SYNTHÈSE

BARPI
DGPR SRT

ARIA
Médiathèque interactive de référence en accidentologie industrielle

Janvier 2020

ACCIDENTOLOGIE DES AUTOMATISMES INDUSTRIELS PARTIE 3/3 :

Les actionneurs

Ministère de la Transition écologique et solidaire

www.aria.developpement-durable.gouv.fr www.ecologique-solidaire.gouv.fr

Sommaire

Introduction

Après les deux premiers volets de l'étude de l'accidentologie des automatismes industriels, voici le 3e volet relatif aux actionneurs. Les deux premiers volets datent de 2012 pour les capteurs et de 2014 pour la fonction traitement. Des exemples récents montrent que les conclusions de ces études sont toujours d'actualité. Néanmoins, pour ce 3e volet, une approche plus concise a été retenue pour mettre en avant, dans un premier temps les perturbations relevées, et, dans un deuxième temps, les causes profondes pour proposer ensuite une série de pistes de recommandations issues d'accidents sélectionnés pour leur pertinence dans la base de données ARIA.

Comme dans les deux volets précédents, des exemples d'accidents sont présentés pour illustrer les propos tout au long de la synthèse. Seuls les éléments de l'accident relatifs à l'actionneur sont mis en avant dans la synthèse. Pour avoir les accidents complets, les résumés sont disponibles en ligne sur le site internet du BARPI https://www.aria.developpement-durable.gouv.fr/.

Méthodologie de l'étude/échantillonnage

Cette synthèse s'appuie sur un échantillon d'accidents industriels répertoriés dans la base ARIA dont le niveau d'information est suffisant pour avoir une bonne compréhension de l'événement (causes, circonstances, conséquences). Une recherche basée sur un champ spécifique de saisie (actionneur automatique et actionneur manuel) puis avec des mots-clés liés aux actionneurs (synonymes, dérivés), suivie d'une analyse du résumé de chaque accident, a permis d'affiner cet échantillon en ne retenant que les accidents répondant à au moins un des 3 critères suivants :

- Un ou plusieurs actionneurs sont à l'origine de l'accident ;
- Un ou plusieurs actionneurs ont aggravé l'accident (par leur non-fonctionnement ou, plus rarement, par leur fonctionnement) ;
- L'absence du (des) actionneur(s) a provoqué ou aggravé un accident (si cette absence est explicitement citée dans l'analyse de l'accident et son installation prévue dans les suites techniques données à l'accident).

Afin de conserver la cohérence avec les deux premiers volets sur les automatismes industriels, les accidents ont été étudiés à partir du 01/01/1992 jusqu'au 31/12/2018. L'échantillon secondaire ainsi obtenu regroupe 326 cas dont 28 étrangers.

Les accidents relatifs au barrage, recensés dans la base ARIA depuis 2010 ont été exclus de l'analyse.

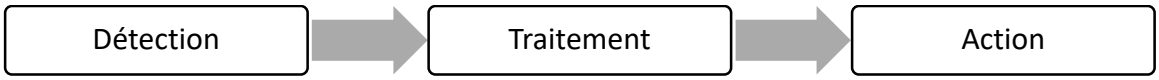
La base ARIA ne recense pas les accidents et incidents concernant les installations nucléaires (bases ASN/IRSN), ni ceux relatifs aux accidents du travail (base EPICEA). Ces spécificités pourraient sous-représenter certains secteurs d'activités pourtant fortement automatisés (centrales nucléaires, secteur de l'automobile et de l'emballage…), qui n'ont donc pas été retenus dans cette étude.

Enfin, la base ARIA étant une base événementielle et non statistique (telles que les bases OREDA, PERD, IEEE, EXIDA), les données collectées et les résumés d'accident ne donnent pas toujours d'informations précises sur la criticité ou la cause technique de la défaillance de l'actionneur, sa technologie, son niveau d'entretien. Il est également possible qu'un biais soit introduit entre les secteurs d'activités étudiés, car la remontée d'informations sur les accidents peut varier fortement d'un secteur à un autre en raison du nombre d'installations en activité, du niveau de relations qui existent entre le BARPI et les représentants des différents secteurs et du classement ICPE du site accidenté (les sites classés Seveso faisant l'objet d'un suivi renforcé par exemple).

Partie 1 : Contexte de l'étude

1- Définition de la fonction « actionneur » des automatismes industriels

Les automatismes industriels sont composés de 3 fonctions :



La première fonction sert à détecter une situation accidentelle ou une déviation dans le fonctionnement d'un procédé. La détection apporte l'information au système automatisé. Plusieurs types de capteurs sont disponibles dans le milieu industriel :

- Capteur de paramètres physiques : température, pression, densité, poids… ;
- Capteur de paramètres spatiaux : état, position, niveau, profondeur, interface… ;
- Capteur de phénomènes anormaux : flamme, fumée, ATEX, substance dangereuse… ;
- Capteur de paramètres cinématiques : débit, vitesse, accélération, vibration… ;
- Capteur de paramètres physico-chimiques : pH, conductivité, résistivité…

L'ensemble de l'accidentologie lié à ces capteurs est disponible dans la synthèse : Accidentologie des automatismes industriels partie 1/3 : Le capteur.

La deuxième fonction regroupe l'ensemble des composantes techniques et humaines d'un automate nécessaire à la transmission de l'information du capteur vers l'actionneur : alimentation de l'unité centrale, transmissions, cartes électroniques, programmations, interfaces homme/machine… La flèche entre la fonction détection et la fonction traitement est prise en compte dans cette deuxième fonction.

L'ensemble de l'accidentologie lié à la fonction « traitement » est disponible dans la synthèse : Accidentologie des automatismes industriels partie 2/3 : la fonction traitement.

Concernant la troisième fonction, « action », objet de la présente synthèse, l'INERIS donne la définition suivante dans son « Guide omega_10 » :

La sous-fonction "action" est réalisée par des actionneurs et des éléments terminaux. Les actionneurs transforment un signal (électrique, pneumatique ou hydraulique) en phénomène physique qui permet de commander le démarrage d'une pompe, la fermeture ou l'ouverture d'une vanne… Selon l'énergie motrice, on parle d'actionneur électrique, pneumatique ou hydraulique. Ils sont couplés aux éléments terminaux. Les éléments terminaux sont commandés par des actionneurs. On retrouve notamment sous cette terminologie : les vannes, les machines tournantes (pompe, compresseur …), les alarmes sonores et visuelles.

Figure 1 : exemple : un actionneur manuel active une pompe à distance - ©BARPI

Parmi les actionneurs étudiés, certains ont une finalité de conduite du procédé industriel, alors que d'autres, intégrés dans des systèmes instrumentés de sécurité (voir définition INERIS ci-dessous), constitue des barrières de prévention, d'atténuation ou de protection.

Les statistiques présentées et l'analyse effectuée sur les perturbations et causes profondes ne prennent pas en compte cette distinction entre ces deux types d'actionneurs. Des recommandations propres aux systèmes instrumentés de sécurité sont par ailleurs formulées dans cette synthèse.

OMEGA 10 INERIS : Dans les systèmes instrumentés de sécurité (SIS), la finalité de la fonction de sécurité remplie partiellement ou totalement par le SIS réside d'une part dans la détection du phénomène dangereux et d'autre part dans la mise en position finale de sécurité de ces éléments (ouvert/fermé, arrêt/démarrage). Le SIS pourra assurer la fonction totalement (détection, traitement, action finale) ou partiellement (le SIS assure par exemple la fonction de détection et de traitement jusqu'à une alarme, l'action finale peut ensuite être réalisée par une action humaine).

Concernant le signal envoyé à l'actionneur, c'est-à-dire le lien entre le « traitement » et l'« action », il est intégré, soit dans la fonction « traitement », comme les interfaces hommes/machine, soit dans la fonction « action » lorsqu'il concerne l'arrivée du signal à l'actionneur (système de commande, fluide vecteur (électricité, air, huile)…). Des exemples sont présentés dans la présente synthèse.

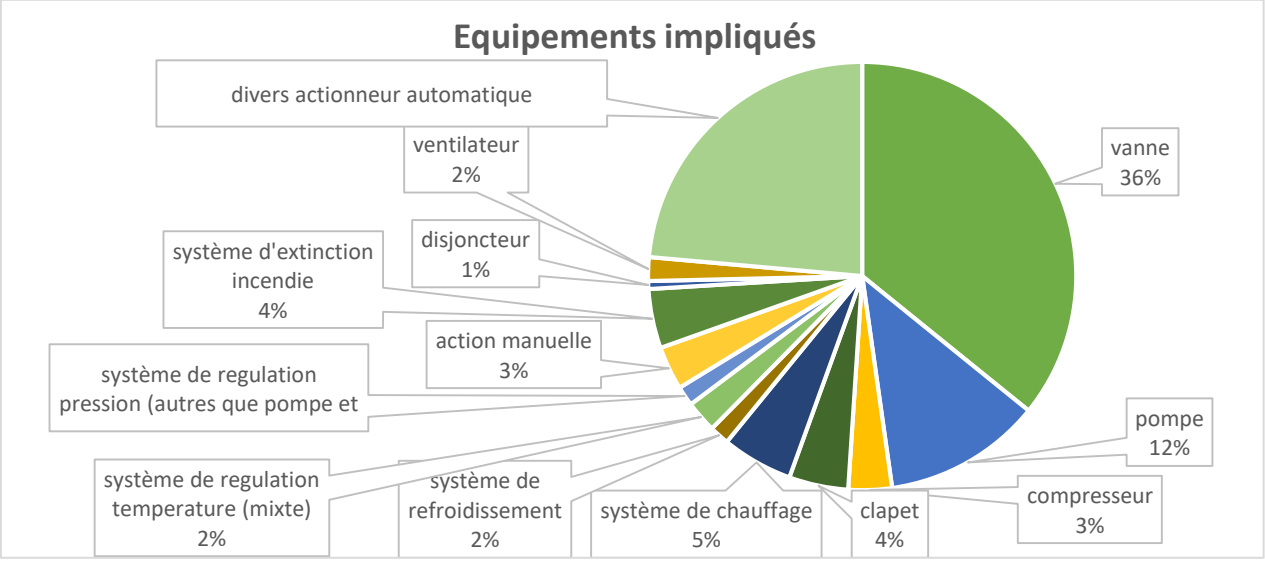
L'actionneur peut aussi disposer d'un ou plusieurs capteurs, qui permettent de transmettre l'information de leur état, position ou de la bonne réalisation de l'action (exemple : le signal de fin de course d'une vanne).

2- Définition du champ de l'étude

Après les capteurs et la fonction traitement, cette synthèse regroupe les accidents mettant en jeu le 3eme élément qui constitue un automatisme industriel, c'est-à-dire les actionneurs comme définis précédemment. Les actionneurs manuels et automatiques ont été étudiés. Pour cette étude, il a notamment été retenu :

- Des équipements à vocation de transfert de fluide (clapet, vanne, pompe, compresseur) ;
- Les systèmes de régulation des paramètres physiques (pression, température) d'un procédé (chauffage, refroidissement…) ;
- Les dispositifs de conduite, de prévention ou de protection, qui relèvent d'un déclenchement automatique ou manuel sur sollicitation d'un automate (traitement) suite à une détection de paramètres par un ou des capteurs (cf. Définitions au paragraphe précédent).

