Etude HAZOP/SIL de l'unité de granulation au sein de Yara Tertre

Cet article fait suite à une première expérience dans l'industrie Seveso seuil haut et explique le fondement de la méthode HAZOP, un des moyens les plus utilisées dans l'analyse du risque au sein du monde industriel, notamment dans le domaine chimique. Afin d'aller plus loin et d'innover, la méthode HAZOP est couplée à la méthode LOPA permettant d'obtenir l'HAZOP/SIL, permettant d'ajouter une notion de semi quantification. Différents principes sont également abordés comme le diagramme de Farmer, le modèle du fromage suisse, la méthode LOPA ou encore la quantification SIL.

Mots-clés : Analyse de risque, HAZOP, SIL, LOPA, Défaillance de barrières.

This article follows a first experience in the Seveso high threshold industry and explains the basis of the HAZOP method which is one of the most used methods in the industrial world risk analysis, especially in chemical industry. In order to go further and innovate, the HAZOP method is coupled with the LOPA method to obtain HAZOP/SIL, adding a notion of semi-quantization. Different principles are also discussed such as the Farmer diagram, the Swiss cheese model, the LOPA method or the SIL quantification.

Keywords : Risk analysis, HAZOP, SIL, LOPA, barrier failure.

Ing. C. COPPIN
Ing. Y. LECLERCQ
Ir. V. VAN ROOST
Ecole d'Ingénieurs, HELHa Mons

1. Introduction

La production de ressources en masse est une nécessité aujourd'hui afin de subvenir à nos besoins. Afin de pouvoir toujours produire plus et plus spécifiquement pour ce travail dans le domaine de la chimie, il faut s'assurer de maintenir un risque acceptable afin d'éviter toute catastrophe industrielle. Peu importe votre orientation professionnelle et votre domaine, vous allez être sans doute confronté à des analyses de risque dans votre carrière car elles doivent impacter un corps pluridisciplinaire.

Cet article fait suite à un stage réalisé chez Yara à Tertre qui est une usine chimique Seveso seuil haut. Le domaine chimique est un domaine où il est nécessaire de comprendre les risques et de les maitriser. Cette affirmation est d'autant plus vraie que ce travail a été produit suite à un stage dans l'unité de granulation produisant de l'engrais azoté afin de pouvoir comprendre les dangers de ce type d'installation qui produit un engrais pouvant exploser sous certaines conditions.

Afin de démontrer la nécessité de réaliser des analyses de risque, il suffit d'étudier l'accidentologie. L'exemple d'AZF semble être tout indiqué de par la similitude des produits et la proximité. L'usine AZF implantée à Toulouse a subi une explosion d'un stock de nitrate d'ammonium qui est l'élément constitutif des engrais azotés, ce qui a causé la mort de plus de 31 personnes et blessé plus de 2500 autres. Cet accident industriel n'est qu'un parmi un grand nombre, dont 17 uniquement concernant le nitrate d'ammonium avec l'accident d'Oppau en Allemagne qui a causé la mort de 561 personnes en 1921.

C'est donc dans ce contexte qu'une des méthodes d'analyse de risques vous sera présentée. Cette méthode est une des méthodes les plus utilisées et fournit un compromis entre vitesse et résultats semi-quantitatifs.

2. Le nitrate d'ammonium

Bien que les analyses de risques soient effectuées sur les procédés en général que ce soit de l'acide nitrique, de l'ammoniac ou pour ce travail du nitrate d'ammonium, il est nécessaire avant de commencer une analyse de risque de comprendre le danger que représentent les produits utilisés.
Le nitrate d'ammonium est produit dans un procédé industriel à partir d'ammoniac et d'acide nitrique selon la réaction exothermique suivante :

$$NH_{3\,g} + HNO_{3\,l} \rightarrow NH_4NO_{3\,s} \qquad \Delta H = -146kJ/mole$$

Le nitrate d'ammonium présente différentes propriétés physiques intéressantes comme des changements de forme cristallographique mais surtout peut subir des réactions de décomposition menant à une explosion.
Il existe deux types de nitrate d'ammonium. Le premier est le nitrate d'ammonium de qualité technique utilisé comme explosif et qui possède une grande porosité, une faible densité et avec une teneur en azote proche de 34,8%. Le second est le nitrate d'ammonium de qualité engrais qui possède une densité plus élevée et une porosité faible ainsi qu'une teneur en azote de 33,5% en masse. Cette explication permet vite de se rendre compte que la possibilité de dégrader le nitrate d'ammonium et d'arriver à des réactions explosives est réelle. Les réactions de décompositions principales vont être détaillées par la suite.

La première réaction possible est une réaction de décomposition endothermique qui se produit à partir de 170°C qui est une température légèrement supérieure à la température de fusion :

$$NH_4NO_{3\,s} \rightarrow NH_{3\,g} + HNO_{3\,g}$$

A partir de 180°C, il est possible d'avoir une réaction de décomposition exothermique qui forme le protoxyde d'azote :

$$NH_4NO_3 \rightarrow N_2O + 2H_2O$$

Il existe un grand nombre de réactions de décompositions différentes qui n'ont pas été représentées dans cet article. Il faut savoir que les réactions de décomposition deviennent auto-entretenues à partir de 210°C, ce qui veut dire qu'à partir de 210°C il est probable d'observer un emballement thermique.
Il est nécessaire d'ajouter deux aspects : tout d'abord la température de décomposition à partir de laquelle la réaction devient auto-entretenue peut être abaissée par la présence de catalyseurs comme des métaux, des matières organiques, des chlorures ou encore un milieu acide.
Par la suite pour obtenir un caractère explosif du nitrate d'ammonium, il faut qu'il soit soumis à une mise sous pression comme dans un incendie par exemple avec un tas de gravats.

3. Méthodologie

3.1. Introduction à la sécurité industrielle

Avant de parler de sécurité industrielle, il est nécessaire de parler du risque. *Le risque est la combinaison de la fréquence d'occurrence de la conséquence finale d'un évènement avec sa gravité.*

