LES CAHIERS DE LA SÉCURITÉ INDUSTRIELLE

2009-09

L'ANALYSE DE RISQUE

FRÉQUENCE DES ÉVÉNEMENTS INITIATEURS D'ACCIDENT

Groupe d'échange "FRÉQUENCE DES ÉVÉNEMENTS"

ICSI
INSTITUT POUR UNE CULTURE DE SÉCURITÉ INDUSTRIELLE

L'*Institut pour une Culture de Sécurité Industrielle* (ICSI) est une association de loi 1901 dont la vocation est de faire progresser la culture de sécurité en France. Il est né en 2003 de l'initiative de huit partenaires fondateurs (Airbus, Arcelor, CNRS, Communauté d'agglomération du Grand Toulouse, EDF, Institut National Polytechnique de Toulouse, Région Midi-Pyrénées et Total) qui ont été rapidement rejoints par d'autres industriels de branches diverses, des Instituts spécialisés, des Écoles et Universités, des acteurs de la société civile (associations de Maires, organisations syndicales, organisations non gouvernementales). C'est donc l'**ensemble des parties prenantes** de la sécurité industrielle que l'ICSI fédère, ce qui en fait son originalité.

Cet Institut poursuit trois objectifs principaux :

- rechercher, pour une meilleure compréhension mutuelle et en vue de l'élaboration d'un compromis durable entre les entreprises à risques et la société civile, les conditions et la pratique d'un débat ouvert prenant en compte les différentes dimensions du risque ;
- contribuer à l'amélioration de la sécurité dans les entreprises industrielles de toute taille, de tous secteurs d'activité, par la prise en compte du risque industriel sous tous ses aspects ;
- favoriser l'acculturation de l'ensemble des acteurs de la société aux problèmes des risques et de la sécurité.

Éditeur : **Institut pour une Culture de Sécurité Industrielle**
Association de loi 1901

http://www.icsi-eu.org/

6 allée Émile Monso - BP 34038
31029 Toulouse Cedex 4
France

Téléphone : +33 (0) 534 323 200
Fax : +33 (0) 534 323 201
Courriel : contact@icsi-eu.org

Synopsis

Title Initiating event frequency and availability of safety barriers

Keywords industrial safety, reliability and availability databases, operational experience feedback

Author ICSI's *Initiating event frequency* working group

Publication date July 2006 (first publication)
August 2009 (this version)

Safety cases for industrial plants are often based on a semi-probabilistic risk assessment method, such as LOPA (Layer Of Protection Analysis). These methods require the ability to estimate in quantitative terms both the frequency of initiating events (such as leaks or pump failures) and the availability of safety barriers (preventive barriers such as pressure relief valves as well as protective barriers such as blastproof control rooms). This failure and availability data is also used for preventive maintenance.

This data concerns rare events, and observations on a single industrial facility are generally insufficient to provide adequate estimations. Therefore, operators collect information on equipment failures and barrier dependability at an industry-wide level, over a large population of installed equipment. However, failure rates are known to depend on numerous factors, such as the quality of the installed equipment (dependent on a plant's purchasing policy), the inspection and maintenance activities, and the age of equipment.

The present document is the result of an ICSI working group on initiating event frequencies and barrier availability in the petrochemical, chemical and non-nuclear energy sectors. Participants from a number of industrial firms operating in Europe exchanged information on the quantitative frequency ranges used in their firm for different types of events, on appropriate data sources and on factors used to select a low or high value within the suggested frequency range. The frequencies and probabilities given in this document are averages over these industries, that working group participants consider to be reasonable generic values.

This document will be useful for people wishing to carry out a risk assessment of an industrial facility or wishing to conduct a critical review of an existing risk assessement. When using values from this document, it is important to take into account the specific characteristics of the plant being studied, including specific technological characteristics and organizational issues.

Table des matières

Introduction

Ce document est issu des travaux du groupe d'échange « Fréquence des événements initiateurs d'accidents et disponibilité des barrières de protection et de prévention » animé par *l'Institut pour une Culture de Sécurité Industrielle*. Il constitue un résumé des éléments quantitatifs discutés au sein du groupe.

Contexte

> *La sécurité est souvent une notion utilisée de façon subjective et, pour la traduire en termes opératoires d'aide à la décision, il s'avère indispensable de développer des approches quantitatives.* [Villemeur 1997]

Les méthodes d'évaluation des risques de type LOPA[1] sont une réponse à cette exigence.

L'évaluation du risque passe par l'évaluation de la fréquence de l'aléa qui, elle, repose sur des données de fréquence des défaillances initiales et de disponibilité des barrières. La validité et la précision de ces données est donc de première importance dans la démarche d'évaluation du risque.

La fréquence d'occurrence des défaillances et la disponibilité des barrières peuvent paraître des données objectives, car on a à disposition des bases de données conséquentes qui appartiennent soit à des entreprises qui pratiquent le retour d'expérience depuis suffisamment longtemps, soit au domaine public. Or on observe des écarts de plusieurs ordres de grandeurs, même au sein d'une même entreprise. Il est important de prendre en compte les hypothèses que sous-tendent la majorité des chiffres utilisés dans ces analyses de risques. La probabilité d'occurrence des événements initiateurs, comme la disponibilité des barrières, peut être largement influencée par des facteurs tels que la fréquence des contrôles et l'efficacité de l'entretien préventif. Ces chiffres s'appuient donc fortement sur l'efficacité du système de management de la sécurité et sur le niveau d'intégration des progrès technologiques dans les standards de conception.