Les systèmes complètement autonomes, ne nécessitant pas de fonction « traitement », comme par exemple les « sprinklers », n'ont pas été retenus pour cette étude.



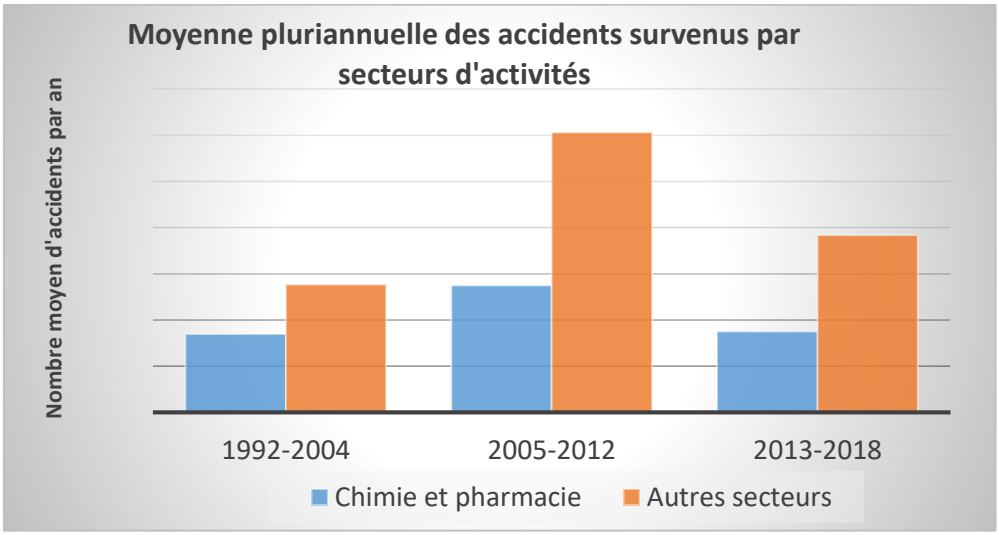
Ce graphique montre la diversité des actionneurs automatiques ou manuels qui peuvent être à l'origine d'incidents ou d'accidents. Les organes de transfert de fluide, type vanne et pompe, représentent une part majoritaire des équipements impliqués.

Partie 2 : Présentation de l'accidentologie

1- Données globales de l'accidentologie

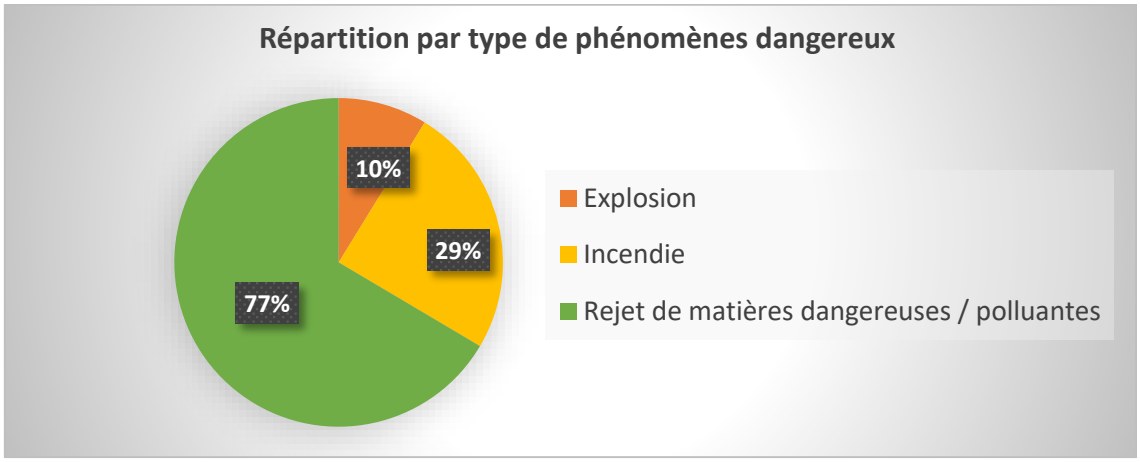
Les secteurs d'activités présentant le plus grand nombre d'accidents impliquant un ou plusieurs actionneurs sont, en premier, le secteur de la chimie/pharmacie, qui regroupe globalement 1/3 des accidents recensés de 1992 à 2018, puis viennent les secteurs de l'industrie alimentaire, le raffinage et la métallurgie, qui représentent pour chacun environ 10 % des accidents.

Le nombre annuel d'accidents impliquant un ou plusieurs actionneurs a connu un fort accroissement à partir de 2005. Le développement de la mise en place d'actionneurs automatiques dans les différentes industries peut expliquer l'accroissement du nombre d'accidents. Puis leur fiabilité a été renforcée, ce qui a permis de faire diminuer le nombre d'accident à partir de 2012.



2- Accidentologie détaillée

D'après l'échantillon retenu, un accident ayant pour origine ou aggravation, la défaillance ou l'absence d'un actionneur, conduit le plus fréquemment à un rejet de substances dangereuses. Il s'agit le plus souvent de rejet prolongé.



La mise hors service volontaire d'un actionneur aboutissant à un événement par absence de mesures compensatoires est aussi prise en compte. Un exemple concret est présenté ci-dessous :

ARIA 40256 (11/03/2011) : Un séisme majeur (Mw = 9) touche l'île de Honshu (Japon).

Une fuite sur une canalisation portuaire de GPL est détectée dans la raffinerie d'un grand complexe pétrochimique. La flaque de gaz se répand sur le parc adjacent de 17 sphères de butane / butylène et s'enflamme sur une source d'ignition inconnue. L'incendie se développe rapidement, entraînant la chute de la plupart des sphères dont les pieds se rompent et 5 BLEVE (boiling liquid expanding vapor explosion) en cascade avec une boule de feu de 600 m de diamètre pour le principal.

La fuite initiale de GPL par écrasement d'une canalisation, résulte de l'effondrement d'une sphère en surplomb remplie d'eau pour une épreuve hydraulique. La mise en sécurité automatique du circuit de transport de gaz déclenchée par les sismomètres était inopérante sur cette partie du réseau, **la vanne de coupure automatique étant shuntée en position ouverte à la suite de problèmes antérieurs de commande pneumatique.** La procédure temporaire de fermeture manuelle de cette vanne dans l'attente de la réparation n'a pu être mise en œuvre en raison d'une flaque importante de GPL.

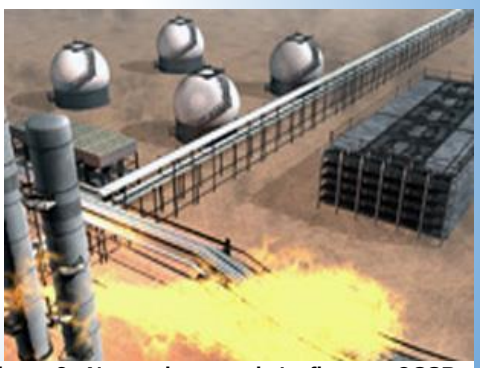


Figure 2 : Nuage de gaz qui s'enflamme, ©CSB

En parallèle des phénomènes dangereux majoritaires mis en évidence dans l'échantillon, les conséquences les plus fréquemment observées sont économiques et environnementales.

	Echantillon étudié (326 cas)	Type IC base ARIA 1992-2018 (32 571 cas)
CONSÉQUENCES HUMAINES	**21%**	**22%**
--> MORTS	2%	5%
--> BLESSES GRAVES	4%	5%
--> BLESSES TOTAUX	21%	21%
CONSÉQUENCES ÉCONOMIQUES	**72%**	**81%**
--> Dommages matériels internes ou externes	62%	83%
--> Pertes d'exploitation internes ou externes	36%	28%
CONSÉQUENCES SOCIALES	**21%**	**23%**
--> Chômage technique, incapacité de travail (tiers)	3%	10%
--> Privation d'usages - eau potable, électricité, téléphone, transport public et autres	3%	3%
--> Nuisance sonore	1%	0%
--> Population évacuée	5%	5%
--> Population confinée	6%	2%
--> Périmètre de sécurité	15%	11%
--> Interruption de la circulation	5%	3%
CONSÉQUENCES ENVIRONNEMENTALES	**53%**	**33%**
--> Type d'atteinte au milieu : air, eau, nappe, sol	58%	33%
--> Atteinte à la faune ou flore sauvage, espèces cultivées ou exploitées, animaux d'élevage	7%	8%
AUTRES CONSÉQUENCES	3%	2%

Figure 3 : Tableau des conséquences

Les conséquences économiques sont significatives dans les accidents impliquant un actionneur. Les dommages matériels sont liés à l'équipement à l'origine du sinistre, qui nécessite dans la plupart des cas d'être remplacé. Des pertes d'exploitation sont observées dans le cas où l'incident ou accident entraine la mise à l'arrêt puis le redémarrage des installations.

Les conséquences environnementales, celles qui portent atteinte au milieu naturel par le biais de pollution ou de rejet de matière dans l'atmosphère, les milieux aquatiques de surface ou souterrains et dans les sols, sont au-dessus de la moyenne de celles rencontrées lors d'accidents survenus dans une installation classée ou assimilée entre 1992 et 2018.

Dans l'échantillon étudié, 6 accidents dont 5 explosions ont conduit à des décès concernant uniquement des employés. Il n'y a pas de victimes externes.

Figure 4: ARIA 3536 : vue de l'unité en cause après l'explosion - ©Exploitant

ARIA 3536 (1992) : Un premier accident a conduit à une explosion faisant 1 décès. L'automatisation partielle de l'arrêt d'urgence de l'unité est mise en cause dans cet accident.

ARIA 5989 (1994) : Deux activités simultanées et un défaut dans la programmation de l'automate indiquant une ouverture de vanne lors de sa réinitialisation conduisent à une fuite d'ammoniac blessant 3 ouvriers et provoquant le décès de l'un d'eux.

ARIA 7956 (1995) : Une explosion d'hydrogène suivie d'un incendie provoque le décès d'un opérateur manœuvrant des vannes. La présence d'une vanne automatique tout ou rien aurait permis d'éviter l'envoi d'un produit dans un réacteur en cours de lavage, la réaction avec l'hydrogène a conduit à l'explosion.

L'exemple ci-après met en cause le signal arrivant à l'actionneur :

ARIA 7069 (1996) : L'inversion de flexibles de commande d'une vanne pneumatique induisant une position contraire à la logique de l'automate local entraine une explosion et un mort. L'exploitant mettra alors en place des synoptiques de positionnement des vannes des systèmes d'introduction des poudres basés sur des fins de course et un système de consignation mécanique.

ARIA 14700 (1997) : Une explosion a été aggravée par l'absence d'arrêt d'urgence automatique. Un employé ayant tenté d'actionner cet arrêt d'urgence est décédé dans l'incendie provoqué par l'explosion.