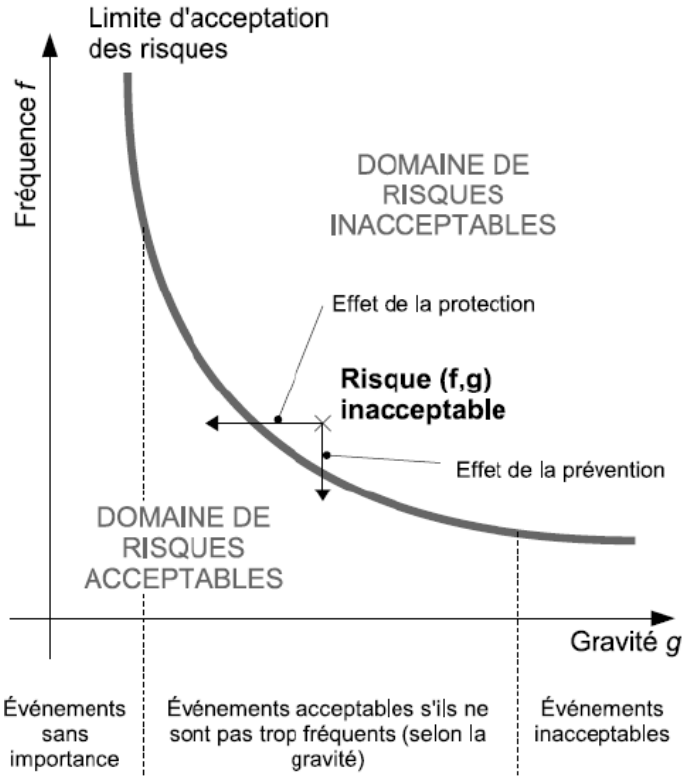


Figure 1 : Diagramme de Farmer

Le diagramme de Farmer relie la gravité à la fréquence d'un évènement. Il permet de bien imaginer la définition du risque car un accident / incident qui est très grave mais peu fréquent possède le même risque qu'un phénomène fréquent mais peu grave.
Il est ainsi possible d'obtenir une courbe iso-risque représentée sur la figure ci-contre où le risque est acceptable en dessous et inacceptable au-dessus de la limite.
Dans le cas où une mesure permet de réduire la fréquence et/ou la gravité par des mesures de prévention ou de protection, un risque plus faible qu'initialement est atteint.

Le modèle du fromage suisse permet d'avoir une image générale et simplifiée de la sécurité industrielle. Dans le modèle du fromage suisse comme dans l'étude HAZOP/SIL, une déviation du système va se produire menant à un accident ou à un incident qui peut engendrer une conséquence quantifiée par son risque (fréquence et gravité).

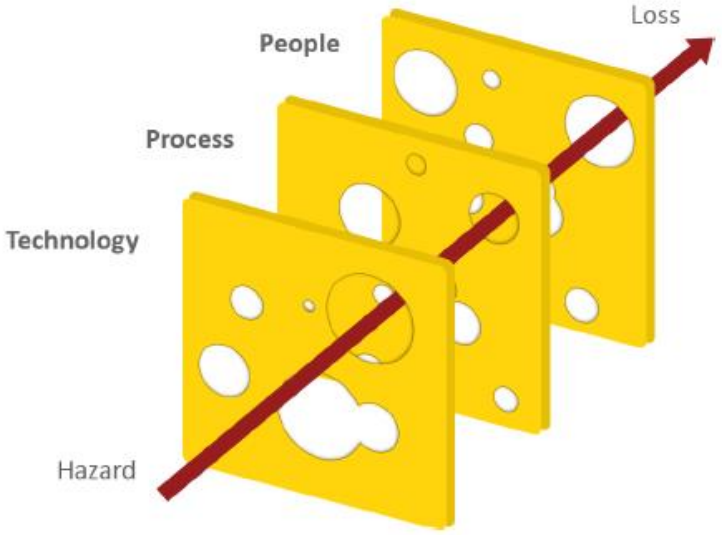


Figure 2 : Modèle du fromage suisse de James Reason

Le danger ici, peut être par exemple une augmentation de température du nitrate d'ammonium. Sur le chemin de cette déviation menant à un événement final tant redouté, se trouvent des barrières. Il existe différents types de barrières qui seront détaillées dans la suite de l'article. Le nom de ce modèle provient du fait que chaque barrière peut être défaillante à un moment donné et que chaque barrière peut empêcher le scénario de se dérouler. La conséquence finale, ici une décomposition du nitrate d'ammonium voire une explosion se produit seulement si la déviation n'est pas arrêtée par les barrières, autrement dit si les barrières sont toutes défaillantes à un même moment. Plus il y a de barrières et plus elles sont efficaces, plus le risque résiduel sera faible.

Trois méthodes vont être détaillées par la suite ; chaque méthode va être une partie d'une grande méthode qui s'appelle la méthode HAZOP/SIL. Elles doivent donc travailler en synergie afin de pouvoir former un outil d'analyse de risque.

4. La méthode HAZOP

La méthode HAZOP a été développée par la Société Imperial Chemical Industries en 1974. C'est une méthode qui vise à étudier les causes et les conséquences qui pourraient survenir par les déviations du système. Le but est de créer le plus possible de scénarios d'accident pour obtenir ainsi le plus grand nombre de causes et de conséquences différentes. Pour faire une analogie avec le modèle du fromage suisse, le but est d'obtenir un grand nombre de déviations et ensuite de conséquences finales sans barrières, qui sont représentées par les tranches de fromage.

La méthode HAZOP doit être réalisée par une équipe pluridisciplinaire comportant entre 3 et 5 personnes. L'équipe doit au moins comporter :

- Un chef de projet ;
- Un spécialiste en instrumentation ;
- Un ingénieur possédant une bonne connaissance dans l'exploitation du procédé ;
- Un contremaitre avec une bonne expérience du procédé étudié.

Le chef de projet est un HAZOP leader qui possède une connaissance dans la gestion des HAZOP. Il a un but primordial car il aide à la formation de l'équipe pluridisciplinaire, il demande l'avis à chacun pour obtenir par la suite un consensus. La méthode HAZOP nécessite en plus de l'équipe pluridisciplinaire certains documents à jour comme des P&ID, Cause and Effect Diagram, la connaissance des régulations ou autres liens logiques dans le procédé étudié.

La méthode HAZOP se base sur les déviations du système. Les déviations sont la combinaison d'un mot clé avec un paramètre physique. Les principaux mots clés sont : *more, less, as well as, part of, other than, reverse, not.* Une fois combiné avec un paramètre physique comme *la température, la pression* ou encore *le débit*, une déviation est obtenue. Ainsi avec un paramètre physique comme le débit, la déviation augmentation, diminution ou encore absence de débit pourront être étudiées. Etablir la liste des déviations est la première étape. Cette liste parfois déjà fournie dans des fichiers HAZOP permet d'imaginer les différents scénarios.

L'étape suivante est l'étude des causes pour chaque déviation. Il est important pour chaque déviation de trouver le plus grand nombre de causes car le but d'une analyse de risques est d'être le plus complet possible. Les causes peuvent être multiples ; l'erreur humaine est souvent mise en avant par l'ouverture ou la fermeture de vanne manuelle, des problèmes de régulation par la défaillance du capteur ou encore de la vanne qui peuvent amener à des *more flow, less flow, no flow* voire *high temperature* ou *less temperature* dans le cas où le flux est de la vapeur. Dans des procédés où la

température peut induire des dangers, un problème de régulation induisant une mauvaise désurchauffe est souvent une source d'occupation car la fermeture de la vanne d'alimentation d'eau par un problème de capteur va directement engendrer une vapeur surchauffée.