Par ailleurs, la méthode de travail – et en particulier le mode de construction des scénarios – peut influencer le type d'événement initiateur. Par exemple, pour un événement de type « fuite », certaines entreprises considèrent plusieurs catégories de fuite : petite, moyenne et grande ; d'autres feront une distinction entre des petits piquages et des piquages ordinaires ; d'autres utilisent une seule catégorie de piquage. Enfin, dans certains secteurs on estime des fréquences par « unité standard », alors que d'autres industriels calculent des fréquences d'occurrence en fonction du nombre de mètres de tuyaux.

En outre, il est important de noter que lorsque l'on met en place une évaluation (semi) probabiliste des risques on a, en fait, deux objectifs :

1. hiérarchiser les risques pour prioriser les actions ;
2. faciliter le processus d'acceptabilité du risque en en donnant une évaluation aussi objective que possible.

[1] LOPA : *Layer of Protection Analysis*, une méthode d'analyse de risque semi-quantitative.

Les analyses de risques des installations industrielles sont davantage utilisées pour établir une **hiérarchisation des niveaux de risque** afin de prioriser les actions, que pour définir une acceptabilité du risque au sens « politique » du terme. La raison en est assez simple : « Alors que le niveau de fiabilité à atteindre [au niveau de la production] peut être défini par une optimisation technico-économique, l'acceptabilité du risque doit tenir compte de facteurs moraux et psychologiques »[2] que l'on cherche à évacuer lorsque l'on conduit une évaluation technique du risque.

Dans le cadre d'une hiérarchisation des risques, ce qui compte ce sont les **valeurs relatives**, plutôt que le niveau de risque absolu qui est estimé. L'on recherche dans les bases de données des **plages de valeur** plutôt que des valeurs absolues. On procède au « calage » de l'échelle en retenant, pour les équipements les plus significatifs, des valeurs clés qui rendent cohérentes l'échelle de gravité, l'échelle des fréquences et les limites d'acceptabilité retenues.

Par conséquent, une méthode d'évaluation du risque, les modes d'évaluation des fréquences (probabilité), les échelles de gravité et le niveau de risque acceptable forment un tout qui est indissociable de la **culture de sécurité de l'entreprise**.

Lorsque l'on cherche à faire plus que la hiérarchisation des risques et que l'on souhaite une évaluation précise de la fréquence, on doit d'une part avoir recours à des méthodes d'analyse aussi fines que possibles (comme les arbres de défaillances) et d'autre part s'appuyer sur un processus de retour d'expérience interne à l'entreprise qui soit bien établi.

L'expérience de l'expert conduisant l'analyse de risques joue donc un rôle primordial dans le choix éclairé des données d'entrée.

Objectifs

Ce document est une synthèse des discussions ayant eu lieu dans le cadre des réunions du groupe d'échange *Fréquence des événements initiateurs d'accident et disponibilité des barrières de prévention et de protection* de l'ICSI. Les groupes industriels ayant participé au groupe d'échange proviennent de secteurs d'activité assez différents, et emploient des méthodes d'analyse de risque qui ne sont pas identiques. Ainsi, les discussions n'ont pas porté sur les méthodes d'évaluation elles-mêmes, mais plutôt sur les valeurs de base qui servent d'entrée à ces analyses de risques.

*Les valeurs données dans ce document sont des **valeurs moyennes**, reconnues par les personnes ayant participé à la rédaction comme étant **vraisemblables**.*

Le document s'adresse à toute personne ayant à conduire ou à évaluer une analyse de risque d'une installation industrielle, en fournissant des repères dans le choix ou l'appréciation de la pertinence des éléments quantitatifs employés. Il fournit des **plages de valeur** pour différents types d'événements initiateurs d'accident et pour la disponibilité des barrières. Les valeurs données dans ce document sont donc des **valeurs moyennes**, reconnues par les participants comme **vraisemblables**. La valeur retenue par l'utilisateur sera fonction des choix technologiques et des organisations en place. Il est également important de retenir de ces données les valeurs minimum au dessous desquelles il n'est pas raisonnable de descendre.

[2] ibid

Structure du document

Le document résume en particulier :

- les éléments quantitatifs des discussions (plages de valeurs pour la probabilité d'occurrence des événements initiateurs, valeurs pour la disponibilité de différents types de barrières) ;
- une liste des facteurs (telles que les caractéristiques du procédé ou du milieu) qu'il convient de prendre en compte pour guider le choix d'une valeur élevée ou basse dans ces plages ;
- des indications sur les sources de données pertinentes.

Les secteurs industriels concernés sont principalement la chimie, la pétrochimie et le raffinage. Il est important de noter que ce document est une synthèse des réflexions menées au cours des réunions du groupe d'échange de l'ICSI. Cette synthèse a été réalisée par l'ICSI.

Remerciements

L'ICSI tient à remercier les personnes suivantes, qui par leur participation aux débats au sein du groupe d'échange, ont contribué à la réalisation de ce document.

Nom	Prénom	Organisme
BAYLE	Jean-Louis	Total Petrochemicals
BOGLIETTI	Bernard	EDF
CAUCHOIS	Didier	Sanofi-Aventis
CHARPENTIER	Dominique	INERIS
CHETRIT	Alain	Total
CHEVALLIER	Jean-Pierre	Shell
CONDEMINE	Stéphane	Total
DAUX	Christophe	Total Petrochemicals
DEHONDT	Armand	Rhodia
DELEUZE	Gilles	EDF R&D
DEROO	Jean-Marc	GESIP
DURCKEL	Bernard	Shell
DUVAL	Denis	Total
GABAS	Nadine	ENSIACET
GUERIN	Christophe	Air Liquide
GUERRILLOT	Luc	Sanofi-Aventis
MARCHAND	Vincent	Arkema
MARSDEN	Éric	ICSI
MILARDO	Charles	Shell
MIQUEL	Pierre	UIC Rhône-Alpes
PALLIN	Jean-François	EDF
PASQUINI	Zeno	Rhodia
PIERRAT	Alain	UIC
PRIMARD	David	Areva
PSENICA	Claude	UFIP
PY	Jean-Louis	Arkema
RENARD	Marc	Solvay
SEBBANE	Philippe	Total
TRIOLLIER	Michel	Rhodia
VACHER	Gilles	ICSI