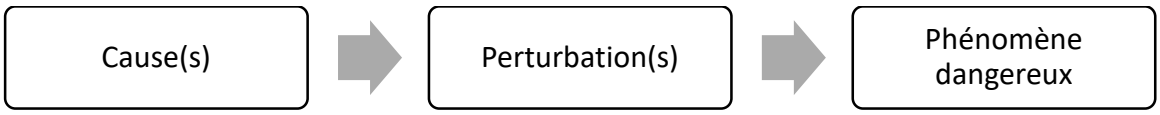
ARIA 12280 (1998) : A l'origine, une défaillance suspectée du dispositif de commande d'une porte de four conduit à l'explosion de ce dernier provoquant un décès.

Depuis 20 ans, aucun décès n'est à déplorer suite à un accident ayant été causé par un actionneur.

Partie 3 : Analyse des causes des incidents /accidents

1- La démarche d'analyse des causes du BARPI

Pour l'analyse des causes des incidents/accidents impliquant un ou plusieurs actionneurs, la méthodologie développée par le BARPI et utilisée dans la présente synthèse, repose sur un processus simple, menant à la caractérisation de 3 blocs distincts :



Les phénomènes dangereux ont été détaillés dans le paragraphe précédent.

Les **perturbations** sont les déviations par rapport à un état attendu de fonctionnement qui conduisent à un phénomène dangereux. On peut citer en exemple : les défaillances de matériel, les interventions humaines inappropriées, les agressions naturelles ou technologiques.

Ces perturbations ont généralement des origines moins visibles. Ce sont les véritables « **causes** », parfois appelées « causes profondes » ou « causes racines » des accidents. Celles-ci peuvent être de plusieurs natures :

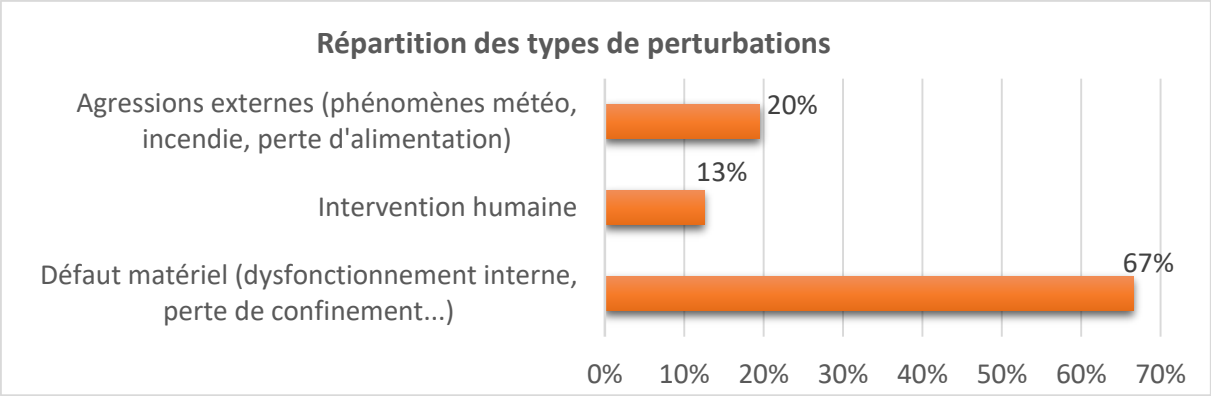
Les facteurs organisationnels	Ils concernent l'environnement de travail et les mesures de gestion du risque tels que l'organisation des contrôles, la gestion de la formation et des compétences internes et externes, les procédures et consignes, l'identification des risques, l'organisation du travail et de l'encadrement, la communication, l'ergonomie, le choix des équipements et des procédés...
Les facteurs humains	Ce sont les facteurs perturbant les capacités physiques / cognitives / mentales d'un employé du site et qui ne sont pas sous la responsabilité de l'organisation.
Les facteurs impondérables	Ce sont les éléments à l'origine d'une perturbation ne pouvant être anticipés ou maîtrisés par l'organisation en place sur le site accidenté. Par exemple les vices de fabrication.

Pour chaque type de blocs, cause, perturbation et phénomène dangereux, il peut y en avoir plusieurs pour un accident. En effet, les accidents peuvent générer un ou plusieurs phénomènes dangereux et être expliqués par des successions de perturbations et différentes causes.

Dans un premier temps, le chapitre suivant traite des principales perturbations à l'origine des accidents impliquant un ou des actionneurs. Les causes profondes sont développées par la suite.

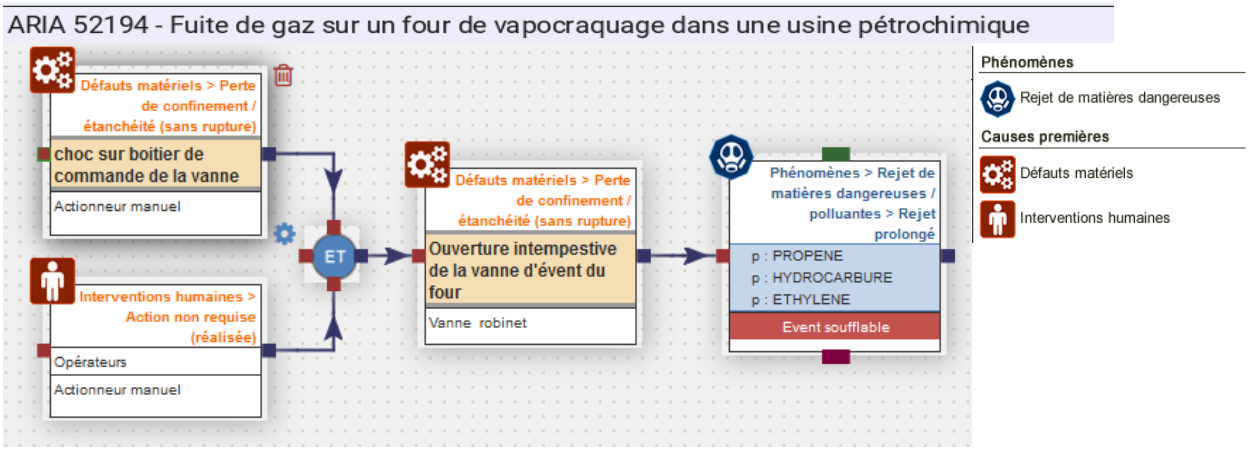
2- Analyse des perturbations

L'histogramme ci-dessous présente la répartition des causes premières, appelées « perturbations », mettant en cause un actionneur à l'origine des accidents. Les pourcentages sont exprimés par rapport au total des accidents pour lesquels l'information est connue : sur 326 accidents, il y en a 287 (soit 88 % des cas) pour lesquels on dispose d'une certaine connaissance (avérée ou supposée) sur la cause première de l'événement. Ce pourcentage élevé s'explique par le fait que les accidents ont fait l'objet d'une sélection selon leur pertinence pour être retenus dans cette étude.



Dans cet histogramme, le pourcentage total est égal à 100 % car seule la cause première a été retenue, c'est-à-dire, celle qui a conduit directement au phénomène dangereux (voir graphique BARPI). Mais cette dernière peut résulter d'une combinaison de perturbations. Par exemple :

- une intervention humaine non requise associée à un défaut matériel :



- une défaillance d'automate associée à une intervention humaine mal effectuée :

ARIA 31023 (16/11/2005) : Pollution de cours d'eau par des phytosanitaires :

Dans une usine de phytosanitaires (herbicides, raticides...), 4,5 m³ d'une solution anti-poux contenant des substances organophosphorées accidentellement déversés dans un cours d'eau polluent sur au moins 4 km plusieurs ruisseaux et étangs. **Résultant conjointement de la défaillance d'une vanne automatique et d'une erreur humaine** (ouverture d'une vanne manuelle) lors d'un transfert, le produit dangereux s'est échappé d'une cuve de stockage et s'est déversé dans une rétention mal dimensionnée. Les vapeurs de phytosanitaire incommodent 2 personnes dont 1 employé ; le chauffeur livreur victime d'un malaise est évacué. Des centaines de poissons morts sont découverts.

2-1- Défauts matériels

La première série majoritaire de perturbations identifiées dans l'échantillon (67 %) relève de la catégorie des « défauts matériels », dans laquelle plusieurs sous catégories peuvent être mises en évidence.

Tout d'abord, les défauts ou dysfonctionnements internes propres à l'actionneur en lui-même ou à son système de commande peuvent notamment être détaillés comme suit :

- Des défaillances ou dysfonctionnement non déterminés avec précision (concernent environ 50 % des défauts matériels) ;
- Des systèmes inopérants à la sollicitation, qui concernent surtout les vannes et clapets, tels qu'un actionneur bloqué fermé ou bloqué ouvert : ARIA 32806, 39929, 46230 ;
- Des déclenchements intempestifs, tels que des actionneurs qui se déclenchent sans raison particulière : ARIA 22858, 42726, 50424, 49833 ;
- Des systèmes de commande défaillants : ARIA 22793 ;
- Des défaillances au niveau du signal de fin de course de fermeture, telles que le signal de fermeture de la vanne indique que celle-ci est fermée alors qu'elle ne l'est pas : ARIA 22553, 25057 ;
- Des pannes pour les actionneurs se présentant comme des systèmes plus complexes tels que les systèmes de refroidissement ou encore les pompes : ARIA 26475, 31935.

Quand les dysfonctionnements internes touchent des systèmes de protection, en cas d'incendie par exemple, les systèmes d'extinction automatique, la défaillance de l'actionneur peut entrainer une aggravation d'un événement en cours : ARIA 32253, 49093.

ARIA 43181 (22/12/2012) : Feu de compresseur de gaz craqué

Dans l'unité de vapocraquage d'un site pétrochimique classé Seveso, un feu d'huile se déclare sur un compresseur de gaz craqué. La mise en sécurité des installations entraîne le torchage des hydrocarbures de l'unité avec émission d'une abondante fumée noire durant 24 h. Les services de secours reçoivent alors de nombreux appels de riverains.

Le site avait redémarré 10 jours plus tôt après un arrêt quinquennal de maintenance durant lequel la ligne de compression avait été révisée.

L'expertise technique post-accident révèle qu'une clé à frappe avait été oubliée, probablement lors de l'arrêt quinquennal, au niveau du 3ème étage du compresseur accidenté. Le jour de l'accident, la clé finit par passer dans les étages inférieurs du compresseur et percuter ses roues, entraînant ainsi d'importantes vibrations, puis finalement son arrêt de sécurité sur déclenchement d'une sécurité « vibration haute ». **Certains dispositifs de sécurités associés à la mise en sécurité du compresseur ont alors mal fonctionné :** défaut d'isolement du compresseur dû à un clapet anti-retour encrassé et d'une vanne motorisée mal fermée, son moteur électrique coupé après la mise en sécurité, mauvais fonctionnement de l'organe interne garantissant l'étanchéité entre l'huile et les gaz et l'équilibrage des pressions lors d'un arrêt de sécurité.

Figure 5 : compresseurs sur un site chimique - ©DRIRE

Ces dysfonctionnements entraînent le passage à travers la garniture d'une partie des gaz craqués dans l'huile qui s'est enflammée.