Une fois une cause identifiée, il faut trouver les conséquences de la déviation sur le système. Pour ce faire, il est obligatoire de ne **jamais considérer des barrières de prévention ou de protection** qui pourraient diminuer le risque. Le but ici va être d'évaluer la conséquence qui pourrait être obtenue dans le cas où toutes les barrières sont défaillantes. Cette méthode permet de montrer une conséquence ultime d'un accident/incident et va permettre de calculer un risque initial ; le scénario doit donc être considéré à nu. Ensuite, il faudra dans la méthode suivante estimer la réduction que fourniront les barrières présentes dans le scénario et estimer si elles sont suffisantes ou pas.
En reprenant le modèle du fromage suisse de James Reason, la méthode HAZOP permet d'imaginer les dangers, leurs causes et les conséquences en sortie du fromage. Il faudra maintenant s'intéresser à une méthode de quantification du risque, aux barrières présentes dans le procédé et à une méthode d'évaluation de celles-ci afin de voir si elles sont suffisantes pour obtenir un risque acceptable.

5. Safety Integrity Level

Afin de comprendre comment le risque est quantifié, il faut se familiariser avec les niveaux SIL. Les niveaux SIL ont été définis dans la norme IEC 61508 et permettent de quantifier un risque. Plus précisément c'est un *niveau relatif inhérent à une fonction de sécurité que ce soit pour une installation ou encore un instrument*. Le niveau SIL peut prendre des valeurs de 0 jusqu'à 4 où 0 peut représenter un risque jugé acceptable et 4 représente le plus haut risque. Le niveau de SIL 0 peut ne pas nécessiter de barrières dans le cas où la fréquence de la gravité dans la matrice de risque interne de l'usine est assez faible. Dans d'autres cas, même si le niveau de SIL atteint 0, il sera nécessaire de fournir des barrières diminuant le risque. Comme le montre le tableau suivant, le niveau de SIL représente en réalité un facteur de réduction du risque.

Tableau 1 : Les niveaux de SIL

SIL	RRF - Facteur de réduction de risque
1	10 à 100
2	100 à 1000
3	1000 à 10 000
4	10 000 à 100 000

Le niveau de SIL va permettre de quantifier le risque en ayant des moyens d'évaluation et de comparaison. Il faut distinguer deux types de niveaux SIL :

- Le SIL **requis** représente le facteur de réduction du risque qu'il faut fournir afin d'obtenir un risque jugé acceptable. Ce niveau de SIL se base sur une matrice interne à l'entreprise.
- Le SIL **installé** est le facteur de réduction du risque qui est présent dans la société pour le scénario étudié précédemment et qui doit être comparé à celui requis.

Le SIL installé sera détaillé prochainement dans la méthode LOPA. Pour chaque scénario étudié dans l'HAZOP avec une déviation, une cause et des conséquences qui impacte la santé, l'environnement, il faudra estimer le risque qu'il représente en calculant le SIL requis.

Le risque comme défini auparavant est la combinaison de la **fréquence** de la conséquence avec sa **gravité**. Il faut ainsi définir pour chaque scénario imaginé dans la méthode HAZOP qui représente un impact sur la santé, l'environnement ou dans une moindre mesure économique une fréquence et une gravité. L'estimation de la fréquence d'un scénario final menant à une explosion qui n'a jamais eu lieu n'est pas chose aisée. Il ne faut pas oublier que pour l'HAZOP, il faut toujours considérer le procédé sans aucune barrière et donc **la fréquence de la cause du scénario sera égale à la fréquence de la conséquence finale** car rien n'empêchera le scénario de se dérouler. Pour gagner un temps considérable, l'analyse de risque va utiliser des classes de fréquence et de gravité.

Les classes de fréquence sont reprises ci-après :

Tableau 2 : Classes de fréquence de la méthode HAZOP

	Très fréquent	Fréquent	Peu fréquent	Très rare	Extrêmement rare	Presque impossible
Fréquence	> 1 fois/ an	> 1 fois/ 10 ans	> 1 fois/ 100 ans	> 1 fois/ 1000 ans	>1 fois/ 10 000 ans	> 1 fois/ 100 000 ans
Classe	F	E	D	C	B	A

Avant de commencer l'analyse de risque, il faut connaitre des fréquences classiques d'évènement. Bien qu'il soit possible de trouver des fréquences dans la littérature, il est souvent admis qu'une erreur humaine comme la fermeture ou l'ouverture d'une vanne manuelle possède une fréquence de classe E, autrement dit que ce scénario peut se dérouler entre une fois par an et une fois tous les dix ans. Une seconde défaillance souvent observée est celle pour la régulation qui possède une fréquence de classe D. Dans la méthode HAZOP classique, il est rare de considérer deux causes strictement nécessaires comme deux vannes en parallèle devant être fermées mais quand le scénario a déjà été rencontré ou doit être mis en avant, la cause peut être étudiée mais alors la fréquence sera abaissée.

Il faut estimer par la suite la gravité du scénario. Pour ce faire, il existe des tables avec des gravités qui peuvent évoluer d'un niveau minime à un niveau catastrophique. La gravité étudie trois paramètres : l'impact sur l'homme, l'environnement et dans une moindre mesure l'impact économique.

Un tableau interne à l'entreprise qui traduit ses valeurs doit classer des niveaux de gravité qui évolue d'un niveau minime à un niveau catastrophique pour les trois critères mentionnés. Ainsi pour un scénario étudié, il est nécessaire d'estimer la fréquence de la cause et la gravité des 3 paramètres séparément. Une fois la fréquence et les trois gravités obtenues, il faut utiliser la matrice interne à la société qui va permettre de calculer le SIL requis, autrement dit le facteur de réduction du risque à fournir.

Consequence	4 Frequent	3 Medium Frequency	2 Low frequency	1 Very rare	0 Extremely rare	-1 Nearly impossible
	..... down to 1/yr	>10-1/yr - 1/yr	>10-2/yr to 10-1/yr	>10-3/yr to 10-2/yr	>10-4/y to 10-3/yr	<10-4/yr to 10-4/yr
1 Severe	Redesign	4	3	2	1	ALARP
2 Major	Redesign	3	2	1	ALARP	ALARP
3 Moderate	Redesign	2	1	ALARP	ALARP	OK
4 Minor	Redesign	1	ALARP	ALARP	OK	OK
5 Minimal	-	ALARP	ALARP	OK	OK	OK

Figure 3 : Matrice interne à Yara

La matrice ici représentée est la matrice de Yara Tertre. Cette matrice reprend bien la **fréquence** avec **la gravité du paramètre le plus majorant**. Il existe ainsi plusieurs zones dans cette matrice. Une première zone est la zone verte qui juge que le scénario étudié possède un risque jugé acceptable.

