Allocations de SIL requis des fonctions instrumentées de sécurité d'une installation lorsque l'analyse de risques est imcomplète

Ahmed Adjadj, Dominique Charpentier

ALLOCATION DE SIL REQUIS DES FONCTIONS INSTRUMENTEES DE SECURITE D'UNE INSTALLATION LORSQUE L'ANALYSE DE RISQUE EST IMCOMPLETE

Adjadj Ahmed, Charpentier Dominique

INERIS
Parc Technologique ALATA BP 2
60 550 – Verneuil en Halatte – France
33 (0) 3 44 55 68 53 – 33 (0) 3 44 55 69 77, ahmed.adjadj@ineris.fr

Résumé :

La norme CEI 61511 décrit différentes méthodes d'allocation de SIL (Safety Integrity Level), qu'elles soient qualitatives ou quantitatives. Aucune méthode n'est à privilégier, le choix d'une technique dépendra de différents critères comme le montre cet article. Nous présentons les critères qui orientent le choix d'une méthode et indiquons les avantages et les inconvénients de ces différentes méthodes. Une application sur une unité de stockage d'ammoniac est présentée afin d'expliciter notre démarche.

Abstract :

The IEC 61511 standard describes various quantitative and qualitative methodology for SIL (Safety Integrity Level) allocation. The choice for one or another methodology will depend on various criteria as illustrated in this paper. We present the selection criteria of a method and we indicate the advantages and the disadvantages of these various methods. In order to illustrate our methodology, we took the example of an ammonia storage.

Mots clés : réduction de risque, CEI 61508, CEI 61511, Sécurité Fonctionnelle, Fonctions Instrumentées de Sécurité (FIS), Niveau d'intégrité de sécurité (SIL)

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 : Safety Integrity Level) pour une Fonction Instrumentée de Sécurité par rapport à l'analyse de risque. Il n'y a pas de règle imposée par ces normes mais des méthodes d'allocation du SIL, plus au moins adaptées en fonction du niveau de détail des analyses de risques réalisées au préalable ainsi que du type et du détail des informations disponibles.
La réduction de risque nécessaire apportée par les Fonctions Instrumentées de Sécurité, pour un objectif de risque résiduel défini, est déterminée en fonction de la contribution des autres systèmes de sécurité. Les données nécessaires à la définition 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 qualitatives (le graphe de risque [1] et [2] ou la grille de criticité [6]) et d'autres sont quantitatives (LOPA : Layer of Protection Analysis [3]). 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 à titre d'exemple.

2 – Organisation d'une étude de sécurité conformément à la norme CEI 61511

Pour toute installation industrielle, il est nécessaire de définir les situations dangereuses, puis de prendre les mesures destinées à supprimer les risques d'accident 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,
- 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.

Toutes ces données ne sont pas toujours accessibles ou n'existent pas. Dans ce cas, un audit de l'installation permet de recenser les documents existants et d'identifier les risques potentiels et les barrières de sécurité existantes. Il permet de rassembler les éléments nécessaires à la définition du SIL et d'identifier les analyses complémentaires à mener.

3 – Méthode de détermination des niveaux d'intégrité de sécurité exigés

La norme CEI 61511 décrit différentes méthodes de détermination de SIL : des méthodes qualitatives telles que le graphe de risque et la grille de criticité et des méthodes quantitatives telles que LOPA (Layer of Protection Analysis).

3.1 – Le Graphe de risques

Le graphe de risque (Figure 001) 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).