L'échantillon étudié fait aussi apparaître des perturbations liées à la conception du système instrumenté :

- Actionneur non conforme au modèle prévu : ARIA 41870 ;

- Matériau de l'actionneur non adapté : ARIA 39629 ;
- Actionneur sous dimensionné : ARIA 34733, ce qui peut entrainer, pour ce qui concerne les actionneurs servant de système de protection, une perte d'efficacité, comme par exemple pour les systèmes d'extinction incendie ;
- Actionneur avec un temps de réponse trop long : ARIA 26925, 22320, 41517 ;
- Problème de discordance : l'information disponible dans le système de traitement ne correspond pas à la position réelle de l'actionneur. Exemples pour des vannes : ARIA 38027 et 41300. Il se peut aussi que l'information de la position réelle de l'actionneur ne soit pas disponible dans le système de traitement : ARIA 52784 ;
- Vice de fabrication : ARIA 51165 ;
- Système qui se dégrade dans le temps : ARIA 41516.

Peuvent ensuite être extraites de l'échantillon, les perturbations telles que les fuites ou pertes de confinement (ARIA 48845, 42415, 41870) ou au contraire les colmatages et/ou encrassement (ARIA 6343, 51505) des automatismes qui ne peuvent alors remplir leur fonction. Pour ce type de perturbations, des causes profondes liées à l'absence de contrôle ou à des défauts de maintenance pourront être mises en évidence (voir chapitre suivant).

2-2- Interventions humaines

Les défauts matériels ne sont pas les seules perturbations qui apparaissent dans l'échantillon d'accidents étudiés. Ils peuvent parfois être associés à des interventions humaines qui ont conduit les opérateurs, soit à faire une action non requise, soit à ne pas réaliser ou mal effectuer une action requise (erreur de perception, d'interprétation, d'exécution, décision…).

Les interventions humaines sur les systèmes comprenant un actionneur peuvent conduire à des actions erronées lors des différentes phases de la vie d'une installation :

Figure 6 Un opérateur face à un tableau de commande - ©BARPI

2-2-1- En phase de conception

Lors de la phase de conception du système automatisé (choix de l'équipement, programmation…), une erreur humaine ou un mauvais choix peut ensuite entrainer un défaut sur l'action à réaliser par l'actionneur lors de sa sollicitation :

- Erreur de programmation de l'actionneur : ARIA, 43695 (voir résumé encadré ci-après), 17253 ;
- Erreur dans le dimensionnement du système : ARIA 18411 ;
- Choix erroné dans la programmation de l'actionneur, choix de la sécurité positive ou non : ARIA 38055, 36390, 42921, 42920, 47536.

Cela signifie que, face à une défaillance, il faut étudier la possibilité de la mise en sécurité positive de l'actionneur et les risques associés.

La **mise en sécurité positive**, pour les actionneurs intégrés dans des SIS, signifie que, en cas de défaillance ou de perte d'énergie de l'actionneur ou du traitement du signal, ce dernier est programmé par défaut dans la position où il assure sa fonction de sécurité. Exemples : si une vanne sert à confiner un circuit en cas de fuite, sa position de sécurité sera alors « fermée » ; au contraire, si une vanne sert à vidanger un circuit, sa position de sécurité sera alors « ouverte ». C'est pourquoi des erreurs de décision ou d'interprétation dans le choix de la position en sécurité positive peuvent survenir.

2-2-2- EN PHASE DE CONSTRUCTION / MONTAGE

D'autres interventions humaines menant à des défaillances des systèmes se produisent lors de l'installation de l'actionneur dans son circuit de commande (montage, branchement, lignage) :

- Erreur de branchements de fluide (électricité) : ARIA 10165 ;
- Erreur dans le positionnement de l'actionneur dans le circuit de l'installation : ARIA 19596 ;
- Défaut de vérification de lignage : ARIA 50755 ;
- Inversion des flexibles de commande (pneumatique) et absence de signal de fin de course : ARIA 7069 ;
- Défaut dans le montage de l'actionneur : ARIA 45061, 49845 ;
- Mauvais réglage de vanne/clapet : ARIA 12671.
- Défaut de serrage : ARIA 49161.

Figure 7: ARIA 44070 : Vanne cadenassable ouverte par erreur - ©Exploitant

Une synthèse complète sur les erreurs de lignage (positionnement de circuit) est disponible sur le site internet du BARPI, certains accidents peuvent concerner des actionneurs, le but n'est pas ici de reprendre les conclusions de cette synthèse.

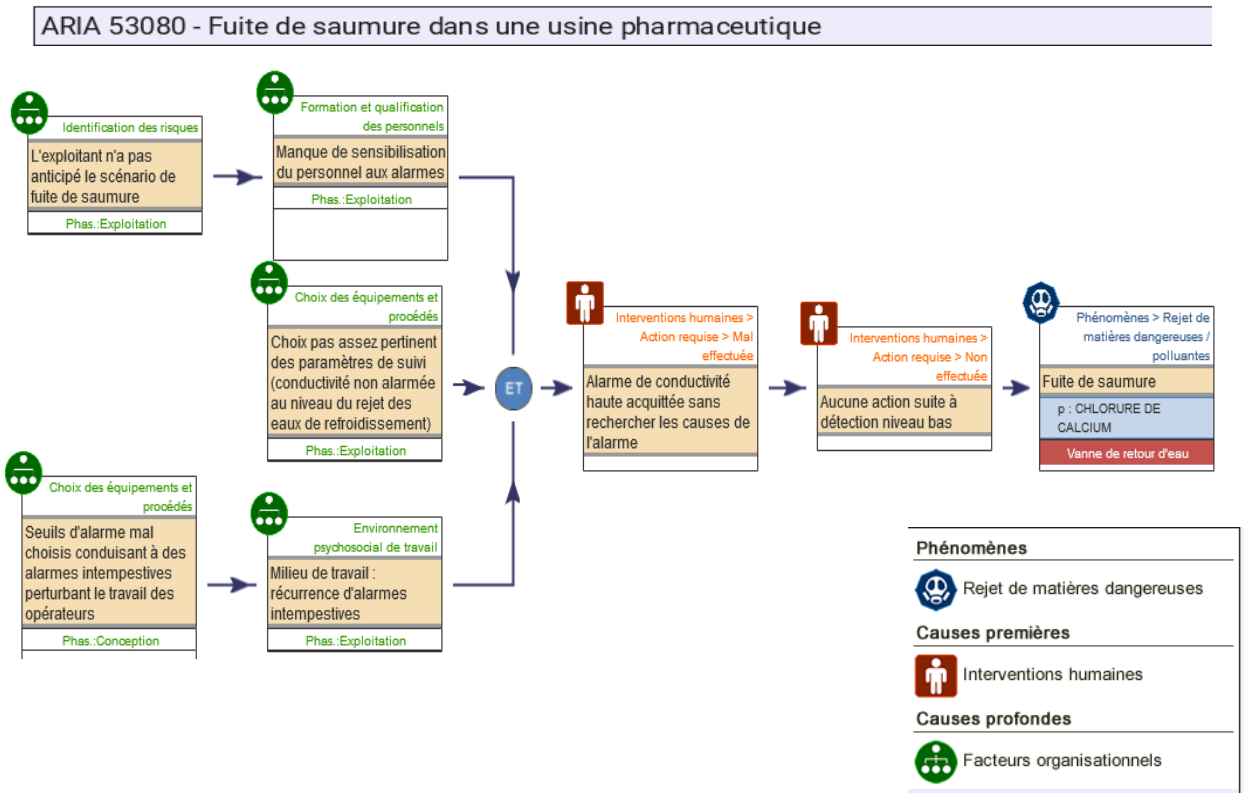
2-2-3- EN PHASE D'EXPLOITATION

Certains systèmes automatisés nécessitent en complément, une action manuelle sur l'actionneur suite à une alarme par exemple. Dans ce cas, l'accident peut être lié à une :

- Alarme acquittée sans action : ARIA 53080 ;
- Erreur sur l'équipement à manœuvrer : action réalisée sur le mauvais réservoir (ARIA 13228), mauvaise vanne fermée ou ouverte par exemple ;
- Erreur sur la manœuvre à effectuer : ARIA 47277, 50055 ;
- Ouverture au lieu de fermeture et/ou inversement : ARIA 35863 ;
- Vanne laissée ouverte : ARIA 10165, 47813 ;

ARIA 8325 (15/02/1996) : Débordement de gazole et pollution de deux cours d'eau

Dans une société de transport, le chauffeur d'un poids lourd s'absente lors du remplissage, pistolet bloqué, du réservoir de son véhicule. La sécurité d'arrêt automatique en fin de remplissage ne fonctionne pas et plusieurs centaines de litres de gazole se déversent sur le sol, puis rejoignent l'ERIE et la LEYSSE. Le directeur de la société doit régulariser sa situation administrative et mettre en conformité son installation de distribution de liquides inflammables.



2-2-3-En phase de maintenance, controles et/ou travaux

Il est constaté dans l'échantillon étudié que des interventions humaines mal menées interviennent plus particulièrement lors des phases de maintenance, de contrôles et/ou de travaux.

ARIA 43695 (18/04/2013) : Incident de chaufferie dans une usine pharmaceutique

Dans une usine pharmaceutique classée Seveso bas, une chaudière au gaz naturel passe en surchauffe lors de sa remise en route. Un technicien sous-traitant en charge de l'exploitation de la chaufferie remet en marche l'oxydation thermique des COV par action sur l'interface homme/machine. Quelques minutes plus tard, l'alarme LIE retentit. La chaudière se met en by-pass, puis automatiquement en sécurité. Le technicien détecte un départ de feu au premier étage, dans la zone du ventilateur général.

L'incendie est dû à la présence d'un excès de combustible fortement chargé en COV qui s'explique par :

- **une erreur de conception du programme de l'installation COV** qui rendait possible le passage en incinération quelle que soit la LIE du mélange. L'installation COV était en redémarrage suite à une opération de maintenance préventive par un sous-traitant. Or, la sécurité existante asservie à des seuils d'explosivité et permettant de dévoyer le flux de COV en cas d'atteinte des seuils ne fonctionnait qu'en mode « incinération » et non en redémarrage.
- une erreur sur la position de vannes (soutirage et régulation) due à la coexistence d'un pilotage différent entre mode automatique et manuel, entraînant la ré-injection totale de condensats fortement chargés en COV.

L'exploitant complète les consignes de pilotage et du processus de gestion des changements des automatismes (automatique/manuel).