Il ne faut donc pas absolument fournir une réduction de risque. La zone jaune est une zone dans laquelle il faut fournir une réduction du risque car le risque n'est pas totalement maitrisé. Elle peut devenir une zone ALARP (**A**s **L**ow **A**s **R**easonably **P**racticable) dans le cas où les solutions possibles de réduction du risque ne sont pas économiquement faisables. Ainsi même si un niveau de SIL 0 est requis, le scénario peut se retrouver soit dans la zone jaune ou dans la zone verte et nécessiter ou pas une barrière supplémentaire. La zone rouge est une zone dans laquelle il faut absolument fournir une réduction du risque et le niveau de SIL est présent dans la case. Enfin, la zone de Redesign est une zone inacceptable car selon Yara, il est intolérable de subir un accident/incident, peu importe sa gravité plus d'une fois par an.

6. La méthode LOPA

Après avoir découvert comment créer des scénarios avec la méthode HAZOP, ensuite comment pouvoir calculer le facteur de réduction du risque à fournir pour chaque scénario nécessitant une quantification, il faut maintenant s'intéresser à l'évaluation des barrières pour chaque scénario qui étaient représentées par les couches de fromage dans le modèle de James Reason. La méthode LOPA (**L**ayer **O**f

Protection **A**nalysis) permet de classer les barrières et donc de quantifier le facteur de réduction du risque présent dans l'installation pour un scénario étudié.

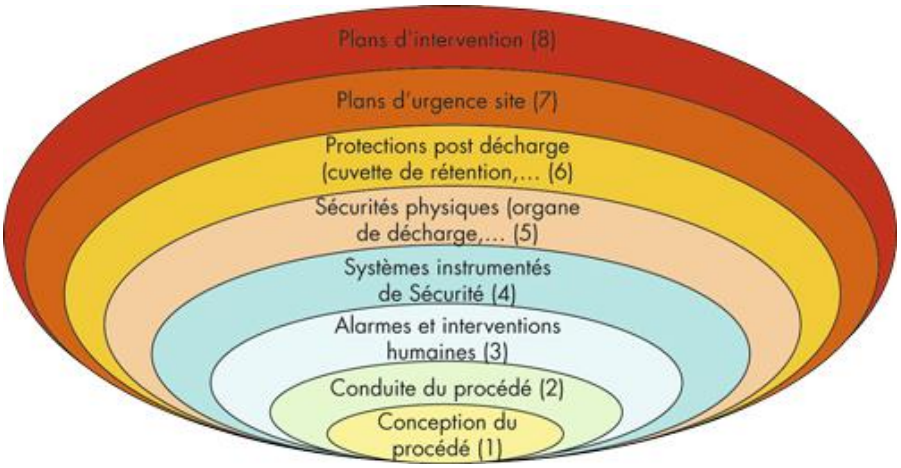


Figure 4 : Classification de la méthode LOPA

Il existe ainsi dans la méthode LOPA huit couches différentes permettant de diminuer le risque en jouant soit sur la prévention ou la protection. Les couches sont les suivantes :

- La conception du procédé permet dans certains cas d'éliminer des scénarios notamment en regardant la température ou la pression de design mais cela peut également être le cas avec un évent permettant dans le cas où il est bien dimensionné d'éviter toute surpression ;
- La conduite du procédé représente le système qui conduit le procédé en détectant des dérives. Cette couche englobe toute la régulation gérée par le BPCS (**B**asic **P**rocess **C**ontrol **S**ystem).
- Les alarmes qui engendrent des interventions humaines bien qu'elles soient gérées par le BPCS ne sont pas classées dans la même couche car c'est le facteur humain qui va être déterminant ;
- Le système instrumenté de sécurité, parfois appelé le SMS (**S**afety **M**anagement **S**ystem) permet par la prise de décisions de mettre le procédé ou une partie en sécurité sans intervention humaine et sans le BPCS par des fonctions de sécurité appelées SIF (**S**afety **I**nstrumented **F**unction);
- Les sécurités physiques ou sécurités passives sont notamment constituées de disques de rupture, de soupape ou d'antiretour ;
- La protection post décharge constitue la dernière barrière qui pourra être considérée dans l'analyse de risque et elle permet de réduire la conséquence.

Ce sont par exemple les cuvettes de rétention ou encore des systèmes de noyage ;
- Les deux dernières couches sont les procédures d'évacuation.

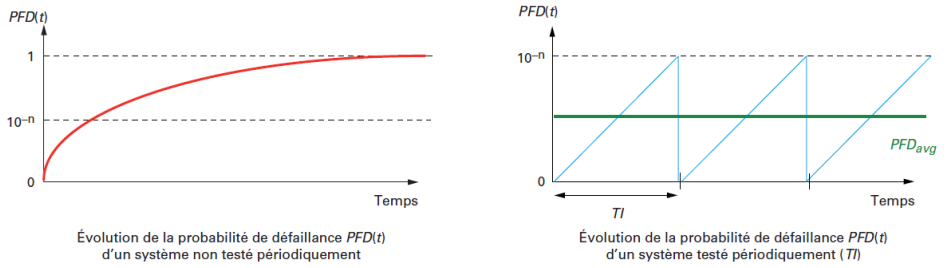
Deux notions sont nécessaires afin de comprendre les barrières qui pourront être considérées dans une analyse de risque. Tout d'abord le fait que **l'efficacité des barrières doit pouvoir être vérifiée**. L'efficacité englobe la réelle efficacité de la barrière, son temps de réponse et sa probabilité de défaillance. Deuxièmement, il faut absolument que les barrières soient considérées comme **indépendantes** (**I**ndependant **P**rotection **L**ayer) l'une de l'autre car si une des deux barrières est défaillante, il n'est pas certain que la seconde ne le soit pas. Avec ces deux notions, il est possible de connaitre les barrières qui peuvent être mises en évidence dans l'analyse de risque. Les deux dernières barrières qui sont les plans d'urgence ne peuvent donc pas être considérées comme des barrières car il n'est pas possible de prouver leur efficacité.
Afin de pousser le raisonnement plus loin, il ne faut jamais qu'il y ait un élément en commun entre les différentes barrières. Une régulation possède forcément au minimum un capteur, un système logique et enfin au minimum un actionneur. Dans le cas où un capteur possède à la fois une alarme et est utilisé pour la régulation, il ne pourra jamais fournir deux barrières car il n'est pas indépendant. En réalité, l'indépendance va plus loin car même s'il existe un second capteur qui n'a aucun lien avec une logique de régulation, il n'est pas possible de considérer deux barrières car le traitement informatique est le même (BPCS).