1

Fréquences des événements initiateurs

Lorsqu'on base ses calculs sur la probabilité de l'événement redouté central (ERC), on perd de l'information sur les éléments conduisant à l'ERC, sur l'effet de l'ensemble des barrières de prévention. On ne sait pas quelles barrières ont été prises en compte implicitement dans le chiffre fourni ; on ne sait pas si les effets dominos sont intégrés ou non.

Pour cette raison, nous avons cherché dans ce chapitre à quantifier la probabilité d'occurrence des événements initiateurs, plutôt que celle des événements redoutés centraux.

1.1 Fuite et rupture d'éléments de tuyauterie

Événement	Ouverture inopinée d'une soupape (par exemple suite à la rupture du ressort)
Valeurs	Entre 10^{-1} et 10^{-3} par an et par soupape. Une entreprise utilise une valeur de 10^{-4}/an, chiffre tiré du retour d'expérience local, mais portant uniquement sur les événements qui auraient des conséquences dangereuses (ouverture franche de soupape plutôt que battement).
Observations	La surveillance du fonctionnement de la soupape, au delà des exigences réglementaires, sera adaptée dans le cadre du SMS selon les conséquences d'un dysfonctionnement. Une soupape est soumise à différents types de défaillance ; une défaillance partielle où la soupape « bat » est relativement fréquente, mais conduit à des conséquences généralement peu graves, donc est peu prise en compte dans les études de dangers. La défaillance par ouverture totale est bien plus rare. Ces chiffres ne concernent pas la probabilité de sollicitation d'urgence de la soupape.

Événement	Ouverture intempestive d'un disque de rupture (événement qui pourrait être classifié avec l'ouverture intempestive de soupape, mais qui est considéré comme étant plus fréquent par certains industriels.)
Valeurs	Fourchette de 10^{-1} à 10^{-2}/an.
Observations	Origines de l'événement : erreur de montage, erreur de valeur et disques qui fatiguent. Le taux de défaillance est fonction du dimensionnement ainsi que des conditions du procédé. Les disques de rupture sont souvent utilisés pour protéger des soupapes de l'encrassement ; dans ce contexte ils ne seront pas impliqués dans événement initiateur.

Événement	Rupture de joint statique
Valeurs	Entre 10^{-5} et 10^{-7} par an pour un seul joint.
Observations	La fréquence type de cet événement peut globalement être prise à 10^{-2} par an et pour une installation chimique « classique ». Les fréquences varient considérablement en fonction du type de bride (à face plate, à simple ou double emboîtement) et de joint (en téflon, spiralé avec jointure métallique, ...). Certains groupes utilisent des joints spiralés de façon systématique, alors que d'autres ont des standards sur le choix des tuyauteries et des techniques de jointure, en fonction de facteurs comme la toxicité des produits, la pression et la température. Différents scénarios sont pris en compte, en fonction de la section ouverte ou du nombre de boulons qui ont lâchés. Des critères comme l'angle de fuite pourront influencer l'évaluation globale du scénario : si la portée d'un dard (feu de chalumeau) dans un angle donné n'atteint aucun équipement, la probabilité du scénario sera réévaluée à la baisse en fonction de cet angle. Pour une entreprise, il existe plusieurs scénarios de fuite/rupture en fonction du débit libéré (3%, 50% et 100%, le modèle dit « FRED » du HSE/HSL). Pour certains types d'installations, l'impact de cette catégorie d'événement initiateur est souvent faible, puisque le scénario n'est pas majorant.

Événement	Rupture de petit piquage (jusqu'à 2")
Valeurs	Pour la majorité des entreprises : valeur de base de 10^{-4}/an par piquage, pouvant varier de 10^{-3} à 10^{-6}/an en fonction de facteurs énumérés ci-dessous.
Observations	Il s'agit de ruptures entraînées par des chocs, des vibrations (par exemple dues à une personne qui marche sur le piquage). Ces chiffres ne prennent pas en compte les questions de corrosion, le degré de renforcement du piquage. Facteurs de réduction de la fréquence d'occurrence : ◇ Dispositifs de renforcement du piquage (facteur 10) ◇ Balisage et politique de circulation sur site interdisant le passage dans des zones sensibles (protection anti-choc) ◇ Politique d'inspection/maintenance spécifique, par exemple avec radiographie Facteurs d'augmentation de la fréquence d'occurrence : ◇ Vibration excessive ◇ Corrosion sous calorifuge ◇ Longueur du piquage et de la masse vibrante ◇ Zone/exposition favorisant les chocs Certaines entreprises ont des campagnes de maintenance spécifiques sur les piquages, avec radiographie. Certaines entreprises estiment que la fréquence diminue lorsque la taille augmente et qu'au dessus de 80 mm la rupture est non réaliste (s'agissant de produits dangereux, des précautions particulières sont prises).

Événement	Rupture d'un flexible de chargement
Valeurs	Entre 10^{-1}/an (pour des tuyaux non inspectés) et 5×10^{-3} pour des tuyaux avec inspection et SMS.
Observations	Il existe différentes catégories de tuyaux flexibles, qui peuvent être armés d'inox ou non ; les taux de défaillance sont plus bas pour les équipements armés. Le degré de tension du flexible peut être pris en compte. Le SMS peut prévoir plusieurs types d'action qui serviront de barrière : inspection visuelle du flexible avant utilisation, rangement spécifique du flexible, ouverture progressive, changement systématique après une certaine durée.