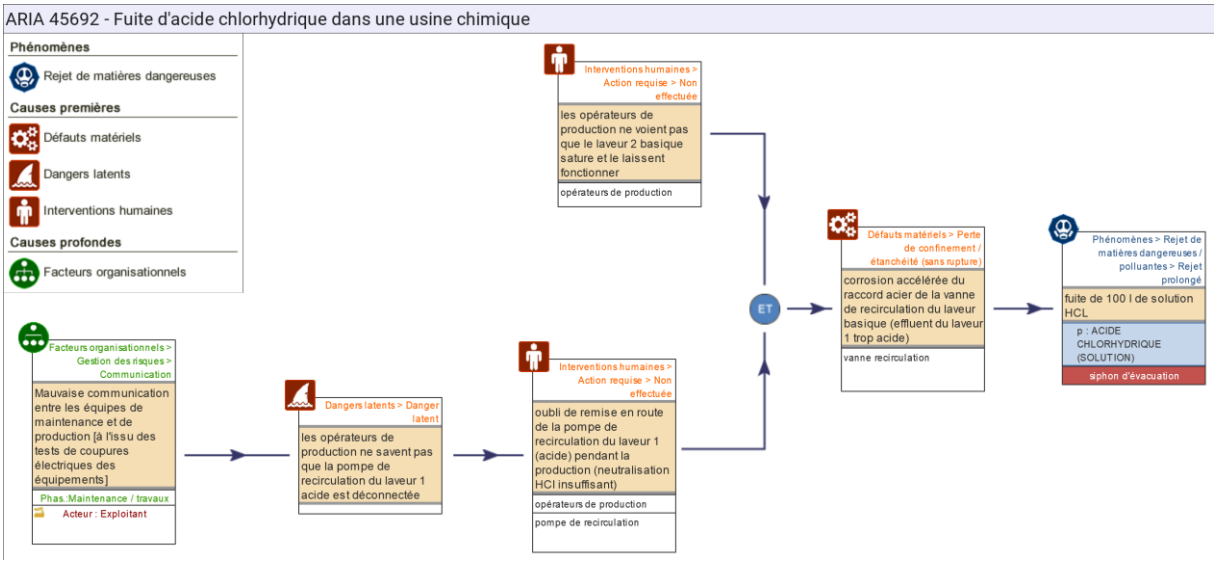
Ces actions malencontreuses sont rencontrées soit lors de l'intervention en elle-même, soit au moment de l'arrêt des systèmes ou lors de leur redémarrage. Ces phases sont des moments transitoires critiques dans la vie d'une installation industrielle.

Des modifications du mode de fonctionnement habituel du système sont mises en place : shunt, by-pass, passage en mode manuel, intervenants différents par rapport à d'habitude (sous-traitant ou opérateur de maintenance interne). Tous ces cas de figure ont pu être à l'origine d'accidents causés par un actionneur.

Shunt ou by-pass : des systèmes automatisés ont pu être mis hors service pour permettre une intervention sur un équipement du système ou sur une autre installation à proximité du système shunté afin d'éviter son déclenchement intempestif (par exemple en phases d'arrêt/démarrage). Dans ces situations, les actionneurs ont été bypassés mais avec des mesures compensatoires au cours de l'intervention. A la fin de cette dernière, lors de la remise en service de l'installation globale, le by-pass n'a pas été supprimé : ARIA 9967, 25239.

Passage en mode manuel : Les phases transitoires arrêt/redémarrage font parfois l'objet de modification de l'exploitation du process dont notamment le passage en mode manuel sur certains actionneurs normalement automatiques : ARIA 11181, 50604, 44896, 35882, 34624, 43736, 45692. Des erreurs sont alors commises par les opérateurs peu habitués à ce mode de fonctionnement. Par exemple, une vanne a été ouverte alors que cet ordre n'était pas requis à ce moment-là : ARIA 44793. Autre exemple, dans cette configuration de pilotage d'une installation, une insuffisance de l'analyse de risque avant intervention peut également être à l'origine d'erreurs humaines : ARIA 32484.

Sous-traitance : Dans les phases de maintenance et/ou travaux, certains accidents impliquent des sous-traitants ayant effectué des réparations sur des actionneurs : ARIA 16080, 22573, 44996, 48569, 50109. Ces accidents mettent aussi en avant un défaut de vérification/réception des travaux par l'exploitant du site suite aux interventions (voir chapitre suivant sur les causes profondes).



Une synthèse complète sur les accidents liés à la sous-traitance a été rédigée par le BARPI, certains accidents peuvent concerner des actionneurs. Les conclusions de cette synthèse sont disponibles sur le site internet du BARPI au lien suivant : Sous-traitance et maîtrise des risques.

2-3- Agressions externes

Dans ce paragraphe, sont présentées les perturbations qui ont une origine extérieure à l'équipement lui-même ou à l'installation dans son ensemble.

2-3-1- LES AGRESSIONS EXTERNES D'ORIGINE NATURELLE

Elles sont principalement liées à la météo : la foudre (ARIA 52087) ou encore des phénomènes de gel de l'actionneur (ARIA 38027) peuvent rendre les actionneurs inopérants.

Un événement présenté précédemment résulte de l'important séisme qui a touché l'île du Japon en 2011 : ARIA 40256.

2-3-2- LES AGRESSIONS EXTERNES D'ORIGINE ANTHROPIQUE

L'actionneur est pris dans un événement ayant une origine anthropique. Exemples :

- Une pompe prise dans un incendie qui ne peut alors plus remplir sa fonction : ARIA 14700 ;
- Un coup de bélier sur une vanne : ARIA 42163 ;
- Un choc sur une vanne : ARIA 52194 ;
- Un incendie de coffret électrique d'alimentation de l'automate pilotant l'actionneur : ARIA 50793.

Des actions de malveillance peuvent également entrainer le non-fonctionnement d'un actionneur : ARIA 7435.

Figure 8 : ARIA 50793 : intervention dans un abattoir pour feu d'un coffret électrique entrainant une fuite d'ammoniac - ©Synergi

2-3-3- LES PERTES D'UTILITES

Des événements de l'échantillon d'accidents étudiés ont pour origine une perte d'utilités. Dans le cas des actionneurs, il peut s'agir de la perte d'alimentation électrique, en air ou encore hydraulique suivant le type d'actionneur :

- Perte d'alimentation électrique (ARIA 42235) : coupure générale de courant (ARIA 35841, 49984), défaut dans le montage électrique (ARIA 36110, 48580), défaut de branchement (ARIA 36198, 49965), orage à l'origine de la perte (ARIA 36770, 40197), court-circuit interne (ARIA 32132, 40506), défaut liaison « Ethernet » (ARIA 43639) ;

Figure 9 : ARIA 54499 : incendie de câbles électriques alimentant une électrovanne de sectionnement d'une tuyauterie d'ammoniac - ©DREAL

- Perte d'alimentation en air : rupture de la tuyauterie d'air comprimé pilotant une vanne automatique (ARIA 7131), fuite d'air comprimé alimentant un système de transfert par mise sous pression (ARIA 19969), ouverture par manque d'air d'une vanne (ARIA 49735) ;

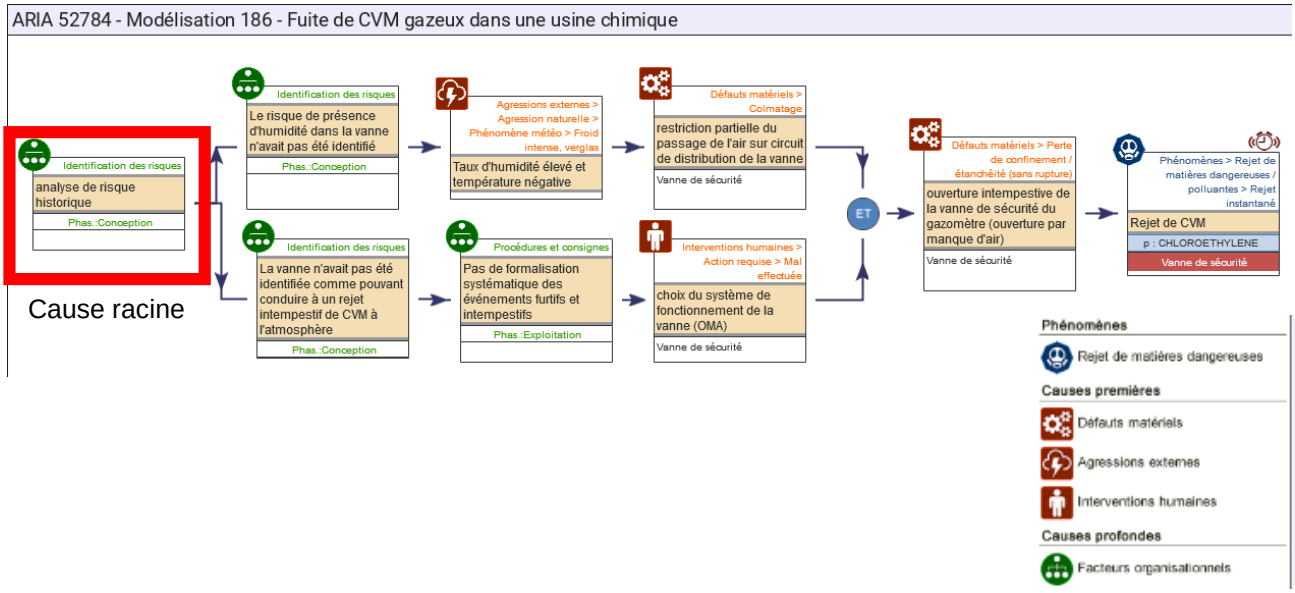
- Défaut d'alimentation sur des organes actionnés par pression hydraulique : ARIA 7440 et 22683.

D'où la nécessité de bien étudier la mise en sécurité positive des actionneurs et les risques associés sur perte d'utilités ou de signal.

Une fois ces différentes perturbations mises en lumière, il convient de mettre en évidence les causes profondes impliquées dans les accidents ou incidents survenant du fait d'un ou plusieurs actionneurs. Les raisons justifiant de rechercher les causes sont multiples :

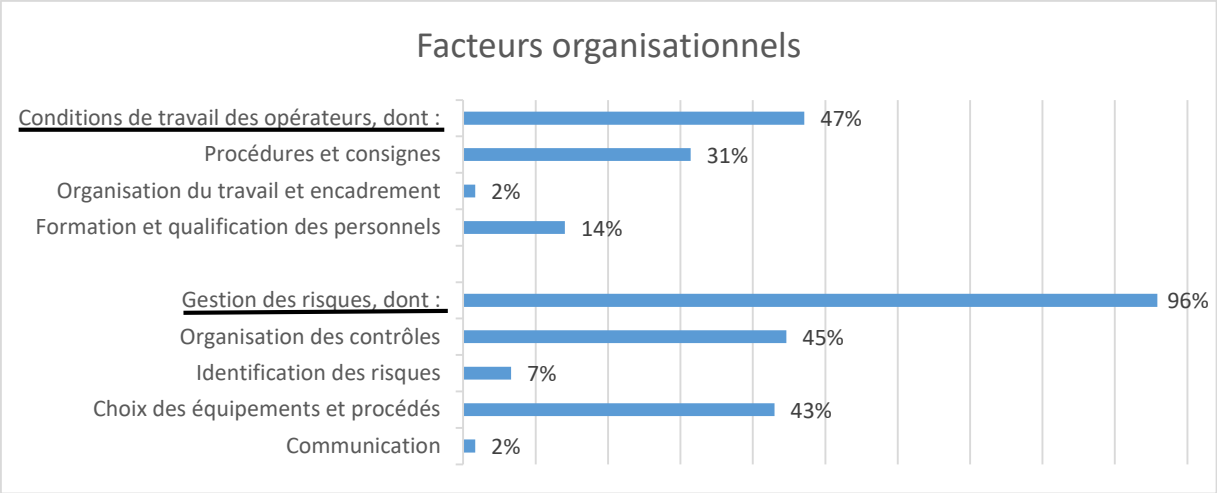
- Éviter que de nouveaux accidents se reproduisent sur un même site ;
- Faire bénéficier l'ensemble des acteurs du risque des enseignements tirés d'un accident en partageant son REX ;
- Identifier efficacement des dysfonctionnements sur un site et y remédier par des mesures adaptées et pas uniquement par des mesures visant à s'attaquer aux symptômes (les perturbations) ;
- Partager avec les autorités une vision plus réaliste de l'organisation relative à la sécurité sur un site industriel. Le Système de Gestion de la Sécurité (SGS), prévoit pour les sites SEVESO, des chapitres traitant de l'organisation des sites en matière de sécurité.
  En revanche, sur les sites soumis à autorisation, les arrêtés préfectoraux ne traitent pas toujours de ces facteurs organisationnels. Quelques chapitres seulement abordent la formation ou les procédures et consignes.