7. La probabilité de défaillance

Comme signalé auparavant, les différentes barrières représentées comme des couches de fromage dans le modèle de James Reason et classifiées par la méthode LOPA ne sont pas efficaces à 100%, d'où les trous présents dans le modèle du fromage suisse. Plus il y a de barrières indépendantes et plus elles sont efficaces et moins il sera facile de passer au travers de toutes au même moment. C'est donc pour cette raison qu'il faut s'intéresser aux défaillances des barrières après les avoir identifiées comme IPL dans le scénario étudié.

Dans le cas où une barrière doit intervenir à un moment donné, il faut comprendre ce qu'est la probabilité de défaillance à la sollicitation. La probabilité de défaillance à la sollicitation (PFD) est la probabilité que la barrière soit défaillante, autrement dit qu'elle ne remplisse plus sa fonction de sécurité. La partie de gauche de la figure 5 reprend la probabilité de défaillance d'une barrière qui évolue dans le temps. En effet si une barrière n'est pas inspectée régulièrement, il est fort probable que les capteurs ou actionneurs deviennent totalement défaillants après un temps trop long. La partie de droite reprend cette probabilité abaissée à une probabilité nulle à chaque

fois que la barrière est inspectée. Cette hypothèse est appelée l'hypothèse AGAN (**A**s **G**ood **A**s **N**ew) qui n'est pas représentative de la réalité car il n'est jamais possible de détecter toutes les sources de défaillances visibles ou non. Le temps d'inspection (TI) est important car plus il est court et plus la probabilité moyenne de défaillance à la sollicitation qui est tout simplement la moyenne de la probabilité de défaillance à la sollicitation dans le temps sera faible.



Évolution de la probabilité de défaillance *PFD*(*t*) d'un système non testé périodiquement

Évolution de la probabilité de défaillance *PFD*(*t*) d'un système testé périodiquement (*TI*)

Figure 5 : Probabilité de défaillance à la sollicitation

Il est donc nécessaire de connaitre la probabilité de défaillance de chaque barrière identifiée dans l'HAZOP. En fonction des barrières, il existe des méthodes différentes pour obtenir la PFD moyenne ; les PFD moyennes des barrières listées ci-dessous sont admises en littérature ou encore via des retours d'expérience.
Les barrières reliées au BPCS comme la régulation ou les alarmes possèdent une PFD moyenne de 10^{-1}. Dans la probabilité de défaillance à la sollicitation d'une régulation, il est en théorie nécessaire d'inclure la probabilité de défaillance des capteurs, logique et actionneurs afin d'obtenir une probabilité de défaillance qui englobe toutes les parties de l'équipement. Le calcul n'est pas réalisé pour la régulation mais va être beaucoup plus poussé par les systèmes instrumentés de sécurité (SIF) présentés dans les couches LOPA.

En réalité la réponse d'un opérateur à une alarme est très compliquée à chiffrer ; la norme IEC 61511-3 fournit la valeur de PFD moyenne de 10^{-1} mais elle doit normalement être fonction de l'expérience de l'opérateur, son taux de fatigue, le temps de réponse disponible et bien d'autres. Il existe différentes méthodes pour affiner si besoin l'estimation de cette probabilité de défaillance comme la TESEO (**T**echnica **E**mpirica **S**tima **E**rrori **O**peratori).

Pour les protections actives, le niveau de SIL dépend de la sécurité. Pour les soupapes, un niveau de 10^{-2} peut être atteint tandis que pour un clapet antiretour, le taux de défaillance est plus faible et il sera parfois possible de considérer une PFD de 10^{-3}.

Pour les protections passives comme les cuvettes de rétention ainsi que les évents, elles possèdent d'office une probabilité de défaillance à la sollicitation de 10^{-2}. Les probabilités de défaillance des sécurités passives ne sont pas évidentes à comprendre car une protection passive comme une cuvette de rétention est dimensionnée pour une certaine durée et intensité. Une fois que la durée ou l'intensité pour laquelle le dispositif a été dimensionné est dépassée, alors une défaillance peut être observée. Le chapitre suivant va détailler comment s'intéresser aux systèmes instrumentés de sécurité.

8. La probabilité de défaillance des fonctions instrumentées de sécurité

Afin de terminer l'évaluation des PFD moyennes pour ensuite pouvoir connaitre le niveau de SIL installé, il faut se pencher sur l'évaluation de cette probabilité de défaillance pour les fonctions instrumentées de sécurité (**S**afety **I**nstrumented **F**unction) qui sont essentielles dans la mise en sécurité des procédés industriels. Une SIF est constituée comme une régulation par au minimum un capteur, une logique et enfin au moins un actionneur. La SIF va permettre de mettre en sécurité l'unité sans l'intervention humaine dans le cas où les valeurs physiques du process dépassent des valeurs inacceptables. Afin d'appréhender les formules mathématiques pour calculer les probabilités moyennes de défaillance à la sollicitation, il faut se pencher sur les taux de défaillance et sur l'architecture des SIF.

8.1. Les taux de défaillance

Selon la norme IEC61508-4 une défaillance est un arrêt de la capacité d'une fonction de sécurité d'assurer son rôle. La norme IEC 61508-4 permet de distinguer deux types de défaillance. Tout d'abord des défaillances dangereuses menant à la difficulté voire l'incapacité du système de sécurité d'agir. La seconde est constituée des défaillances en sécurité où la conséquence est de modifier le système sans pour autant nuire à sa fonction de sécurité mais pouvant engendrer des déclenchements intempestifs. La défaillance dangereuse pour un capteur de pression sera de sous-estimer la pression et au contraire de la surestimer dans le cas d'une défaillance en sécurité. Il faut également différencier les défaillances qui sont détectées des non détectées avec des moyens de diagnostics, lors de son fonctionnement ou encore par des tests périodiques. Dans le cas où une barrière de sécurité subit une défaillance critique comme la cassure d'un capteur, il est possible d'installer une valeur « erreur » supérieure à la valeur critique déclenchant la protection ou une alarme. Cette méthode peut permettre de transformer certains taux de défaillance dangereux en taux de défaillance sûr détecté.