Événement	Rupture d'un élément fragile (niveau à glace, équipements en verre, soufflet – éléments dont la fragilité augmente avec le temps)
Valeurs	Traitement au cas par cas.
Observations	La pratique industrielle tend à limiter l'utilisation d'équipements en verre, lorsque d'autres types d'appareillage peuvent remplir les mêmes fonctions.

1.2 Défaillances d'organes de contrôle

Événement	Fonctionnement accidentel (ouverture ou fermeture inopinée) d'une vanne « tout ou rien »
Valeurs	Valeur type entre 10^{-2} et 10^{-3}/an par vanne.
Observations	Ces chiffres s'entendent naturellement avec entretien complet planifié (exigence de maintenance cohérent avec le niveau du SIL requis). Remarque : très dépendant de la fonction de la vanne dans le contrôle du procédé.

Événement	Défaillance d'une vanne de régulation
Valeurs	Valeur type : 10^{-1}/an
Observations	

Événement	Défaillance d'un système de régulation
Valeurs	Valeur typique : 10^{-1}/an
Observations	On considère généralement que les défaillances de systèmes de régulation sont provoquées dans 15% des cas par la logique, pour 50% par les actionneurs et pour 35% par les capteurs.

1.3 Défaillances d'équipements mécaniques

Événement	Défaillance d'une pompe
Valeurs	Entre 1/an, toutes causes confondues (perte de la fonction de pompage, sans secours), et 10^{-1}/an.
Observations	Inclut la rupture des joints dynamiques.

Événement	Perte d'alimentation électrique (indisponibilité d'un générateur de secours)
Valeurs	Fourchette de 10^{-1}/an pour une alimentation non importante pour la sécurité, à 10^{-2}/an pour une fonction importante pour la sécurité.
Observations	Sur certains sites des turboalternateurs tournent en permanence pour assurer une alimentation partielle même en cas d'indisponibilité de l'alimentation électrique. Cette fréquence suppose que les générateurs de secours soient testés en charge de manière régulière (typiquement une fois par semaine).

Événement	Défaillance d'un système d'utilité (de type refroidissement par eau, alimentation en azote)
Valeurs	Fourchette de 1 à 10^{-1}/an par utilité.
Observations	Cet événement pourra également apparaître en tant que PFD d'une barrière de protection (au sens de la probabilité de la perte de la fonction de refroidissement de sécurité) ; la PFD sera alors de 10^{-1} ou 10^{-2}.

Événement	Perte de la fonction agitation
Valeurs	De l'ordre de 1 à 10^{-1}/an.
Observations	Cette fréquence d'occurrence intègre toutes les causes de défaillance. Afin de mieux évaluer l'impact de ce type d'événement, il est possible de décomposer le scénario en prenant comme événements initiateurs la défaillance des différents composants du dispositif (moteurs, courroie, arrêt électrique, corrosion de l'arbre, pales corrodées, rupture de l'entraînement).

1.4 Autres types d'événement

Événement	Mise sous contrainte d'un équipement due au froid, entraînant la rupture fragile (ainsi que ruptures entraînées par la dilatation thermique où par des efforts mécaniques).
Valeurs	Traitement au cas par cas ; difficile de fournir une fréquence d'occurrence.
Observations	Problème : n'entraîne pas une défaillance immédiate (fragilisation dans le temps). Dans certains cas pourra être pris en compte en tant que facteur aggravant un scénario, plutôt que comme événement initiateur.

Événement	Corrosion d'un équipement, entraînant une perte de confinement
Valeurs	Traitement au cas par cas ; difficile de fournir une fréquence d'occurrence
Observations	Dans certaines branches d'activité, ce type d'événement ne peut pas être associé à une fréquence d'occurrence. En effet, on supposera que le matériau est adapté au produit transporté ; il n'est pas pertinent de faire des études de sécurité sur une utilisation inappropriée d'un équipement. Dans d'autres branches d'activité, l'impact de la corrosion peut être pris en compte par « dire d'expert » ou par retour d'expérience (notamment sur des installations existantes). Facteurs d'augmentation de la fréquence : • proximité de la mer entraînant une corrosion par l'extérieur Facteurs de réduction de la fréquence : • politique d'inspection/maintenance spécifique, dans le cadre du SMS

Événement	Impact de foudre
Valeurs	Traitement au cas par cas ; difficile de fournir une fréquence d'occurrence
Observations	Certains industriels (raffineries) intègrent cet événement autrement que comme événement initiateur, l'hypothèse étant que l'installation est bien conçue (ATEX *etc.*), donc que l'impact de la foudre est nul. Il existe des consignes spécifiques pour que certaines activités soient interdites par temps d'orage. Il est possible de prendre en compte un événement initiateur qui sera impact ou électricité statique qui entraîne une inflammation. Nota : Il existe une directive sur ce sujet (« étude foudre »).

Événement	Ignition (feu ou explosion) d'un rejet à l'atmosphère
Valeurs	À étudier au cas par cas, mais exemple de probabilité générique de 10^{-1}, pouvant varier de 1 à 10^{-2}.
Observations	Dépend de multiples critères : ◇ zone ATEX ou non ; ◇ nature des produits rejetés ; ◇ point chaud à proximité.

2

Disponibilité des barrières

Il est important de bien préciser au niveau du scénario le caractère *préventif* ou *protectif* de la barrière[1].