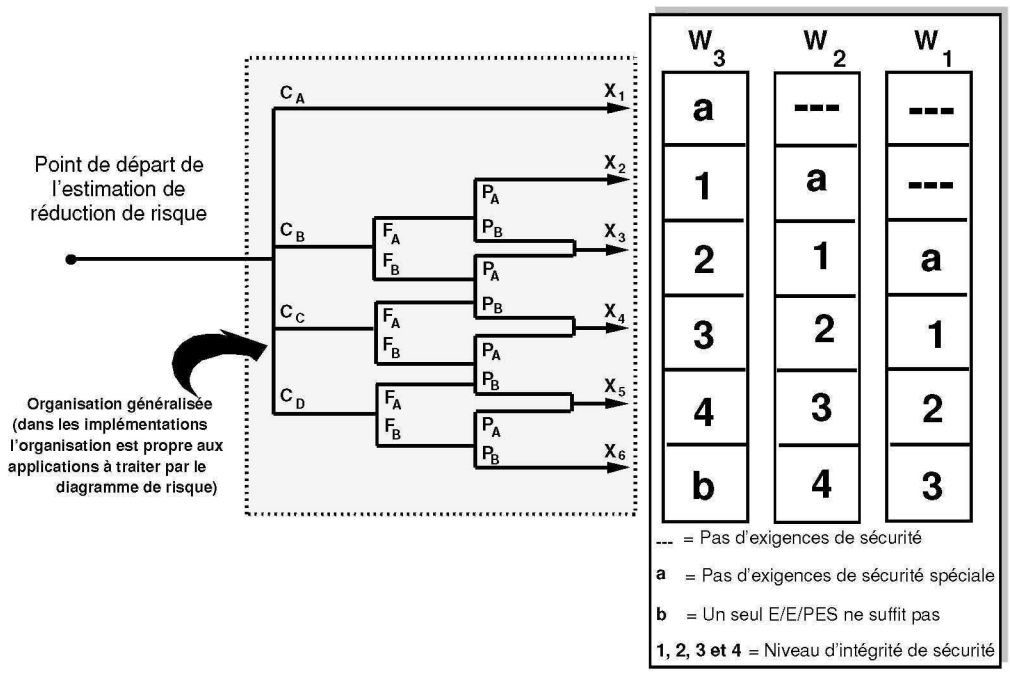

Figure 001 : Graphe de hiérarchisation du risque

La classification repose sur une hiérarchisation en 6 classes d'exigences graduées de "a, SIL 1 à SIL 4, b" dans laquelle la catégorie "a" ne correspond à "aucune exigence particulière de sécurité" et "b" est inacceptable (le système instrumenté est insuffisant).

Les niveaux affectés aux paramètres du graphe constituent la base de l'évaluation du risque. Une phase de calibration ou d'étalonnage du diagramme de risque est nécessaire (Tableau 003). Elle permet d'adapter les paramètres en prenant en compte les spécificités de l'entreprise et la réglementation.

3.2 – La Grile de criticité

L'analyse de risque consiste à positionner les différents scénarios d'accidents 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 de l'arrêté du 21/09/05 [4] et [5] et sur la grille de criticité (Tableau 001) de sa circulaire d'application [6].

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

Tableau 001 : Grille d'analyse de la justification des mesures de maîtrise du risque

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».

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 EN 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'accident, 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.

3.3 – LOPA (Layer Of Protection Analysis)

Contrairement aux techniques d'évaluation des risques purement qualitatives, l'analyse des couches de protection (Tableau 002) permet d'estimer la fréquence d'un événement redouté. Cette méthode [3] intègre toutes les couches de protection de l'entreprise, tant organisationnelles que techniques. Elle 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:
1. Définir l'impact de l'événement redouté (gravité);
2. Déterminer et énumérer tous les événements initiateurs;
3. Déterminer et énumérer toutes les couches de protection qui empêchent la propagation de l'événement initiateur conduisant à l'événement redouté;
4. Déterminer la fréquence des événements initiateurs, basée sur des données de REX et/ou de jugement d'experts;
5. Déterminer l'efficacité des couches de protection en probabilité de défaillance sur demande, basée sur des données de REX et/ou de technologie;
6. Calculer la fréquence de l'événement redouté.

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}	**…**						

Tableau 002: Exemple de tableau LOPA

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 ci-dessus, un SIL 3 est requis pour l'événement redouté "Défaillance boîte froide" et de 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).

4 – Application à une installation industrielle

4.1 – Description de l'installation

L'installation est un réseau de refroidissement à l'ammoniac (Figure 002). Elle permet de contrôler une réaction dans des réacteurs.