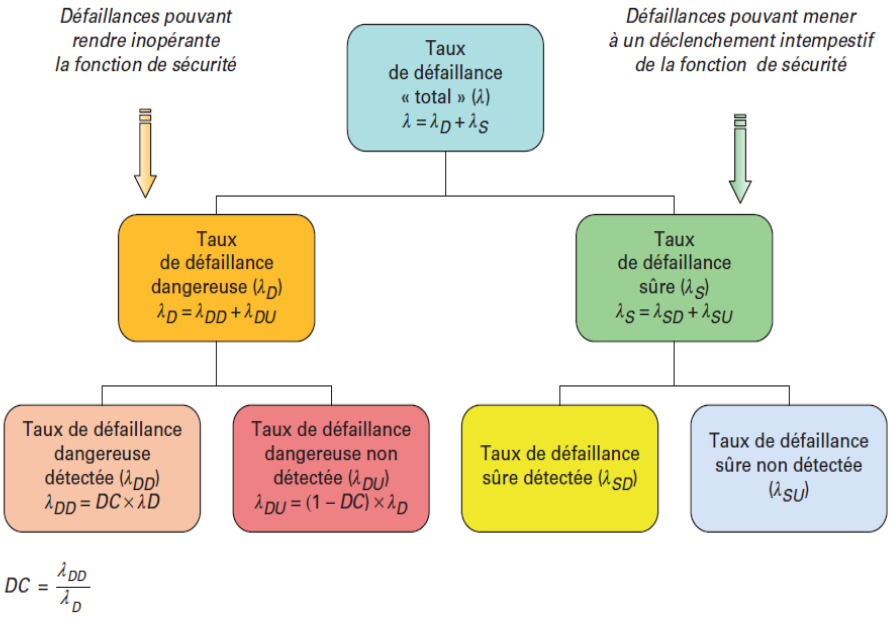


Figure 6 : Les différents taux de défaillance

8.2. L'architecture des SIF

K00N représente l'architecture, « K » signifie le nombre d'instruments qui va permettre de déclencher la sécurité et le « N » le nombre d'instruments au total pour la fonction de sécurité. Ainsi une architecture de capteur 1001 possède un capteur et nécessitera que l'unique capteur détecte le problème pour agir. Dans ce cas-ci, si le capteur ne fonctionne plus, une faille de sécurité apparaît. Il existe ainsi un grand nombre de structures possédant des caractéristiques fort différentes.

Les différentes architectures souvent abordées sont reprises ci-dessous :

- 1oo1 : Un seul élément est présent comme un capteur qui permet de pouvoir agir sur une fonction de sécurité. Si ce capteur subit une défaillance dangereuse alors la fonction de sécurité n'est plus assurée ; cependant si ce capteur subit une déviation haute, il va produire un déclenchement intempestif. Cette architecture ne permet pas d'être sécurisée car avec une seule défaillance dangereuse la fonction n'assure plus la sécurité nécessaire et ne permet pas d'avoir une disponibilité importante, car avec une seule défaillance non critique un déclenchement intempestif se produit.

- 1oo2 : Un seul des deux capteurs doit détecter une défaillance pour pouvoir agir sur une fonction de sécurité. Si un des deux éléments possède une

déviation haute, alors encore une fois un déclenchement a lieu ce qui pourrait par exemple arrêter l'installation. Comme cela peut être observé sur la figure 8, si les éléments en question sont des vannes d'ouverture d'eau de noyage par exemple en cas de haute température, il faut qu'une des deux vannes soit ouverte pour ainsi noyer le réacteur. Le raisonnement inverse peut être tenu pour la fermeture de vanne. Mais si une des deux déclenche sans raison du fait d'une déviation, alors le processus de sécurité est également activé. La sécurité est plus élevée que précédemment mais la disponibilité est plus faible, car il suffit qu'une des deux déclenche pour que la sécurité soit activée.

- 2oo2 : Cette structure permet quant à elle d'éviter un arrêt intempestif du procédé, car il est nécessaire que deux capteurs sur les deux fournissent une valeur d'alarme pour que le processus se déclenche. La disponibilité est ainsi grandement améliorée, mais la sécurité l'est moins. En effet si un des deux capteurs est défaillant et qu'il ne réagit plus à aucune élévation de température par exemple, alors la fonction de sécurité ne peut plus être assurée.

- 2oo3 : Cette architecture peut être une solution au problème de sécurité de l'architecture 2oo2, car une défaillance dangereuse peut avoir lieu, mais c'est un compromis, car la disponibilité est diminuée par la présence d'un nouveau capteur.

Une fois l'architecture connue pour la partie actionneur et capteur, il va falloir calculer la probabilité moyenne de sollicitation de la SIF. Pour ce faire, la probabilité de défaillance de chaque partie va être calculée et ensuite sommée (méthode LEGO) pour connaitre la probabilité moyenne à la sollicitation de la SIF.

Des formules sont présentes dans la norme IEC 61508-6 qui tient compte des deux taux de défaillance dangereuse (détectée ou non), du type d'architecture K00N, la période de test (TI) et d'autres paramètres. Ces formules ne sont pas à titre obligatoire, elles ne reposent pas sur des démonstrations ce qui peut remettre en cause leur existence. La formule la plus simple, pour l'architecture 1001 est reprise :

$$PFD_{avg} = \lambda_{DU} * \left(\frac{TI}{2} + MTTR\right) + \lambda_{DD} * MTTR$$

Où :
- λ_{DU} est le taux de défaillance dangereuse non détectée exprimé en année^{-1} ;
- λ_{DD} le taux de défaillance dangereuse détectée exprimé en année^{-1} ;
- TI le temps entre les inspections exprimé en année ;
- MTTR le temps moyen de réparation exprimé en année.

Dans les formules pour les architectures plus complexes, il est également possible de rencontrer un terme de défaillance commune qui tient compte de l'aspect d'indépendance qui n'est pas respecté à 100% pour toutes les parties de la SIF.

9. Calcul du niveau de SIL installé

Après avoir identifié des scénarios dans l'HAZOP et calculé le facteur de réduction à fournir pour obtenir un risque jugé acceptable, il fallait déterminer le facteur de réduction du risque présent dans un scénario et le comparer à celui requis.

Avec les probabilités de défaillances moyennes à la sollicitation des différentes barrières mises en évidence dans le scénario HAZOP qu'elles soient connues ou calculées pour chaque barrière, il faut maintenant calculer un niveau de SIL installé pour chacune. Il est donc possible de relier par la définition du niveau de SIL chaque barrière qui possède une probabilité de défaillance à un niveau de SIL installé car l'inverse de la probabilité de défaillance fournit un facteur de réduction du risque qui permet de diminuer significativement le risque initial.

Tableau 3 : Relation entre les niveaux de SIL et le facteur de réduction du risque

SIL	PFD Probabilité de défaillance moyenne à la sollicitation	RRF Facteur de réduction de risque
1	10^{-1} à 10^{-2}	10 à 100
2	10^{-2} à 10^{-3}	100 à 1000
3	10^{-3} à 10^{-4}	1000 à 10 000
4	10^{-4} à 10^{-5}	10 000 à 100 000

Ainsi chaque barrière fournit un niveau de SIL installé. Il suffit de sommer tous les niveaux de SIL installés pour les barrières présentes dans le scénario HAZOP et d'obtenir un niveau de SIL installé global.

Plusieurs cas se présentent alors :

- Le niveau de SIL installé pour le scénario étudié est supérieur au niveau de SIL requis, alors aucune mesure supplémentaire n'est nécessaire ;

- Le niveau de SIL installé est égal au niveau de SIL requis, alors il faut fournir une mesure supplémentaire de réduction du risque. Dans le cas où la solution n'est pas possible économiquement parlant (après démonstration), le cas devient acceptable et rentre donc dans la zone ALARP ;
- Le niveau de SIL installé est inférieur au niveau de SIL requis, il faut absolument fournir d'autres mesures pour réduire considérablement le risque pour se trouver dans un des deux cas ci-dessus.