2.1 Barrières de prévention

La disponibilité d'une chaîne instrumentale de sécurité est indiquée par son SIL (*Safety Integrity Level*), évalué par le concepteur et/ou mesuré par le retour d'expérience (*cf.* les normes IEC 61508 et 61511 [IEC 2004]).

Barrière	Vanne « tout ou rien » (TOR) de sécurité
Valeurs	PFD variant entre 10^{-1} et 5.10^{-3} par vanne.
Observations	Ces chiffres s'entendent naturellement avec entretien complet planifié (exigence de maintenance cohérent avec le niveau du SIL requis).

Barrière	Soupape de prévention ou protection surpression/dépression
Valeurs	PFD de base de 10^{-2}, pouvant varier de 10^{-1} à 10^{-3}. Remarque : il n'est pas raisonnable de considérer une valeur inférieure à 10^{-3}.
Observations	La valeur donnée concerne le fonctionnement en sécurité de la soupape (non ouverture sur sollicitation). Facteurs de réduction de la probabilité de défaillance : ◇ procédures d'observation/inspection ◇ qualité de la procédure de montage[2] ◇ qualité du produit propre ◇ association avec un disque de rupture, et contrôle intermédiaire ◇ ... Facteurs d'augmentation de la probabilité de défaillance : ◇ produit encrassant ou corrosif ◇ température du produit ◇ utilisation sur vapeur

Barrière	Disque de rupture
Valeurs	Valeur typique de PFD : 10^{-3}
Observations	Les disques de rupture sont souvent couplés à une soupape de protection.

[1]Certains experts distinguent une troisième catégorie de barrières de *mitigation*, qui tout en admettant le phénomène dangereux, permettent d'en limiter la portée (cas d'un évent d'explosion par exemple). Le terme *barrière de prévention* est alors limité aux seules barrières qui limitent l'occurrence des initiateurs, et *barrière de protection* est réservé aux les moyens de secours, aux refuges (salles sous pression permettant de respirer une atmosphère saine, *etc.*).

2.2 Barrières de protection

Concernant les barrières de protection, on distingue deux valeurs :

- sa **disponibilité**, au sens du PFD (*Probability of Failure on Demand*, ou probabilité de défaillance à la sollicitation) ;
- son **efficacité**, c'est à dire sa capacité à réduire les effets du phénomène dangereux. Une efficacité de 100% voudrait dire que l'on a entièrement éliminé l'impact du phénomène.

Il peut également être utile, pour certains types de barrière, de prendre en compte le **temps de réponse** de la barrière. En effet, certains types de barrières n'atteignent leur efficacité maximale qu'après un temps de « déploiement ». Considérons par exemple une vanne motorisée asservie à une alarme sur un ensemble de détection de gaz. Cet ensemble a une certain PFD et une efficacité qui est proche de 100% pour juguler une fuite. Toutefois, cette efficacité ne sera observée qu'après détection et action de fermeture, qui peuvent requérir une durée non négligeable. Caractériser explicitement cette durée ou temps de réponse est souvent utile dans les analyses de risque.

Barrière	Action de pompiers ou d'intervenants du site (lutte incendie et secours aux victimes)
Disponibilité	Pas de quantification de la disponibilité pour ce type de barrière.
Efficacité	Ne peut être mesurée que via des exercices réguliers.
Temps de réponse	Dépendant du niveau d'intervention : personnes au poste de travail (valeur typique de 5 minutes pour une première intervention à l'extincteur) ; pompiers sur site ; pompiers extérieurs. Doit être testé régulièrement afin de s'assurer que le temps fixé dans l'étude de dangers est réaliste.
Observations	Mélange de facteur humain et organisationnel et de technique. Ne pas oublier de prendre en compte la disponibilité de l'eau (défaillance de pompes ; moyens de stockage sur site).

Barrière	Dispositifs fixes de lutte contre l'incendie (sprinkler, rideau d'eau, lance monitor, déluge, couronnes, *etc.*)
Disponibilité	Typiquement 10^{-2} si test régulier.
Efficacité	Peut varier de 10% à 100% ; à évaluer au cas par cas. Dépend également du temps de réponse de l'ensemble du dispositif (avec mécanisme de détection).
Temps de mise en œuvre	Devra être testé régulièrement. Dépend du fait que le réseau d'eau est ou non sous pression.
Observations	Différence à analyser entre des dispositifs à déclenchement automatique et ceux à déclenchement manuel. Nécessité d'entretien régulier pour assurer la disponibilité des dispositifs.

Barrière	Détection catalytique de gaz (et de l'alarme associée) : toxicité ou explosivité
Disponibilité	Exemple de 5.10^{-2} avec test (et calibrage) tous les 2 à 3 mois, pour un mécanisme redondant.
Efficacité	Liée à la configuration physique de la zone à couvrir et au placement des capteurs, à l'orientation du vent, à la quantité de gaz diffusé.
Temps de réponse	Typiquement moins de 30 secondes. Pour les systèmes à balayage de type chromatographie, le temps de réponse est bien plus long (plusieurs minutes). Toutefois, ils permettent une détection à des concentrations bien plus faibles. Ces équipements semblent donc bien adaptés pour la détection de micro-fuites de gaz, mais moins adaptés à la détection de fuites plus importantes.
Observations	La valeur donnée concerne la probabilité de non fonctionnement lorsque le nuage passe sur un capteur ; il n'intègre pas la possibilité pour le nuage de passer à côté de tous les capteurs. Les détecteurs de type infrarouge ont une meilleure fiabilité et un temps de réponse plus faible.