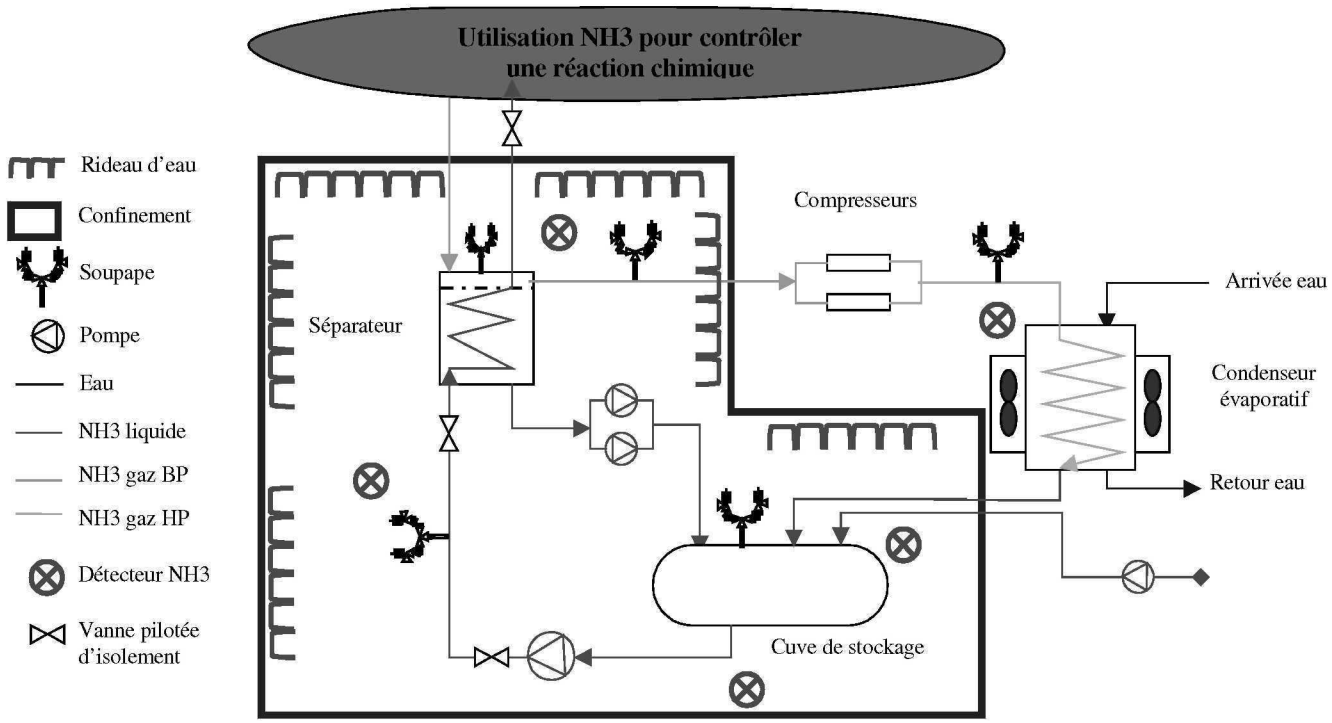

Figure 002 : Schéma de principe d'un réseau de refroidissement à l'ammoniac

4.2 – 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).

4.2.1 – 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 insuffisante 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.

4.2.2 – Identification des risque par le retour d'expérience en accidentologie

Une recherche d'accidents sur la base de données ARIA du BARPI [7] 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.

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.

4.2.3 – Identification des risque par l'avis d'experts

Des travaux sur les barrières de sécurité relatives à l'emploi de l'ammoniac dans les établissements industriels [8] 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 ouvre des moyens nécessaire pour maîtriser le risque et fixer des recommandations dans le cas contraire.

4.3 – Définition des fonctions instrumentées de sécurité

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

- contrôle de pression dans le réseau gaz avec déclenchement d'alarme et démarrage des compresseurs lorsque des seuils critiques sont atteints
- 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.

4.4 – 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

Nous avons donc opté pour le graphe de risque qui s'imposait dans ce cas de figure.

Une phase de calibration ou d'étalonnage des paramètres du graphe de risque (Tableau 003) fut nécessaire. Elle a permis de prendre en compte les spécificités de l'entreprise et le retour d'expérience.

Le tableau 004 présente l'affectation du SIL des fonctions instrumentées de sécurité définies auparavant. Les paramètres de hiérarchisation du niveau de sécurité ont été définis pour les raisons suivantes :

- C_c pour la conséquence du risque sur les personnes car vu l'étendue du site (assez importante), une fuite d'ammoniac peut avoir des effets létaux mais limités au site ;

- F_B pour la fréquence d'exposition au risque car il y a une présence permanente de personnes dans la zone dangereuse considérée ;

- P_A pour la possibilité d'éviter le danger lorsqu'il existe d'autres moyens de prévention ou de protection pour éviter le phénomène dangereux considéré et P_B dans le cas contraire ;

- W1 pour la probabilité d'occurrence de l'explosion car cela n'a jamais été observé sur le site et W_2 pour le débordement ou soulèvement par les soupapes car cela a déjà été observé une fois sur le site (données relevées lors de la visite sur site).

Cette méthode est la plus simple d'utilisation cependant le SIL requis peut facilement varier d'un niveau en fonctions 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.

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)

Tableau 003: Etalonnage des paramètres du graphe de risque

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

Tableau 004: Affectation des niveaux de SIL

5 – 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 exemple.

L'exemple 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.

Références :

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

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

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

[4] *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

[5] *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

[6] *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

[7] Base de données d'accidentologie ARIA du BARPI, *Bureau d'Analyse des Risques et Pollutions Industrielles 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*, France

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