En particulier pour le thème étudié ici, certains accidents ont pour origine une suite de défaillances. Dans ces cas, la recherche des causes profondes s'avère primordiale afin de remonter jusqu'à d'éventuels modes communs et supprimer une cause racine qui pourrait potentiellement engendrer d'autres accidents pas encore survenus.



3- Analyse des causes profondes

Les accidents étudiés ont fait l'objet d'une sélection basée sur leur pertinence vis-à-vis du sujet d'étude. Ils sont, pour la plupart, porteurs d'enseignements au regard des facteurs organisationnels. En effet, comme vu précédemment, nombre de perturbations touchant les actionneurs sont d'origine matérielle. Mais l'analyse ne peut s'en tenir là sinon tous les accidents pourraient être évités sous réserve de la seule fiabilité des équipements. Derrière ces perturbations, il convient d'identifier les dysfonctionnements « racine », appelées « causes » ou « causes profondes » pour éviter leur répétabilité. Ces causes, multiples ou communes suivant les accidents, seront les bases pour mettre en œuvre les actions appropriées pour lutter durablement contre les défaillances premières, d'origine matérielle, humaine ou encore, extérieure au système telles que décrites dans le chapitre précédent.



Les principales causes profondes identifiées peuvent être regroupées dans les 3 catégories suivantes :

- La conception et choix des équipements et matériels (43 %) ;
- L'organisation des contrôles et de la maintenance (45 %) ;
- Les procédures, consignes et formation des opérateurs (45 %).

Le pourcentage est supérieur à 100 % car plusieurs causes profondes ont pu être identifiées pour un accident.

Les causes profondes qui ressortent ensuite dans l'échantillon étudié sont la gestion des modifications et les analyses de risques. Lorsque l'analyse de l'accident est poussée en profondeur, il est mis en évidence une succession de causes profondes, dont les causes racines sont souvent l'organisation du travail ou la communication pour l'échantillon en question.

3-1- Conception et choix des équipements et matériels (43 %)

Dans un premier temps, les problèmes liés à la conception des actionneurs ou aux choix des équipements et matériaux qui ont été faits à l'origine pour les actionneurs et qui n'ont pas été remis en cause au cours de l'exploitation ont été identifiées dans les accidents étudiés :

- Défaut de conception interne de l'actionneur lui-même ; voir exemple perturbations : actionneur non conforme ou matériau de l'actionneur non adapté ;
- Absence d'actionneur automatique : vanne ou pompe non automatisée, système global de mise en sécurité non automatisé, par conséquent une action manuelle était requise mais n'a pas été ou a été mal effectuée (voir interventions humaines en phase d'exploitation) : ARIA 53080 ;
- Système complètement absent : ARIA 47536, 51178 ;

- La fonction remplie par l'actionneur n'est pas pertinente en cas de dérive du procédé : ARIA 52379 ;
- La conception dans la conduite du procédé ne convient pas : ARIA 49983, 41517, 40522 ;
- Problème de seuil de déclenchement de l'actionneur pour les systèmes intégrés type régulation de la pression ou de la température : ARIA 47781 ;
- Absence de redondance : ARIA 40092 ;
- Absence de retour de bon et/ou mauvais fonctionnement en salle de commande : ARIA 32484.

Figure 10: redondance des automates - ©pxhere

3-2- Organisation des contrôles et de la maintenance (45 %)

Ensuite, pour tous les actionneurs qui n'ont pas pu remplir leur fonction du fait d'une panne, d'une perte d'étanchéité ou encore d'un colmatage, les causes profondes sont le plus souvent liées à des défauts de maintenance et ou de contrôles :

- Absence de contrôle : ARIA 49735, 36385, 33626, 50755 ;
- Absence de programme de maintenance préventive : ARIA 42275, 51721 ;
- Maintenance insuffisante : ARIA 48833, 21967 ;
- Contrôle prévu mais non réalisé : ARIA 6343, 51505 ;
- Contrôles insuffisants : ARIA 46555, 50235 ;
- Absence de tests préalables de l'équipement : ARIA 17740 ;
- Test inadapté : ARIA 49752, 50339 ;
- La chaine de mise en sécurité n'a pas été testée dans son ensemble : ARIA 30920 ;
- Absence de suivi des anomalies : ARIA 7069 ;
- Défaut de contrôle suite à l'intervention d'un sous-traitant sur l'équipement : ARIA 36198.

ARIA 45744 (22/09/2014) : Projection d'ammoniaque lors d'une opération de maintenance sur un bain de gravure

Dans une usine fabriquant des circuits imprimés, **les pompes d'alimentations d'un bain de gravure se déclenchent inopinément alors qu'une opération de maintenance est en cours.** Les deux agents en charge de l'inspection visuelle des buses d'injection reçoivent des projections d'ammoniaque et de chlorure d'ammonium.

La machine n'a pas été mise en arrêt complet pour cette opération de maintenance hebdomadaire. Elle était en mode "attente ou chauffe". Ce mode permet à l'automate de commander régulièrement des redémarrages des pompes pour homogénéiser le bain. L'exploitant modifie la procédure d'intervention en précisant l'obligation d'arrêt de la machine au niveau du sectionneur avant l'ouverture du module de gravure.

Concernant la sous-traitance, des erreurs humaines ont pu être mises en évidence dans le paragraphe précédent. Dans la suite de ce document, quelques recommandations seront émises concernant spécifiquement les actions des sous-traitants sur les actionneurs et l'importance de leur suivi. L'analyse complète de l'accidentologie liée aux opérations de sous-traitance est disponible sur le site du BARPI : Sous-traitance et maîtrise des risques.

3-3- Procédures, consignes et formation (45 %)

En parallèle des actions à mener au quotidien par les opérateurs en charge de la conduite du procédé, ou encore de la maintenance et des contrôles des équipements, les procédures et formation associées doivent être mises en œuvre. Celles-ci font parfois défaut, ou ne sont pas suffisamment explicites, pour permettre aux opérateurs de mener les actions appropriées :

- Absence de consignes ou procédures : ARIA 33487, 19596 ;
- Consignes ou procédures inappropriées : ARIA 12671, 27564, 39629 ;
- Manque de clarté des consignes et procédures existantes : ARIA 3536 ;
- Consignes ou procédures non respectées : ARIA 48639, 18563 ;
- Méconnaissance des opérateurs sur le fonctionnement du système automatique : ARIA 2684 ;
- Formation : ARIA 23010.

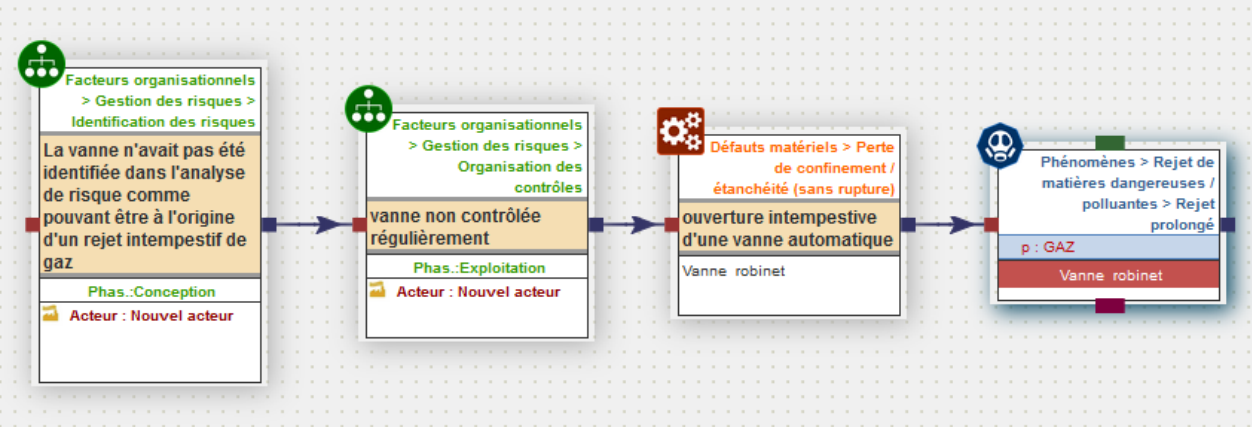
3-4- Gestion des modifications

Les accidents ayant pour origine ou ayant été aggravé par l'action ou la non-action d'un actionneur, peuvent parfois faire suite à des modifications opérées sur les systèmes. L'organisation doit permettre de s'assurer que les équipements sont aptes à remplir leur fonction, notamment lorsqu'ils sont considérés comme des barrières de sécurité. Pour les établissements SEVESO seuil haut, le SGS est un moyen de suivre ces modifications :

- Modifications non prises en compte par les opérateurs ou non intégrées dans le système de conduite ou de sécurité : ARIA 16080 (modification effectuée par un sous-traitant également), ARIA 36599 ;
- Modifications entrainant un montage provisoire : ARIA 30691 ;
- Gestion des modifications sans analyse de risque préalable : ARIA 35863.

3-5- Analyse de risques

Les causes profondes rattachées à l'analyse de risques, vient, le plus fréquemment, en second niveau d'une première cause profonde identifiée. Par exemple, dans la modélisation ci-dessous, le rejet de matière dangereuse est dû à une perturbation matérielle, liée à un défaut de contrôle, du fait d'une lacune d'identification du risque lors de l'analyse.



Parmi l'échantillon étudié, différents accidents illustrent cette situation dont notamment :

- Des équipements qui n'étaient pas intégrés dans l'analyse de risques : ARIA 52784 ;
- Des événements initiateurs non étudiés dans l'analyse de risques : ARIA 38601 ;
- Un scénario non envisagé par le constructeur : ARIA 50490 ;
- Scénario non envisagé par l'exploitant dans son étude de dangers : 35215, 36110, 39898 ;
- Insuffisances de l'analyse de risques : ARIA 21967, 25057, 32484.

Attention à la bonne prise en compte des phases transitoires dans les analyses de risques : elles doivent faire l'objet d'une attention particulière, notamment les modifications impliquant le mode de conduite des installations lors de ces phases : passage en mode manuel alors que normalement l'installation est en mode automatique (cf chapitre interventions humaines lors de ces phases critiques).

3-6- Organisation du travail, répartition des tâches, communication

Comme l'analyse de risques, l'organisation du travail et/ou la communication interviennent dans les accidents, le plus souvent, en 2eme niveau de causes profondes.

Pour remonter à ces causes, l'analyse de l'accident doit être menée de manière approfondie jusqu'à remettre en question certains socles communs d'une organisation en place, comme par exemple :

- La définition des rôles et responsabilités de chacun, pour les opérations de maintenance par exemple : ARIA 31238 ;
- La communication lors des passages de consignes au cours des changements de poste : ARIA 42644, 35863, 46230.