Barrière	Déclenchement d'une alarme
Disponibilité	Valeur typique de PFD de 10^{-3} (probabilité de non fonctionnement de la sirène sur sollicitation)
Efficacité	Attention au facteur humain (réflexe pour évacuer de façon disciplinée)
Temps de réponse	
Observations	*cf.* section § 2.3 pour le déclenchement de l'alarme par l'opérateur

Barrière	Confinement contre risque explosion / toxique (bulle, blockhaus)
Disponibilité	PFD proche de 0
Efficacité	Varie en fonction de la qualité de fabrication.
Observations	Vérifier le degré de fuite des portes.

2.3 Facteur humain

L'homme est « facteur faillible de fiabilité » ; il intervient donc à la fois en tant qu'événement initiateur d'accident et élément de rattrapage (ou barrière).

La caractérisation du comportement humain est un domaine complexe, et il est bien entendu réducteur de l'exprimer en tant que composant ayant une fréquence de défaillance ou en tant que barrière avec un taux de disponibilité. Les valeurs et commentaires proposés permettent néanmoins – dans le contexte auquel nous nous intéressons qui est celui des études de dangers d'ICPE, principalement dans les industries du procédé – une prise en compte raisonnable du rôle de l'homme dans la sécurité des installations.

Les chiffres donnés ci-dessous pour la fréquence d'erreurs d'une action humaine, comme pour la disponibilité d'une tâche humaine considérée en tant que barrière, dépendent de multiples facteurs, dont :

- le niveau de formation initiale et de mise en situation de l'opérateur (qu'elle soit externe ou interne) ;
- le niveau d'urgence de la tâche ;
- la nature de l'installation (processus continu ou batch ; processus manuel ou automatisé) ;

- la nature de l'organisation : un pilote de chasse aura vraisemblablement des réactions différentes de celles des membres d'une petite équipe, et encore des membres d'une équipe de taille importante ;
- la complexité de la tâche (routinière ou non ; nombre de tâches concomitantes). Par exemple, certaines entreprises estiment qu'il ne faut pas dépasser 20 alarmes répertoriées comme nécessitant une action opérateur sur un poste de travail, ou 300 boucles de régulation à surveiller ;
- le temps de réponse disponible, s'agissant de situations complexes (certaines entreprises estiment que si le temps de réflexion disponible est inférieur à 30 minutes, il est difficile de prendre en compte l'action de l'opérateur comme constituant une barrière de prévention) ;
- la gravité de l'événement redouté ;
- la réaction individuelle et la perception du danger ;
- les qualités ergonomiques de l'installation, des aspects sociaux (qualité des relations dans le collectif).

Pour atteindre les valeurs les plus basses citées ci-dessous, il est nécessaire de respecter certains grands principes :

- ergonomie adaptée de poste de travail ;
- formation adéquate de l'opérateur à la tâche en question ;
- temps de réponse sur sollicitation adapté à la disponibilité de l'opérateur (valeur typique : au moins 30 minutes).

Événement	Erreur humaine sur une tâche habituelle Exemples : ◇ écart de configuration d'une machine au lancement d'un processus batch ; ◇ erreur lors d'une opération de jointage ; ◇ tâche continue de surveillance du niveau d'un bac.
Valeurs	La méthode classique d'évaluation de la fréquence de ce type de défaillance sur une tâche isolable consiste à partir de la PFD pour une activité humaine (conditionné par divers facteurs évoqués ci-dessus), et multiplier par le nombre d'opération par an pour obtenir une fréquence d'occurrence. Valeurs de PFD de l'ordre de 10^{-3} à 10^{-4} par opération. Autre méthode d'évaluation : s'appuyer sur le principe de « l'unité type », en considérant des fréquences de l'ordre de 1/an pour des travaux routiniers et entre 10^{-1}/an et 10^{-2}/an si mise en œuvre des Bonnes Pratiques de Fabrication.
Sources pertinentes	[Villemeur 1997]
Observations	On pourrait distinguer l'erreur humaine sur sollicitation (par exemple sur alarme) de l'erreur sans sollicitation. Cette distinction revient à la différence entre un processus où le procédé est piloté par machine, et un processus où l'opérateur est maître du processus de fabrication. Pour des évaluations préliminaires des risques, l'erreur humaine sera généralement prise comme ayant une fréquence de 10^{-1}/an dans un premier temps. Cette fréquence dépendra de multiples facteurs, (*cf.* ci-dessous). Remarque : Il n'est pas recommandé de considérer une action humaine comme barrière si une action humaine est à l'origine du scénario, sauf à démontrer l'indépendance de ces deux actions humaines.

Événement	Erreur humaine sur une action de type procédurale (sur action non répétitive)
Valeurs	D'après [Villemeur 1997] : 10^{-2} par opération, à multiplier par le nombre d'opérations par an pour obtenir une fréquence.
Observations	

Événement	Réaction inappropriée face à une situation inhabituelle et non procédurale (action réfléchie)
Valeurs	D'après [Villemeur 1997] : plage entre 1 (en situation d'urgence) et 10^{-1} par opération, à multiplier par le nombre d'opérations par an pour obtenir une fréquence.
Observations	

Barrière	Action d'un opérateur dans une salle de contrôle qui répond à une sollicitation (par exemple à une alarme)
Valeurs	PFD entre 1 (lorsque le temps de réponse disponible est faible) et 10^{-2}.
Sources pertinentes	Table F.3 de l'annexe F « Méthode LOPA » de la norme IEC 61511 [IEC 2004]. Ouvrage de Villemeur [Villemeur 1997]. *Étude de faisabilité d'une méthode d'intégration des facteurs humains dans les activités d'analyse de sécurité et de développement des systèmes de transports terrestres guidés*, [Telle et al. 1997].
Observations	On considère parfois l'action humaine collective (de l'ensemble des personnes présentes dans la salle de commande) plutôt que l'action d'un opérateur individuel. Points qui peuvent améliorer l'efficacité de l'action humaine : • mise en place d'une procédure de double contrôle : deux personnes effectuant un test avec des procédures différentes, et chacun apposant sa signature (notion de défense en profondeur). Toutefois, le degré de réduction de la fréquence venant d'une même famille de mécanismes de protection doit être borné. Par exemple, on ne pourra pas utiliser trois « barrières humaines » supposées indépendantes pour atteindre un facteur de réduction du risque de 10^{-4}. • existence d'une checklist détaillée ; • valorisation des actions de l'opérateur ; les tâches doivent avoir un sens pour l'opérateur.

