risques du Ministère de l'Ecologie et du Développement Durable.
pour des installations impliquant de l'ammoniac permet d'identifier les dangers suivants :

- la rupture d'une canalisation véhiculant de l'ammoniac,
- l'éclatement mécanique de capacités,
- l'explosion d'un nuage de vapeurs inflammables d'ammoniac,
- l'épandage d'une solution contenant de l'ammoniac.

Le BARPI à réaliser une étude de retour d'expérience sur ce type d'installation [8] [9].135 cas d'accidents entre 1992 et 2001 impliquant l'ammoniac ont été identifiés et répartis comme présenté dans le tableau 3.2-1.

Tableau 3.2-1 : Récapitulatif des accidents entre 1992 et 2001

Type d'accident (135 cas)	France (91 cas)		Etranger (44 cas)	
	Nb cas	%	Nb cas	%
Rejets dangereux (NH_3/ NH_4OH)	66	72,5	43	97,7
➔ Dans l'air	47	51,6	41	93,2
➔ Dans l'eau (ou dans un égout)	16	17,6	2	4,5
Rejet NH_3/ NH_4OH non précisé	24	26,4	2	4,5
Sans objet (aucune fuite constatée)	5	5,5	-	-
Incendies	29	33,8	15	34,1
Explosions	2	2,2	21	47,7
Projections, chutes d'équipements	2	2,2	-	-
Presque accidents	1	1,1	-	-
Effets domino	7	7,7	4	9,1

Cette recherche a permis de prendre en compte le retour d'expérience après accidents sur des installations similaires ainsi que les recommandations définies suite à ces accidents.

3.2.3. Identification des risques par l'avis d'experts

Des travaux sur les barrières de sécurité relatives à l'emploi de l'ammoniac dans les établissements industriels [10] réalisés par l'INERIS et par des organismes similaires ont permis de compléter les données recueillies précédemment.

Ce complément d'informations a permis de s'assurer de la mise en œuvre des moyens nécessaires pour maîtriser le risque et fixer des recommandations dans le cas contraire.

3.3 Définition des fonctions instrumentées de sécurité

Les fonctions de sécurité à assurer sur le réseau de refroidissement à l'ammoniac ont été identifiées grâce aux éléments recueillis dans les différentes étapes d'identification de risques présentées auparavant. Les fonctions instrumentées de sécurité, indépendantes des fonctions de contrôle et de régulation, pour lesquelles il faut déterminer le SIL ont pu être déterminées. Parmi toutes ces fonctions, nous pouvons citer :

- le contrôle de la pression dans le réseau gaz avec déclenchement d'alarme et démarrage des compresseurs lorsque des seuils critiques sont atteints
- le système de détection de gaz NH3 dans la zone de stockage pour contrôler et surveiller la concentration de gaz en cas de fuite (risques toxique et explosion).

Cette étape permet d'associer une ou des fonctions à un risque donné. Ces fonctions peuvent être existantes ou à implanter afin de maîtriser le risque.

3.4 Détermination du SIL et choix de la méthode

Le choix de la méthode dépend principalement de la nature des données à notre disposition suite à l'analyse des risques. Nous n'avions pas d'éléments sur les événements initiateurs et leur fréquence d'occurrence, ainsi que sur les probabilités de défaillance des barrières de sécurité. Cependant, l'analyse des risques a fourni les données suivantes :

- distances d'effet
- nombre de personnes exposées
- temps d'exposition
- les différentes possibilité d'éviter le dangers
- le retour d'expérience du site en termes d'accidentologie

Le graphe de risque s'est donc imposé dans ce cas puisque les valeurs des données d'entrées n'étaient pas assez précises. La quantification n'aurait donc pas eu de sens.

Une phase de calibrage ou d'étalonnage des paramètres du graphe de risque (tableau 2.1-1) fut nécessaire. Elle a permis de prendre en compte les spécificités de l'entreprise et le retour d'expérience.

Le tableau 3.4-1présente l'affectation du SIL des fonctions instrumentées de sécurité définies auparavant. Les paramètres de hiérarchisation du niveau de sécurité sont les suivants.

La conséquence du risque sur les personnes a été fixée à C_c étant donné l'étendue du site (assez importante). Une fuite d'ammoniac peut avoir des effets létaux mais limités au site ;

La fréquence d'exposition au risque a été évaluée au niveau F_B car une présence humaine permanente est envisagée dans la zone dangereuse considérée ;

La possibilité d'éviter le danger est considérée au niveau P_A lorsqu'il existe d'autres moyens de prévention ou de protection pour éviter le phénomène dangereux et P_B dans le cas contraire ;

Enfin en ce qui concerne la probabilité d'occurrence de l'explosion, le seuil W1est pris car ce danger ne s'est jamais produit sur le site En revanche, pour le débordement ou soulèvement par les soupapes le seuil est évalué à W_2 car ce danger a déjà été observé une fois sur le site (données relevées lors de la visite sur site).