10.Résultats pouvant être obtenus

Afin de comprendre au mieux la méthode et de rendre cet article plus pédagogique, voici un exemple du déroulement de la méthode HAZOP/SIL. Dans cet exemple lié au monde des nitrates, une cuve de mélange permet de préparer une bouillie qui sera pulvérisée par la suite pour produire un engrais solide. Pour ce faire, les matières premières sont ajoutées en continu dans une cuve de mélange, la bouillie est en continu soutirée par une pompe. Pour éviter que la bouillie ne fige, il est nécessaire de chauffer en continu la solution avec une vapeur de 11 bars.
La régulation ici va être détaillée bien qu'elle ne va pas être reprise dans la première partie de l'analyse de risque. Il existe dans ce cas quatre capteurs de température qui vont permettre à la fois de fournir des alarmes en cas de température haute ou basse et de réguler la température. La cuve possède quatre autres capteurs permettant de provoquer un noyage de la cuve de mélange.
Afin de s'assurer de ne pas avoir de déviation sur la vapeur, une vanne de sectionnement sera également présente dans l'avenir afin de couper l'arrivée vapeur par une température haute en entrée vapeur et sur la cuve de mélange.

Il est possible d'étudier un grand nombre de déviations dans ce cas. Des *no flow* en entrée de cuve peuvent engendrer une diminution de niveau menant inexorablement à la non alimentation de la pompe qui va ainsi baigner dans son jus et s'échauffer. *L'échauffement d'une pompe à nitrate peut mener à une décomposition et donc à une explosion.* Dans le cas des *more flow,* il va être possible de faire déborder le tank et ainsi d'occasionner des brulures à des opérateurs à proximité car la solution peut se rapprocher de 150°C. Le cas étudié ici va être un *high temperature* sur la vapeur ; en effet il est possible que la vapeur subisse une mauvaise désurchauffe et soit plus chaude que prévue. Dans ce cas, la vapeur peut arriver à une température supérieure à 180°C et donc potentiellement chauffer la solution à une température de décomposition.

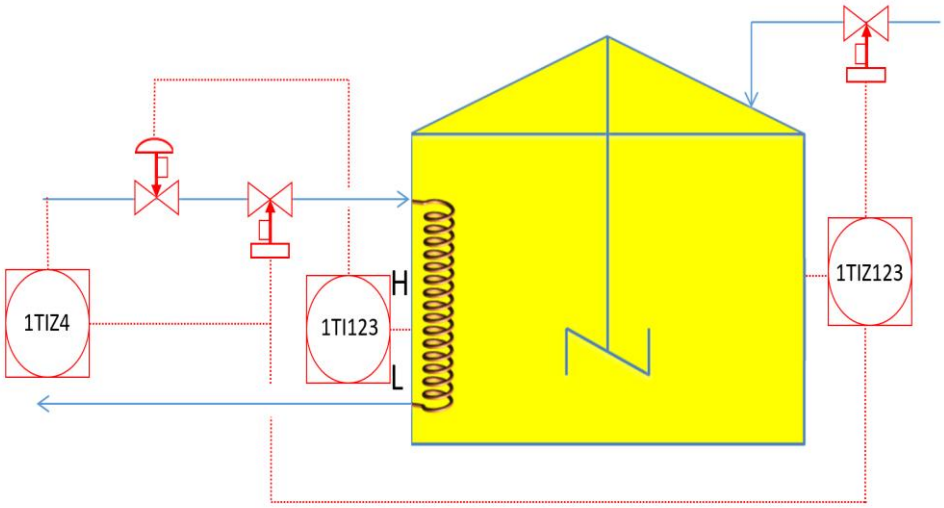


Figure 7 : Cuve de mélange pour la réalisation d'engrais solide

En suivant la logique de l'article, il faut couper la méthode en trois parties.

La première est la **création d'un scénario** par la réalisation de l'HAZOP qui étudie dans ce cas la déviation *high temperature*. La cause est un problème de désurchauffe qui aura comme conséquence une augmentation de la température de la solution menant à une réaction de décomposition et ensuite à une explosion de la cuve.

Ensuite arrive la seconde partie qui va être la **quantification du risque** par la fréquence et la gravité du scénario pour obtenir un niveau de SIL requis, autrement dit un facteur de réduction du risque à obtenir pour avoir un risque jugé acceptable. Dans l'HAZOP, la cause est ici un problème de désurchauffe qui se déroule en amont de cette unité. La désurchauffe est une régulation de température, la température est contrôlée par l'ajout d'eau déminéralisée. La cause est une défaillance sur la régulation de cette arrivée d'eau en considérant que la vapeur n'est plus refroidie à cause de la vanne automatique ou par un problème de capteur. La fréquence communément admise est une fréquence de classe D, entre une fois tous les 10 ans et une fois tous les 100 ans pour les problèmes de régulation.
La gravité majorante va être ici l'impact sur l'homme car une explosion ou une rupture de cette cuve peut causer la mort de plusieurs personnes, la gravité est donc catastrophique. Afin d'affiner l'analyse de risque, il existe parfois des paramètres supplémentaires qui tiennent compte de la fréquence des personnes dans la zone d'impact ou encore de conditions nécessaires en plus de la déviation pour obtenir le scénario complet. Dans ce cas-ci, la faible fréquentation à proximité de la cuve de mélange a été retenue afin **d'abaisser le risque d'un facteur**. En combinant la fréquence avec la gravité obtenue dans la matrice de risque présentée auparavant, un

niveau de SIL requis de 3 est obtenu, ce qui signifie qu'il faut fournir un facteur de réduction du risque d'au moins 1000 pour obtenir un risque acceptable.

Pour terminer, il faut **quantifier la réduction du risque présent dans le procédé**. Il faut regarder maintenant le scénario avec les barrières présentes car en théorie, même si une défaillance sur la désurchauffe est observée, la régulation de température va fonctionner et va permettre d'éviter le problème. Il est possible donc de considérer la régulation de température vers la cuve de mélange, il n'est par contre pas possible de considérer les alarmes car, comme expliqué précédemment, le système logique reste identique. Il est néanmoins possible de considérer un système de noyage en cas de température haute et une vanne de sectionnement sur SMS présente après la régulation qui permet de couper la vapeur en cas de température haute. Afin de s'assurer de l'individualité des barrières, ce sont bien des capteurs de température différents qui sont utilisés pour couper l'arrivée vapeur et noyer la cuve.