3

Sources de données

Les chiffres cités dans le présent document sont d'origine diverse. La principale source d'information est l'**accidentologie**, qu'elle soit issue de données internes de groupes industriels, ou la moyenne constatée dans une industrie donnée. Les principaux recueils publics de données issues de l'accidentologie sont les suivants :

- *OREDA* : base de données sur la fiabilité des équipements pour l'exploration et la production pétrolière et gazière, gérée par des compagnies pétrolières [OREDA 2002]. Contient des informations assez détaillées, avec taux de défaillance, temps de réparation, distribution des modes de défaillance. (*cf.* www.oreda.com).
- Document *Failure Rate and Event Data for use within Land Use Planning Risk Assessments*[1] (106 pages) du *Health and Safety Executive* anglais. Ce document comprend des propositions de probabilité de défaillance pour des équipements sous pression, cuves non-pressurisées, cuves refrigérées, soupapes, pompes, tuyauterie, pipelines, équipements électroniques, fret par voie routière ou chemin de fer.
- *NPRDS* (Nuclear Plant Reliability Data System) : base de données sur les taux de défaillance des équipements utilisés dans les centrales nucléaires aux USA.
- Ouvrage *Guidelines for quantitative risk assessment* de la *Publication Series on Dangerous Substances* du VROM, ministère néerlandais chargé de l'environnement (ouvrage généralement connu sous le nom du *Purple Book* du TNO [Committee for the Prevention of Disasters, Netherlands 1999]). Ce document décrit la démarche d'analyse de risques QRA, et fournit des éléments quantitatifs pour certains types d'événement initiateur d'accident.
- Base *Process Equipment Reliability Database* (PERD) du *Center for Chemical Process Safety* (CCPS), AIChE.
- La base de données *FRED* (Failure Rate and Event Database) du HSE (non diffusée).
- La base de données de l'UIC.
- La banque de données *Victor* qui est alimentée et consultable par les membres du GESIP (*cf.* www.basevictor.com). Cette banque de données centralise les informations liées aux accidents, à leurs causes, ainsi que les enseignements retenus, dans un but d'enrichissement mutuel. Elle est surtout alimentée par l'industrie pétrolière, plutôt que par l'industrie chimique.
- La base *Eireda* (European Industry Reliability Data Bank) contient des données sur les défaillances de matériels électriques, mécaniques et électromécaniques, collectés dans des centrales nucléaires de production d'électricité.

[1]Document téléchargeable à l'adresse `http://www.hse.gov.uk/landuseplanning/failure-rates.pdf`.

- Le Guide FIDES *Méthodologie de fiabilité pour les systèmes électroniques* a été établi par des industriels des secteurs de l'aéronautique et les systèmes de défense. Il est basé sur la physique des défaillances et calibré par des données issues du retour d'expérience et de campagnes d'essais[2].
- Le recueil *UTE 80-810 édition 2000*, issu des travaux du groupe RDF 2000, est un recueil de données de fiabilité de l'*Union de Technologie Électronique*. Il fournit un modèle universel pour le calcul de la fiabilité prévisionnelle des composants, cartes et équipements électroniques.
- Aminal : organisme public flamand qui édite des rapports qui donnent des fréquences d'occurrence pour plusieurs catégories de d'événement initiateur du secteur du procédé (*cf.* www.mina.be).
- Le Rapport Rijnmond (1982) : *Risk Analysis of Six Potentially Hazardous Industrial Objects in the Rijnmond Area: a Pilot Study*, D. Reidel Publish. Co. (dit également le « Rapport Covo »). Cette étude de la fiabilité de composants mécaniques (pompes, canalisations, bras de chargement, vannes, appareils de mesure, équipements électriques, réservoirs) a été conduite dans les années 1970 sur plusieurs établissements industriels aux Pays Bas.

Note : les valeurs d'une base de données à prendre en compte pour un scénario donné doivent correspondre au cas de figure qui serait dangereux pour ce scénario. Si l'on considère par exemple les informations fournies par la base OREDA pour les soupapes, il existe plusieurs chiffres pour différents types de panne : défaillance à l'ouverture, défaillance à la fermeture, *etc.* ; il est important d'utiliser le chiffre adéquat pour son scénario.

3.1 Autres références

- Ouvrage *Methods for determining and processing probabilities* de la *Publication Series on Dangerous Substances* du VROM, ministère néerlandais chargé de l'environnement ([Schüller et al. 1997], ouvrage généralement connu sous le nom du *Red Book* du TNO). Ce document fournit des conseils sur la bonne utilisation des probabilités dans la conduite des analyses de risque. Disponible en ligne au format PDF depuis le site du VROM.
- Guide *ESReDA – Handbook on Quality of Reliability Data*, édité par la société DNV [ESReDA working group on quality of reliability data 2001].
- Rapport d'étude *Évaluation des Barrières Techniques de Sécurité* (Ω10) de l'INERIS, disponible en ligne depuis www.ineris.fr. Ce document fournit des principes généraux d'évaluation de l'efficacité, du temps de réponse et du niveau de confiance accordé à différents types de barrières techniques.
- Rapport d'étude *Démarche d'évaluation des Barrières Humaines de Sécurité* (Ω20) de l'INERIS, disponible en ligne depuis www.ineris.fr. Ce document vise à permettre à des non-experts en facteur humain de prendre en compte de manière simplifiée les opérations humaines composant une barrière de sécurité dans le contexte du scénario d'accident majeur.