Tableau 3.4-1: Affectation des niveaux de SIL

Fonction Instrumentée De Sécurité	**Risque combattu Conséquences (C)**		**Fréquence d'exposition (F)**	**Possibilité d'évitement (P)**		**Probabilité d'occurrence (W)**	**SIL**
Contrôle de pression dans le réseau gaz avec déclenchement d'alarme et démarrage des compresseurs lorsque des seuils critiques sont atteints	Soulèvement des soupapes	C_C	F_B	aucun	P_B	W2	3
Système de détection de gaz NH3 dans la zone de stockage pour contrôler et surveiller la concentration de gaz en cas de fuite (risque toxique et explosion)	Explosion	C_C	F_B	aucun	P_B	W1	2
	Nuage toxique	C_C	F_B	aucun	P_B	W2	3

Cette méthode est la plus simple d'utilisation. Cependant le SIL requis peut facilement varier d'un niveau en fonction des incertitudes sur les paramètres d'entrée. La méthode LOPA est en principe plus précise à condition que les données chiffrées en probabilité d'évènement et de défaillance reposent sur des données validées et pertinentes.

4. CONCLUSION

La norme EN 61511 offre une démarche globale de maîtrise de risques à travers une méthode qui va de l'analyse de risque jusqu'à l'évaluation du système instrumenté de sécurité. La quantification du niveau de sécurité est associée à un facteur de réduction de risque, ce qui permet d'apprécier la contribution de la fonction instrumentée de sécurité à la réduction de risque de l'installation. Cette démarche se base sur un ensemble de recommandations qui tendent à maîtriser le risque par des méthodes d'analyses cohérentes. Cet article présente différentes méthodes de détermination de SIL, dont une méthode est illustrée à travers un cas réel. L'application montre qu'une première étape indispensable, reposant sur un audit sur site, permet d'analyser le fonctionnement de l'installation et ses principales caractéristiques et de rassembler les éléments disponibles. La deuxième étape permet, quant à elle, de définir les fonctions instrumentées de sécurité ainsi que leur SIL requis en s'appuyant sur les informations fournies par l'exploitant et les spécificités du site étudié (retour d'expérience) et complétée par l'expertise dans le domaine considéré. Le choix de la méthode de détermination du SIL dépend essentiellement de la nature des données d'entrée. Il est préférable de bien utiliser une méthode qualitative (graphe de risque ou matrice de criticité) que d'utiliser une méthode quantitative lorsque les données d'entrée (fréquences d'occurrence d'événements initiateurs, probabilités de défaillance des barrières de sécurité) sont insuffisantes. Ces dernières s'appliqueront mieux lorsqu'il y a des données de retour d'expérience quantifiées et lorsque l'organisation du site permet une analyse en couches fonctionnelles indépendantes.

5. REMERCIEMENTS

Les auteurs tiennent à remercier le Laboratoire d'évaluation des équipements électriques (LEEL) de l'Institut national de l'environnement industriel et des risques (INERIS). Nous remercions également et tout particulièrement le Ministère de l'Écologie, de l'Énergie, du Développement Durable et de l'Aménagement du Territoire (MEEDAT) qui finance nos recherches.

6. RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Commission Electrotechnique Internationale, 1998, CEI 61508 (partie 1, 4 et 5) Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité. Commission Electrotechnique Internationale.

[2] Commission Electrotechnique Internationale, 2003, CEI 61511 (partie 1, 2 et 3)Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le domaine de la production par processus.,.

[3] Circulaire du 29 septembre 2005 relatif 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, Ministère de l'Ecologie et du Développement Durable, France

[4] CCPS of the AICHE , 2001, Layer of Protection Analysis, simplified process risk assessment, New York.

[5] Arrêté du 29 septembre 2005 modifiant l'arrêté du 10 mai 2000 modifié relatif à la prévention des accidents majeurs impliquant des substances ou des préparations dangereuses présentes dans certaines catégories d'installations classées pour la protection de l'environnement soumises à autorisation, Ministère de l'Ecologie et du Développement Durable, France

[6] Arrêté du 29 septembre 2005 relatif à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des installations classées soumises à autorisation, Ministère de l'Ecologie et du Développement Durable, France

[7] Ashgate Publishing Ltd, 2006, Resilience Engineering - Concepts and Precepts, Erik Hollnagel, David D. Woods, Nancy Leveson.

[8] Ministère de l'environnement, , février 1995, l'ammoniac et la réfrigération, SEI/BARPI ED0389.

[9] Ministère de l'environnement, 2002, l'ammoniac et la réfrigération, Complément.

[10] INERIS, Octobre 2002, Synthèse sur les barrières techniques de sécurité disponibles en matière de prévention des accidents - Ammoniac, France.