Une fois l'ensemble des causes identifiées, il convient de mettre en œuvre les actions pour y remédier.

Partie 4 : Recommandations

A la suite de l'analyse de l'échantillon d'accidents et de l'identification des perturbations et causes profondes à leur origine, des recommandations peuvent être émises afin d'éviter leur renouvellement. Tout d'abord, des dispositions techniques peuvent agir sur les défaillances matérielles principalement et prévenir des interventions humaines mal effectuées. Comme expliqué précédemment, ces dispositions techniques ne peuvent suffire à l'amélioration en profondeur des systèmes. C'est pourquoi, un ensemble de dispositions organisationnelles seront proposées afin d'agir sur les facteurs du même nom et humains. Ci-dessous, en introduction, un exemple d'accident, relativement ancien, dresse un panel de dispositions techniques accompagnées d'indispensables modifications organisationnelles.

ARIA 3536 (22/04/1992) : Explosion / incendie d'une unité d'eau oxygénée

Une explosion perçue à des dizaines de km et un incendie détruisent 1 000 des 4 000 m² d'une unité d'eau oxygénée (H2O2) proche de réservoirs d'hydrogène et de chlore.

L'accident résulte de la défaillance d'une carte d'alimentation électrique dans l'une des armoires du système de conduite (SNCC) de l'unité. Parmi les éléments aggravant la situation, il est précisé : **automatisation partielle de l'arrêt d'urgence de l'unité**, dispositifs de commande / sécurité non indépendants agissant sur les mêmes organes, **contrôle insuffisant du bon déroulement de la mise en sécurité des installations** couplé à **plusieurs opérations manuelles non réalisées par les opérateurs** pour conforter l'arrêt de l'unité.

Parmi les améliorations techniques prises après ce sinistre, il est à noter **l'amélioration du système de contrôle / commande** : système de sécurité assurant l'arrêt d'urgence indépendant du système de conduite, nouvelle salle de contrôle, amélioration du confort et de **l'ergonomie des postes de travail**. L'exploitant prévoit aussi : la redéfinition des missions des intervenants et l'amélioration de **leur information / formation**, la rédaction de **consignes de sécurité adaptées**, la réalisation **d'études de dangers** pour la fabrication, le transfert et le stockage d'H2O2...

1- Des dispositions techniques

La première recommandation qui ressort de façon récurrente de l'analyse de l'échantillon est l'étude de l'opportunité de la mise en place d'actionneurs automatiques dans les cas où ceux-ci était absents ou dans les cas où une action manuelle était requise à la place.

 Il faut rester vigilant sur cette transformation des systèmes. En effet, elle ne peut se faire sans évaluation préalable de la réalisation technique (conception, emplacement, accès, modification pendant un arrêt technique…) et de l'adéquation (temps de réponse, action répondant au besoin…) de l'actionneur à mettre en place. Pour ces modifications, il est important d'impliquer les experts appropriés :

- Les utilisateurs de l'ancien et du futur système, qui apporteront la connaissance du process dans lequel sera intégré le futur actionneur ;
- Les constructeurs, qui ont une connaissance avancée des différentes technologies développées et qui pourront fournir la meilleure réponse au besoin ;
- Les opérateurs de maintenance pour vérifier la maintenabilité des systèmes dans le temps.

Dans le cadre de l'élaboration des modifications des systèmes automatiques, il est nécessaire de faire au préalable une étude de l'impact de ces changements sur la conduite du procédé, la sécurité, la maintenance… Pour cela, des analyses de risques doivent être menées ou mises à jour si elles existent.

En fonction des modifications, les dispositions organisationnelles liées au système de conduite et/ou de mise en sécurité devront être mises à jour : procédures, formation, conditions de by-pass… (Voir paragraphe suivant).

De l'échantillon étudié, ressortent également de simples modifications de matériel pour répondre d'avantages à la fonction souhaitée, comme par exemple :

- Modification de matériaux utilisés pour l'actionneur : ARIA 39629 ;
- Ajout de deux vannes automatiques tout ou rien : ARIA 7956 ;
- Simplification des systèmes : ARIA 16080 ;
- Changement de la position de sécurité : ARIA 36390 ;

Figure 11: chaine de sécurité électrique de transmission du signal de défaut (ARIA 54305) - ©Exploitant

A la lecture des accidents, il apparait clairement une généralisation des modifications effectuées sur le système en cause vers des systèmes similaires sur l'installation en elle-même ou dans d'autres ateliers, voire d'autres sites. Ce report des mesures prises vers des systèmes équivalents paraît indispensable au non renouvellement d'un accident dans une même unité ou sur un même site. Le partage du REX vers d'autres sites fait ensuite évoluer la sécurité collective.

L'amélioration de la fonction remplie par un actionneur peut également passer par la mise en place de redondances :

- Ajout d'une deuxième chaine complète de sécurité, indépendante de la première : ARIA 2684, 30920, 40379 ;
- Redondance pour l'alimentation de l'actionneur afin d'éviter les pertes d'utilités : ARIA 35841.

La mise en place d'alarmes complémentaires est également un moyen de détecter les défaillances d'actionneur afin d'améliorer la fiabilité des systèmes automatiques :

- Indicateurs de position ou capteurs de fin de course : ARIA 7069, 20941, 32798, 38485 ;
- Report d'alarmes pour signaler le fonctionnement d'un actionneur : ARIA 46555 (pompe) ;
- Alarmes sur les systèmes électriques afin de prévenir les pertes d'utilités : ARIA 36110, 50121 ;
- Alarme de discordances : ARIA 52784 ;
- Mise en place d'un dispositif permettant de voir la position de l'actionneur : ARIA 39362.

En général, les alarmes entrainent ensuite une action manuelle. Par conséquent, elles nécessitent un « traitement de l'information » de la part des opérateurs avant action. Il est donc primordial d'avoir une attention particulière quant à la **gestion des priorités des alarmes**, notamment, soit par le biais de consignes et procédures, ou encore par l'ergonomie et l'organisation des salles de contrôle, et encore la répartition des rôles et responsabilités des opérateurs...

La fiabilité des capteurs de position des actionneurs doit également être vérifiée, ce qui revient à étudier les conclusions du la partie 1/3 de la synthèse de l'accidentologie des automatismes industriels, volet concernant les capteurs : Accidentologie des automatismes industriels partie 1/3 : Le capteur.

2- Des dispositions organisationnelles

Les dispositions organisationnelles sont prépondérantes afin d'éviter les biais liés aux systèmes sur-automatisés : l'homme doit rester maître du système et il est parfois le moyen ultime de rattraper les dérives possibles. Pour cela, il doit avoir à disposition les bons outils, avoir une bonne connaissance du terrain avec des recyclages réguliers, qui s'adressent également aux experts, et une certaine autonomie dans les actions qu'il peut réaliser. Plus le système sera complexe, plus il lui faudra du temps pour analyser une situation et apporter la réponse adéquate.

L'ergonomie des salles de contrôles et la définition des responsabilités sont des moyens pour clarifier les actions à mener suivant les possibles défaillances des actionneurs en jeu dans les systèmes automatisés.

Comme évoqué précédemment, la **conception des systèmes** s'est avérée comme une cause profonde pouvant souvent être à l'origine des défaillances des actionneurs. Les moyens pour y remédier sont par exemple :

- Mener une enquête au niveau du fabricant concernant la conformité et l'efficacité de ces dispositifs de sécurité (fiabilité de la vanne pneumatique) : ARIA 23010 ;
- Réaliser des essais, vérifier si l'actionneur rempli sa fonction dans son contexte d'utilisation : test de l'ensemble de la chaine de sécurité (capteur, automate, actionneur) et en conditions réelles : ARIA 23589 ;

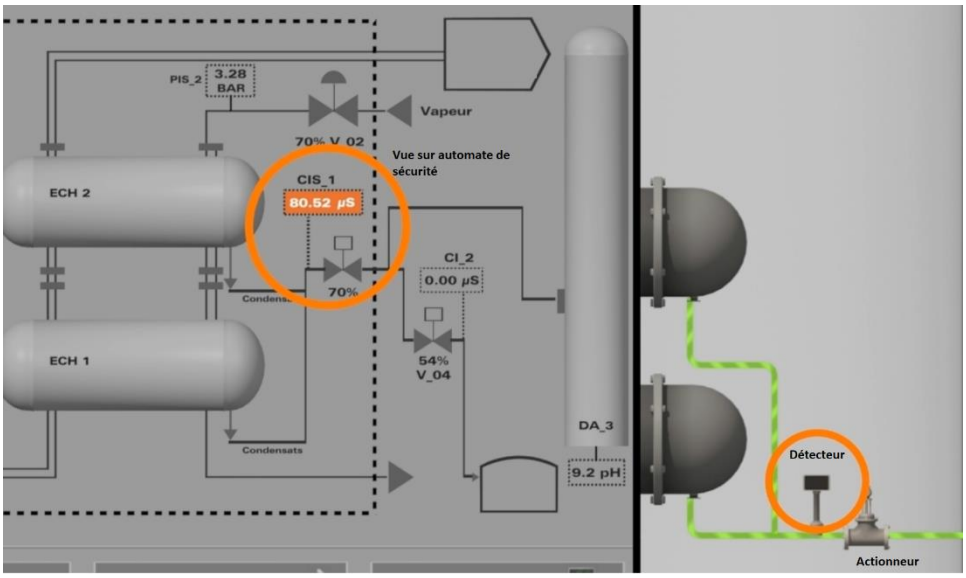


Figure 12: vue d'ensemble d'une chaine de sécurité : capteur, automate, actionneur - ©BARPI

- Modifier la conduite du procédé : ARIA 49983 ;
- Modifier la programmation des automates : ARIA 40522, 47536 ;
- Modifier les asservissements entre actionneur et capteur : ARIA 50490 ;
- Vérifier le temps de réponse des équipements : l'analyse sur l'ensemble d'une chaine permet de vérifier que la réactivité des équipements est en adéquation avec la fonction à remplir : ARIA 41517 ;

- Intégrer la sécurité positive dès la conception et vérifier que l'actionneur agit bien en sécurité positive (exemple : ARIA 36390), sauf si son déclenchement peut générer un nouveau risque et/ou conduire à des pertes d'exploitation et/ou matérielles importantes ; dans le cas où l'appareil ne passe à l'état de sécurité, la perte d'alimentation et l'intégrité du circuit doivent être détectées et signalées et des actions compensatoires doivent être prévues ;
- Vérifier que le concept est bien éprouvé ;
- Vérifier le niveau de sécurité des actionneurs qui sont identifiés comme des barrières de sécurité (certification QUALISIL par exemple pour les établissements Seveso).

En ce qui concerne, l'organisation des **contrôles et de la maintenance**, deuxième ensemble de causes profondes identifié précédemment, son amélioration peut notamment reposer sur :

- Le renforcement des tests périodiques et de la maintenance préventive : ARIA 23629, 26475, 33626, 35533, 48384, 49845 ;
- L'augmentation de la périodicité et du nombre de points de contrôles : ARIA 21960, 37226, 42921 ;
- La qualification ou reconfiguration des équipements avant tout démarrage d'un nouveau batch : ARIA 7069 ;
- Le contrôle des intervenants : ARIA 25248, 50339 ;
- La bonne maîtrise des mises hors service des barrières : ARIA 42163.