Le niveau de SIL installé est de 3,54 pour un SIL requis de 3. La sécurité présente actuellement est donc suffisante. Si ce n'était pas le cas, il faudrait prendre une action pour augmenter la sécurité ou dans le cas où le niveau de SIL installé est équivalent à celui requis prouver que la sécurité n'est pas économiquement envisageable.

11. Conclusion

Les résultats obtenus permettent tout d'abord de fournir une grande quantité de scénarios. Avec les HAZOP, il est possible de réaliser une liste des barrières qui vont être vérifiées par la suite car toutes les barrières de l'HAZOP, comme indiqué précédemment, doivent être vérifiées et contrôlées. Il faut absolument le faire afin d'abaisser la probabilité moyenne de défaillance à la sollicitation à son niveau le plus bas. L'analyse de risque peut également permettre de fournir un fichier qui sans doute après traitement peut estimer l'impact de bypass de sécurité parfois nécessaire dans une usine. Ainsi, il sera possible d'observer l'impact que possède un bypass dans un scénario spécifique et donc d'éviter de supprimer momentanément toutes les barrières d'un scénario.

La méthode HAZOP/SIL possède tout de même un gros désavantage. En effet, la préparation de tous les documents ainsi que la mise à jour des P&ID requièrent un temps considérable. De plus, chaque ligne doit normalement être réalisée durant les réunions avec les avis et les idées de chacun. Il est tout de même possible de gagner un temps non négligeable en préparant à l'avance les réunions HAZOP. C'est ce qui a été réalisé durant l'étude sur l'unité de granulation. La préparation de l'étude résidait dans la compréhension du procédé et de ses paramètres de fonctionnement, de la nature des flux, de la quantité, du design des équipements et surtout dans l'imagination préalable des scénarios de l'HAZOP avec quantification du risque et

identification des barrières LOPA et leurs valeurs de seuil. Il est primordial d'attirer l'attention sur la nécessité de relire chaque ligne de l'HAZOP durant les réunions avec toute l'équipe pluridisciplinaire pour comprendre les scénarios, ajouter, modifier voire supprimer des lignes. Le but est de gagner un temps considérable pour les personnes présentes tout en augmenter la qualité de l'HAZOP. La personne préparant l'étude HAZOP se renseigne sur un nombre important de renseignements qui ne devront plus être vérifiés par après. Il a ainsi été possible de réaliser une analyse de risque sur une unité industrielle complète, grande de 8 nœuds durant un turn around. L'étude a nécessité 11 réunions de 4 heures chacune et 295 scénarios ont été étudiés. La mise à disposition d'un Process Safety Engineer a été nécessaire dans le cadre de la préparation et de la gestion de cette étude.

Bibliographie

[1] CAGNITA Stefania, 2014, *Compréhension des mécanismes d'incompatibilité chimique du nitrate d'ammonium par modélisation moléculaire*, Thèse de doctorat , Chimie physique et chimie analytique, université Pierre et Marie Curie
[2] ARNAUDIES Jean-Marie, 2006, *La catastrophe de Toulouse*, Natures Sciences Sociétés, Vol. 13, pp 421-425
[3] ANDRÉ Laurent, *Sécurité des procédés chimiques : connaissances de base et méthodes d'analyse de risque*, 2e éd, Paris, TEC & DOC, 2003, pp610
[4] BRUSSET Isabelle et al., 2002, *Le nitrate d'ammonium : Description, production, utilisation et précautions d'usage* [Travail scolaire en école d'ingénieur], pp 72.
[5] *Etude détaillée du scénario 10 : Unité de production d'engrais à base de nitrate d'ammonium* [document interne], 2017, pp 1564
[6] GARET Christelle, 2009, *Outils d'inspection : Nitrate d'ammonium* [outil du service d'inspection Seveso], pp84
[7] *Manuel opératoire : granulation* [document interne], pp 31
[8] LAJIMI Chokri, *Diagramme de Farmer* [en ligne], consulté le 31/12/2018 https://www.researchgate.net/figure/Diagramme-de-Farmer_fig3_323127112
[9] *Erlend andreas gjaere, 2017, Human errors in cyber security – A swiss cheese of failures* [en ligne], consulté le 25/10/2018 https://securityandpeople.com/2017/07/human-errors-in-cyber-security-a-swiss-cheese-of-failures/

[10] MORTUREUX Y. (2016). Fondamentaux de l'analyse de risque, regard fiabiliste sur la sécurité industrielle. Numéro 2016-02 de la Collection Les Regards sur la sécurité industrielle, Fondation pour une culture de sécurité industrielle, Toulouse, France.

[11] *Danger et risque* [en ligne], consulté le 26/12/2018 https://www.cchst.ca/oshanswers/hsprograms/hazard_risk.html

[12] IDDIR Olivier, 2009, *Principes d'évaluation de la probabilité de défaillance des Mesures de Maîtrise des Risques (MMR)*, Techniques de l'ingénieur, SE4057 Vol. 1, pp 18

[13] CCPS, *guidelines for Hazard Evaluation Procedures*, 3ième edition, New York, Wiley interscience, 2008, pp461

[14] ROYER Michel, 2009, *HAZOP : une méthode d'analyse des risques-Présentation et contexte*, Techniques de l'ingénieur, SE4030, Vol. 1, pp 10

[15] CRAWLEY Frank et TYULER Brian, *HAZOP : Guide to best practice guidelines to best practice for the process and chemical industries*, 3ième édition, Amsterdam, Elsevier, 2015, pp150

[16] *Outils en management QHSE* [en ligne], consulté le 25 octobre 2018 https://www.previnfo.net/sections.php?op=listarticles&secid=7

[17] LEQUIME Bruno, *L'analyse de risque des ESP dans les études d'ingénierie d'unités industrielles « Pétrole et gaz »* [formation], 2008, pp22

[18] Profluid, *Le SIL Safety Integrity Level* : Niveau d'intégrité de sécurité [brochure] , 2011, pp 36

[19] IDDIR Olivier, *Probabilité de défaillance à la sollicitation d'une fonction instrumentée de sécurité*, Techniques de l'ingénieur, SE4058, Vol.2, 2015, pp24

[20] IDDIR Olivier, *Méthode LOPA : principe et exemple d'application*, Techniques de l'ingénieur, SE4075, Vol.1, 2012, pp 29

[21] KAREN A et al., 2009, *LOPA Misapplied : Common Errors can lead to incorret conclusions*, Wiley Interscience, pp 8

[22] LAMY Pascal, *Probabilité de défaillance dangereuse d'un système : explication et exemple de calcu*l [note scientifique et technique], 2002, pp 50

[23] *Principes opératoire : granulation* [document interne], 1995, pp 128

[24] *Rapport Seveso de Yara Tertre : partie analytique* [document interne], 2017, pp 1564

[25] KERSTEN R.J.A et BOERS M.N, 2003, *Safety aspects of ammonium nitrate solutions at high temperatures*, pp 49