[2] Document téléchargeable à l'adresse `http://fides-reliability.org/`.

4

Glossaire

ATEX : Atmosphères explosibles. Plus généralement, il s'agit des directives européennes 94/9/EC réglementant les appareils et systèmes de protection destinés à être employés dans les zones potentiellement explosibles, et la directive 99/92/EC prescrivant des exigences minimales pour la protection des travailleurs susceptibles d'être exposés aux atmosphères explosibles.

Disponibilité : La disponibilité est l'un des attributs de la sûreté de fonctionnement. Elle caractérise l'aptitude d'un système à délivrer un service de confiance justifiée, au moment où elle est sollicitée. La disponibilité est une mesure sans unité ; elle correspond à la proportion du temps de bon fonctionnement sur le temps total d'exécution du système.

Fiabilité : La fiabilité est l'un des attributs de la sûreté de fonctionnement. La fiabilité est définie comme l'aptitude d'un système à accomplir une fonction requise, dans des conditions données, pendant une durée donnée. Un exemple de mesure de fiabilité est le taux de défaillance, inverse du MTTF (*Mean Time To Failure* : temps moyen jusqu'à la première défaillance).

LOPA : *Layer of Protection Analysis*, une méthode semi-quantitative d'analyse des risques.

SIL : *Safety Integrity Level*, ou niveau d'intégrité de sécurité. La norme IEC 61508 spécifie quatre niveaux de sécurité (ou de SIL) pour une fonction de sécurité ; elle détaille les exigences nécessaires pour atteindre chaque niveau d'intégrité.

SIS : *Safety Instrumented System*, ou système instrumenté de sécurité.

SMS : Système de Management de la Sécurité.

PFD : *Probability of Failure on Demand*, ou probabilité de défaillance à la sollicitation.

IEC 61508 : Cette norme porte sur la sécurité fonctionnelle des systèmes électriques, électroniques, et électroniques programmables concernés par la sécurité. Cette norme est orientée « performance » : elle fournit une méthode basée sur des classes de risque pour déterminer le niveau d'exigence en disponibilité des systèmes de sécurité.

IEC 61511 : Cette norme concerne la sécurité fonctionnelle des systèmes instrumentés de sécurité pour le secteur de l'industrie des procédés continus.

Conclusion

Les bases de données de fiabilité fournissent des informations sur la fréquence d'occurrence des événements initiateurs d'accident (tels que les fuites de tuyauterie), ainsi que sur les disponibilité des barrières de prévention et de protection mises en place dans les installations industrielles. Ces données sont employées dans les analyses de risque ainsi que pour la mise en œuvre de politiques de maintenance préventive.

Ces données concernent des événements rares, pour lesquels on ne dispose généralement pas d'un retour d'expérience riche ; elles sont donc incertaines. De plus, la fiabilité des équipements et la disponibilité des barrières dépend de nombreux facteurs, dont la politique d'achat et la politique d'inspection et de maintenance.

Bibliographie

Committee for the Prevention of Disasters, Netherlands (1999). *Guidelines for quantitative risk assessment (the "Purple Book")*. CPR – 18E. Directorate-General for Social Affairs and Employment, Netherlands, The Hague, 1st édition. ISBN 9012087961. 15

ESReDA working group on quality of reliability data (2001). *Handbook on Quality of Reliability Data*. DNV. ISBN B000S1HH16. 16

IEC (2004). IEC61511 : Functional safety – Safety instrumented systems for the process industry sector. Disponible à l'URL : `http://www.iec.ch/`. 9, 13

OREDA (2002). *OREDA – Offshore Reliability Data Handbook*. DNV, 4th édition. ISBN B000K3Z8QS. 15

Schüller, J., Brinkman, J., van Gestel, P., et van Otterloo, R. (1997). *Methods for determining and processing probabilities*. CPR 12E. Kema Nederland BV, The Hague. ISBN 90-12-08543-8. 16

Telle, B., Vanderhaegen, F., et Gautiez, J. (1997). Étude de faisabilité d'une méthode d'intégration des facteurs humains dans les activités d'analyse de sécurité et de développement des systèmes de transports terrestres guidés. vers un modèle d'analyse de la fiabilité humaine basée sur l'évaluation des conséquences de l'activité humaine sur le système. Rapport technique, INRETS. 13

Villemeur, A. (1997). *Sûreté de fonctionnement des systèmes industriels*. Direction des études et recherches d'Electricité de France. Eyrolles, 1ère édition. ISBN 978-2-212-01615-4. 1, 12, 13

Reproduction de ce document

Vous pouvez télécharger le document (et d'autres version des *Cahiers de la Sécurité Industrielle*) au format PDF depuis le site web de l'ICSI.

Institut pour une Culture de Sécurité Industrielle
Association de loi 1901
http://www.icsi-eu.org/

6 allée Émile Monso – BP 34038
31029 Toulouse cedex 4
France

Téléphone : +33 (0) 534 32 32 00
Fax : +33 (0) 534 32 32 01
Courriel : contact@icsi-eu.org

ISSN 2100-3874

ICSI
INSTITUT POUR UNE CULTURE
DE SÉCURITÉ INDUSTRIELLE

6 allée Emile Monso
Zac du Palays - BP 34038
31029 Toulouse Cedex 4
www.icsi-eu.org