De même, l'amélioration des **procédures et consignes et de la formation** doit être faite à tous les niveaux hiérarchiques et impliquer les sous-traitants, comme par exemple :

- Mise en place de check-lists, sensibilisation des opérateurs, encadrement et astreinte encadrement : ARIA 15397 ;
- Sensibilisation des intervenants extérieurs : ARIA 50339 ;
- Recyclage de la formation des chauffeurs : ARIA 49921 ;
- Mise en place d'une action de sensibilisation du personnel sur les risques inhérents à une installation : ARIA 34116 ;
- Révision de la formation pour les titulaires et les nouveaux embauchés et rédaction de fiches réflexes pour indiquer la procédure à suivre en cas de remontée d'alarme critique : ARIA 48639 ;
- Sensibilisation des opérateurs sur le risque et la vigilance indispensable : ARIA 34205 ;
- Pour répondre à la gestion des phases transitoires, la formation du personnel est améliorée quant à la mise hors service temporaire des dispositifs de sécurité : ARIA 32484.

ARIA 42163 (14/05/2012) : Emission accidentelle de phosgène

Vers 23h30, des capteurs extérieurs détectent des concentrations de phosgène. A 23h52, un capteur de pression sur le circuit vapeur atteint quelques dizaines de bars et déclenche l'arrêt de l'unité avec fermeture des vannes d'isolement de l'enceinte de confinement**. Cette fermeture rapide provoque un coup de bélier qui rompt l'une des vannes de purge en pied d'échangeur** ; l'encours de COCl2 se déverse dans l'enceinte, entraînant une perte de dépression et la fermeture de ses clapets de sécurité. Seul le bon fonctionnement de la 2ème barrière de sécurité (capteur de pression et sa chaîne de sécurité, mais aussi enceinte de confinement intégrée) a permis d'éviter le rejet d'une grande quantité de gaz toxique hors de l'usine (habitations à 260 m).

Des procédures sont formalisées ou renforcées :
• **Fiche réflexe** sur la conduite à suivre lors de l'activation des barrières techniques de l'unité ;
• Shunt des barrières techniques de l'unité: sensibilisation des opérateurs et de l'encadrement, définition des rôles et des droits de chacun, **clarification et restriction des conditions de shunt autorisés ;**
• **Conditions d'habilitation des opérateurs** de l'unité sur les aspects sécurité du procédé et inspection des équipements ;
• **Formalisation des échanges d'information** entre équipes de conduite et service d'entretien des équipements.

Piliers de la maîtrise des risques industriels, les analyses de risques font souvent l'objet de mises à jour ou d'approfondissements suite à des accidents impliquant un ou plusieurs actionneurs, comme, par exemple :

- L'actualisation des études de dangers (site soumis) suite à un incident : ARIA 42415 ;
- La réalisation d'HAZOP pour des systèmes complexes : ARIA 34305, 48639 ;
- L'identification préventive des conséquences des défaillances de l'alimentation électrique sur les différentes fonctions de sécurité et définition des fonctions prioritaires à alimenter pour la sécurité : ARIA 13689 ;
- Des réflexions sur le contrôle des ouvertures automatiques des vannes pour vérifier les risques pouvant découler d'une ouverture non contrôlée de ces vannes : ARIA 50424 ;
- L'analyse de risques suivant les différentes conditions de fonctionnement : ARIA 28649.

 La prise en compte des phases transitoires est obligatoire dans les analyses de risques. De plus, certains biais techniques (manque de connaissance des installations par exemple) et/ou économiques (cadrage préalable de l'analyse de risques suivant le temps que les opérateurs ont à y consacrer par exemple) sont à éviter. Comme précisé précédemment, tous les acteurs concernés doivent être impliqués dans les analyses de risques.

Il peut s'en suivre, pour les sites concernés, une modification du système de gestion de la sécurité du site pour tenir compte de l'expérience acquise lors d'un événement : ARIA 35841.

Enfin, de manière très globale, certains accidents mettant en jeu un ou plusieurs actionneurs ont permis de mettre en évidence des actions pour améliorer l'organisation du travail ou encore la communication :

- Amélioration de la communication entre les chefs de ligne et les chefs de poste pour transmettre à l'équipe suivante un bilan exhaustif des problèmes rencontrés : ARIA 46230 ;

- Mise en place d'une liaison complémentaire et directe entre le bureau d'exploitation et les navires arrivant au dépôt par achats de téléphones portables ATEX : ARIA 34205 ;
- Mise en place d'une fiche de passage de consignes et d'un livret de postes : ARIA 42644…

Ne concernant pas uniquement les actionneurs mais étant d'actualités, de nouveaux risques sont à prendre en compte, comme notamment :

- La prévention du vieillissement des installations : ARIA 36722, 41516 ;
- La cybersécurité : face à l'émergence de la programmation et du contrôle à distance (exemple : ARIA 51131), il est important de se poser les bonnes questions. Des pistes de réflexion ont été menées pour les capteurs et les automates, celles-ci peuvent être rappelées pour les actionneurs, elles sont disponibles dans la synthèse sur la Cybersécurité dans l'industrie ;
- La malveillance pouvant atteindre les utilités ;
- Le développement de nouvelles technologies d'actionneurs.

Enseignements tirés (conclusion)

Au terme de l'analyse des 326 accidents de l'étude, certaines leçons peuvent être tirées dans l'objectif d'éviter les accidents répondant à au moins un des 3 critères suivants :

- Un ou plusieurs actionneurs sont à l'origine de l'accident ;
- Un ou plusieurs actionneurs ont aggravé l'accident (par leur non-fonctionnement ou, plus rarement, par leur fonctionnement) ;
- L'absence du (des) actionneur(s) a provoqué ou aggravé un accident (si cette absence est explicitement citée dans l'analyse de l'accident et son installation prévue dans les suites techniques données à l'accident).

Pour les deux premiers points, des perturbations matérielles peuvent être évitées par une attention plus grande dans la conception des systèmes, leur adéquation au process (emplacement, matériau utilisé…), leur maintenabilité dans le temps. Il s'avère essentiel de mobiliser l'ensemble des services au sein des organisations afin d'assurer la fiabilité des automatismes industriels.

Pour le troisième point, l'étude a permis de constater que certains accidents auraient pu être évités si un actionneur automatique était en place à l'endroit voulu. Les actionneurs automatiques, s'ils remplissent correctement leur fonction, permettent de rattraper une dérive d'un système. Lorsque cette dérive peut causer des dommages, ces systèmes assurent alors un maintien en sécurité des installations. Leur mise en place doit donc être étudiée dès que possible tout en préservant la connaissance et la maitrise des installations par les opérateurs. Le niveau d'exigence pour les systèmes assurant une fonction de sécurité doit répondre aux enjeux qu'ils protègent. Les « certifications » des barrières humaines et techniques peuvent s'avérer indispensables dans le cas où elles ont été valorisées dans les études de dangers ayant mené à des plans de protection des populations et/ou de maîtrise de l'urbanisation.

Par ailleurs, afin d'agir en profondeur sur les causes des accidents, les moyens et priorités d'action sur les automatismes industriels doivent faire l'objet d'un engagement de la hiérarchie. L'unique modification matérielle ou le changement de comportement humain ne sont pas suffisants. La gestion des facteurs organisationnels et humains dans son ensemble doit reposer sur une organisation mettant en avant la sécurité. Il convient de la repositionner comme prioritaire par rapport aux contraintes économiques. Les accidents étudiés mettent d'ailleurs en avant les pertes économiques liées aux événements impliquant un ou plusieurs actionneurs. Il est nécessaire de mener une réflexion approfondie sur les process dans leur ensemble, surtout dans un contexte d'automatisation de plus en plus fréquente et de volonté de diminution des contraintes humaines. Il faut garder à l'esprit que l'homme reste une ultime barrière et parfois, un moyen de rattrapage des dérives. Les compétences doivent évoluer avec la technique. La connaissance du terrain et de ses risques doit rester au cœur des préoccupations des décideurs.

Il apparait primordial également de mettre au cœur des actions de prévention, la transmission et le partage du REX. L'amélioration de la sécurité industrielle passe par la diffusion et l'échange de bonnes pratiques. Les nouvelles technologies doivent pouvoir être maitrisées de façon collective afin de ne pas perdre de vue la responsabilité humaine dans leur conception, exploitation, maintenance, démantèlement…

Les trois volets étudiés dans le cadre de l'accidentologie des automatismes industriels ont permis de mettre en évidence un certain nombre de recommandations pour chacune des fonctions prises séparément. Il apparait maintenant cohérent d'étudier ces systèmes dans leur ensemble afin qu'ils assurent leur fonction dans les meilleures conditions.

ACCIDENTS TECHNOLOGIQUES EN LIGNE

Sécurité et transparence sont deux exigences légitimes de notre société. Aussi, depuis juin 2001 le site www.aria.developpement-durable.gouv.fr du Ministère de la Transition écologique et solidaire, propose-t-il aux professionnels et au public des enseignements tirés de l'analyse d'accidents technologiques.
Les principales rubriques du site sont présentées en français et en anglais.
Sous les rubriques générales, l'internaute peut, par exemple, s'informer sur l'action de l'Etat, disposer de larges extraits de la base de données ARIA, découvrir la présentation de l'échelle européenne des accidents, prendre connaissance de l'indice relatif aux matières dangereuses relâchées pour compléter la « communication à chaud » en cas d'accident ou d'incident.
La description des accidents, matière première de toute démarche de retour d'expérience, constitue une part importante des ressources du site : déroulement de l'événement, conséquences, origines, circonstances, causes avérées ou présumées, suites données et enseignements tirés.
Une centaine de fiches techniques détaillées et illustrées présente des accidents sélectionnés pour l'intérêt particulier de leurs enseignements. De nombreuses analyses par thème ou par secteur industriel sont également disponibles. La rubrique consacrée aux recommandations techniques développe différents thèmes : chimie fine, pyrotechnie, traitement de surface, silos, dépôts de pneumatiques, permis de feu, traitement des déchets, manutention...
Une recherche multicritères permet d'accéder à l'information sur des accidents survenus en France ou à l'étranger.
Le site www.aria.developpement-durable.gouv.fr s'enrichit continuellement. Actuellement, près de 50 000 accidents sont en ligne et de nouvelles analyses thématiques verront régulièrement le jour.

Les résumés des événements présentés sont disponibles sur le site :
www.aria.developpement-durable.gouv.fr

Crédit photo couverture : *Arnaud Bouissou, Terra*

Pour toute remarque / suggestion, pour signaler un accident ou pour obtenir l'autorisation d'utiliser ces données en vue d'une publication:
barpi@developpement-durable.gouv.fr

Bureau d'analyse des risques et pollutions industriels
5 place Jules Ferry
69006 Lyon
Téléphone : 04 26 28 62 00

Service des risques technologiques
Service des risques naturels et hydrauliques
Direction générale de la Prévention des risques
Ministère de la Transition écologique et solidaire
Tour Sequoia
92055 La Défense cedex
Téléphone : 01 40 81 21 22

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE