ACCIDENTOLOGIE DES AUTOMATISMES INDUSTRIELS
PARTIE 2/3

LA FONCTION TRAITEMENT

DE L'ÉCRAN ... À L'ACCIDENT

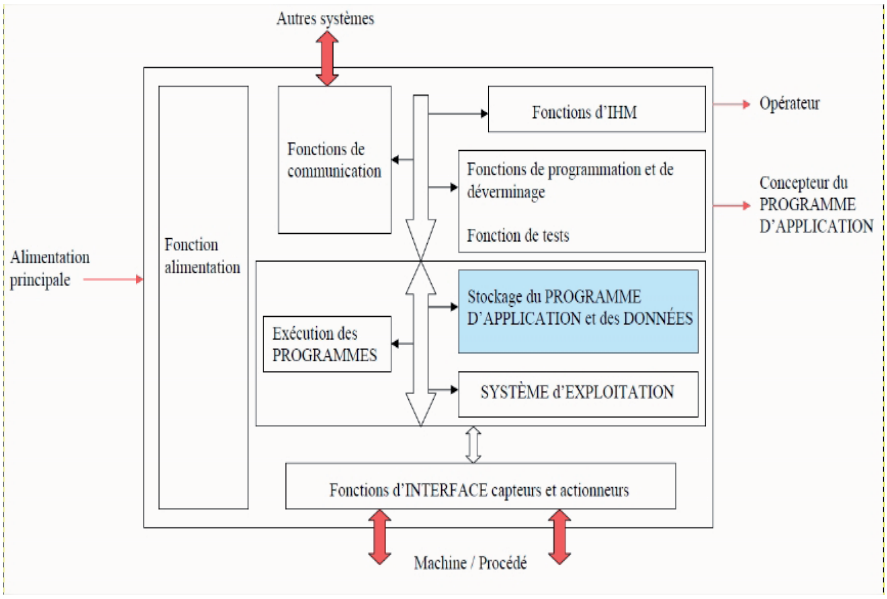
ARIA
dgpr srt barpi

SOMMAIRE

Illustration de la page de garde : Salle de contrôle d'une unité automatisée de chimie fine (source : PAS, Inc.)

Méthodologie de la synthèse

Deuxième volet d'un tryptique consacré à l'accidentologie des automatismes industriels, la présente synthèse analyse les dysfonctionnements de la fonction traitement d'un automate industriel vue dans son ensemble : les différentes composantes techniques de l'unité centrale (alimentation, transmission, cartes électroniques, programme, interfaces homme-machine...), mais aussi la composante humaine qui joue un rôle fondamental dans la conduite des procédés automatisés depuis une salle de contrôle.



Architecture de la fonction traitement d'un automate industriel (source : SURLOG S.A.)

Cette synthèse s'appuie sur un échantillon d'accidents industriels français répertoriés dans la base de données ARIA jusqu'au 31/12/2012 dont le niveau d'information est suffisant pour permettre une bonne compréhension de l'événement (circonstances, conséquences, causes). Une recherche par mots-clefs liés à la fonction traitement des automates industriels (synonymes, dérivés), suivie d'une analyse des résumés des accident, a permis d'affiner cet échantillon en ne retenant que les événements répondant à au moins un des 3 critères suivants :

- la fonction traitement d'un automate de procédé est à l'origine de l'accident ;
- la fonction traitement d'un automate de procédé ou de sécurité a aggravé l'accident ;
- l'absence de la fonction traitement / centralisation des données d'un automate industriel a provoqué ou aggravé un accident, dans la mesure où cette absence est explicitement citée dans l'analyse de l'accident et son installation prévue dans les suites techniques données.

L'échantillon secondaire obtenu regroupe 325 cas, en incluant les accidents provoqués ou aggravés par une défaillance de la supervision humaine pour les unités de production conduites à distance, les actions de conduite et de supervision humaines étant considérées comme parties intégrantes de la fonction de « traitement » d'un automate industriel.

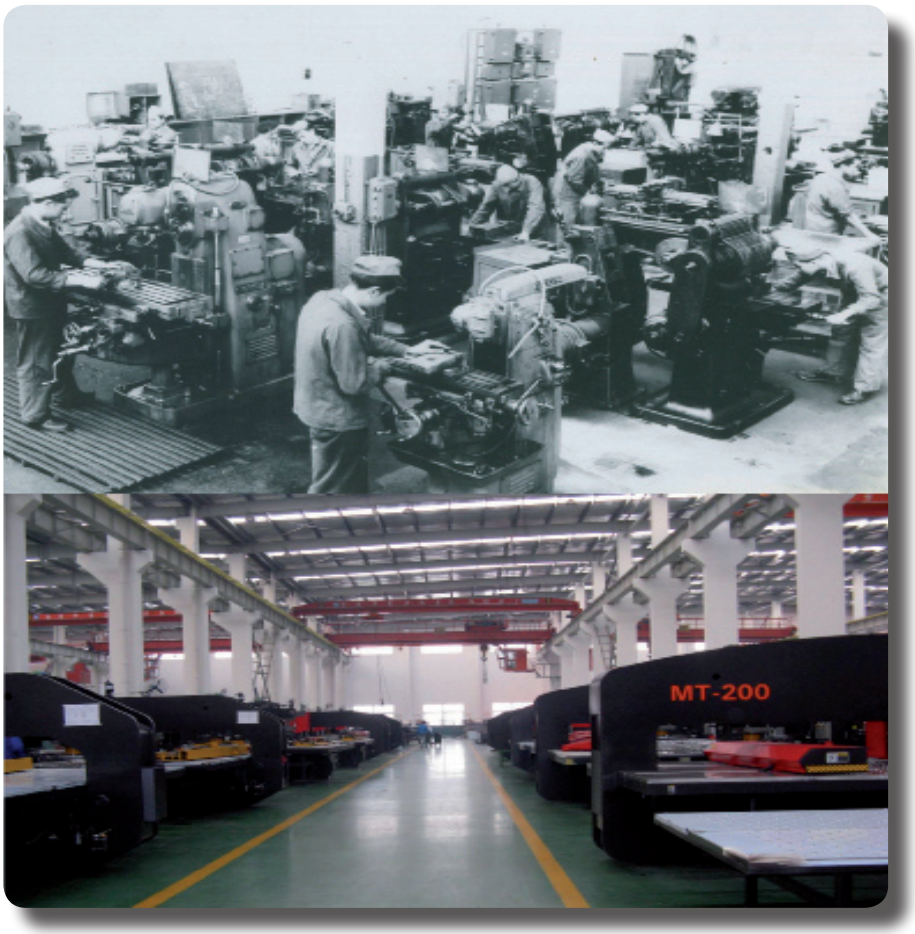
Enfin, la base ARIA étant une base événementielle et non fiabiliste (telles que les bases OREDA, PERD, IEEE, EXIDA...), les données collectées et les résumés d'accident ne donnent pas toujours d'informations précises sur le niveau de criticité ou la cause technique de la défaillance du module de traitement d'un automate, sa technologie... Il est également possible qu'un biais soit introduit entre les secteurs d'activités étudiés, la remontée d'informations sur les accidents pouvant varier fortement d'un secteur à un autre en raison du nombre d'installations en activité en France (beaucoup plus réduit pour le raffinage que pour la chimie par exemple), 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).

1. La fonction traitement des automates industriels

L'examen des données fiabilistes existantes, comme celles de la base OREDA, montre que la partie matérielle de la fonction traitement des automates industriels est rarement une source de défaillance (8 % des défaillances matérielles enregistrées entre 1981 et 2009 dans les installations de 10 groupes pétroliers internationaux). Toutefois, et contrairement aux capteurs dont l'accidentologie a été étudiée dans une synthèse précédente [1], cette fonction fait encore largement appel à l'homme au travers de salles de contrôles et d'écrans de visualisation toujours plus présents dans les sites industriels. C'est là un premier paradoxe découvert au début des années 1980 [2] car beaucoup prédisaient, dès la 2ème moitié du XXème siècle, la disparition de l'homme dans les usines, remplacé par la machine selon le concept de « l'usine sans lumière ». Si ces prédictions avaient bien pris en compte l'extraordinaire rendement des automates et leur percée dans la conduite des procédés, l'accidentologie étudiée montre que le postulat de la disparition du facteur humain comme source d'accident, entraînant une réduction des accidents industriels, s'est révélé largement infondé.

« Dans l'usine du futur, il n'y aura que 2 employés : un homme et un chien. L'homme sera là pour nourrir le chien. Le chien sera là pour empêcher l'homme de toucher aux machines. »

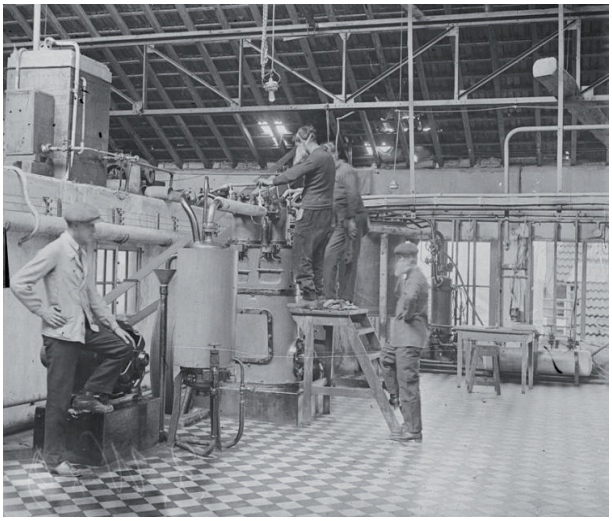
Warren G. Benis, consultant nord américain,1996



Exemple d'automatisation des usines entre les années 1950 et 2000

Un deuxième paradoxe est apparu avec l'automatisation croissante des usines : le facteur humain n'a pas disparu mais s'est déplacé. Plus le niveau d'automatisation augmente, plus le rôle de l'opérateur devient critique en passant de simple exécutant (ouvrir ou fermer des vannes, régler une machine...) à celui de superviseur d'un procédé plus ou moins sophistiqué.

En tant que cause accidentelle, le facteur humain va donner lieu à des erreurs plus complexes susceptibles de faire intervenir l'état physique et mental de l'opérateur, son degré de perception de l'état du procédé (concept de *situation awareness*) et l'ergonomie de son poste de travail. Il en découle naturellement des causes accidentelles profondes liées à des facteurs organisationnels tels que la formation, la répartition des tâches, la spécification et la programmation de l'automate. Ces constats se vérifient aussi hors de l'industrie dans des domaines devenus fortement automatisés comme le transport aérien ou maritime. Une abondante littérature confirme cette prééminence des facteurs humains et organisationnels dans les accidents industriels liés au traitement des informations délivrées par un système automatisé, et plus largement dans l'ensemble des accidents technologiques [3].



Réacteur dans une usine chimique française en 1917 : son chargement et sa surveillance nécessitent la présence rapprochée des opérateurs

Réacteur dans une usine chimique française moderne : son chargement et la surveillance sont pilotés à distance depuis une salle de contrôle

Face à cette situation, les exploitants de sites industriels ont été conduits à repenser en profondeur les critères de recrutement, ainsi que l'organisation du travail et des tâches. De nouveaux défis sont apparus et continuent à apparaître pour réduire dans les usines une accidentologie certes moins quantitative, mais potentiellement plus grave, se situant au niveau de l'interaction de l'homme et de la machine et ne se réduisant plus aux seuls aspects techniques. Grâce à son jugement, son expérience, mais aussi ses capacités d'adaptation et de perception, l'homme reste plus que jamais au cœur de l'efficacité et de la sûreté des procédés automatisés. L'opérateur pouvant détecter des situations à risques qu'un automate ne détectera probablement jamais, un juste équilibre doit être trouvé dans l'automatisation d'un procédé pour lui permettre de rester un élément central de cette efficacité et de cette sécurité.

« Comment un groupe d'opérateurs bien intentionnés, très motivés et apparemment compétents peut-il commettre un tel ensemble d'erreurs et de violations de consignes ? ».

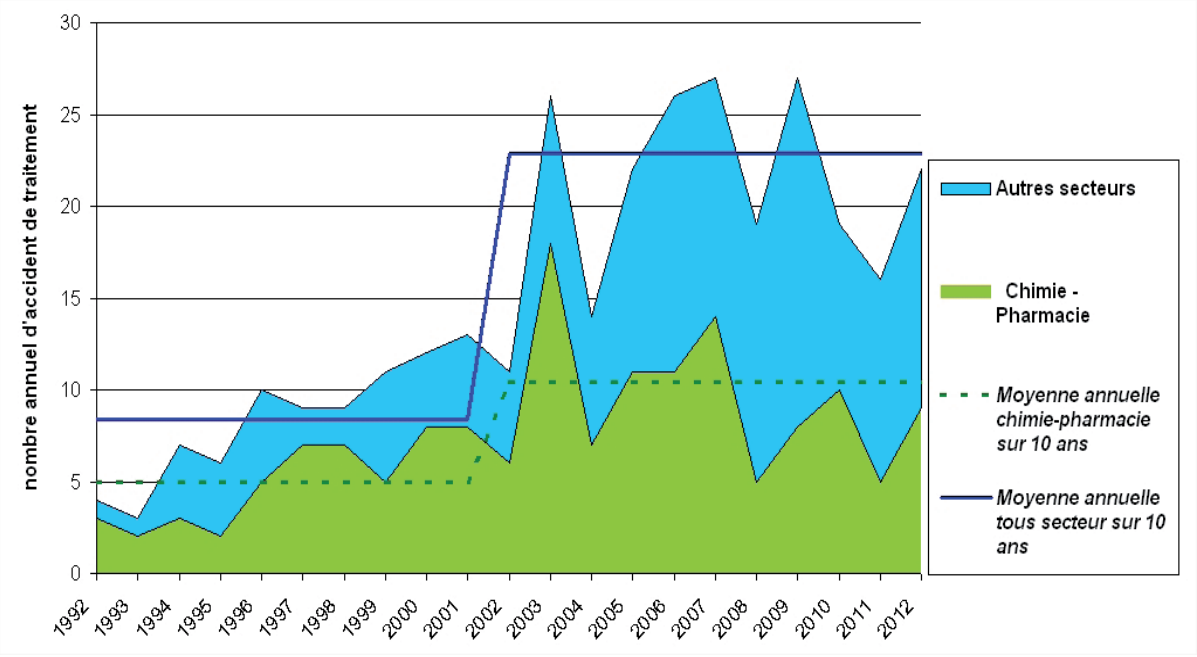
James Reason, psychologue expert en facteurs humains, 1987 (à propos de l'accident de Tchernobyl)

1.1 Données générales

Si l'impact sur l'emploi de l'automatisation des usines a soulevé de nombreuses critiques, peu de personnes contestent aujourd'hui son apport pour la sécurité des travailleurs et des procédés. L'opérateur, éloigné des matières et installations dangereuses, peut cependant accéder rapidement à tous les paramètres de contrôle ; les automates surveillant en permanence et en temps réel des centaines de paramètres et réagissant souvent plus rapidement en cas de dérives ou de situations accidentelles (voir des exemples d'accidents qui auraient pu être évités par un automate page 7). L'influence de la réglementation ou des normes qualités, ainsi que les pressions sociétales pour améliorer la sécurité des sites industriels, ont aussi conduit les exploitants à généraliser l'automatisation pour réduire la composante facteur humain dans les accidents ou les non-conformités. Enfin, du point de vue industriel, l'investissement dans une barrière technique comme l'automatisation est encouragé par sa réputation de grande fiabilité, alors que l'investissement dans la gestion du facteur humain (formation, organisation, ergonomie) peut sembler plus aléatoire et complexe à gérer.

L'analyse de l'échantillon d'accidents retenu confirme que les composants matériels de la fonction traitement sont globalement fiables : 1 % des accidents industriels d'installations fixes sur la période 1992-2012 impliquent cette fonction, alors que la fonction « capteur » représente à elle seule 3 % des accidents de la période 1992-2011 [1]. La revue *Mesure* confirmait en 2009 les conclusions des grandes bases fiabilistes : moins de 10 % des défaillances dangereuses des systèmes automatisés sont dues aux composants matériels de la fonction traitement, les autres étant dues aux actionneurs et aux capteurs [4].

Figure 1 *Nombre annuel d'accidents impliquant la fonction traitement*

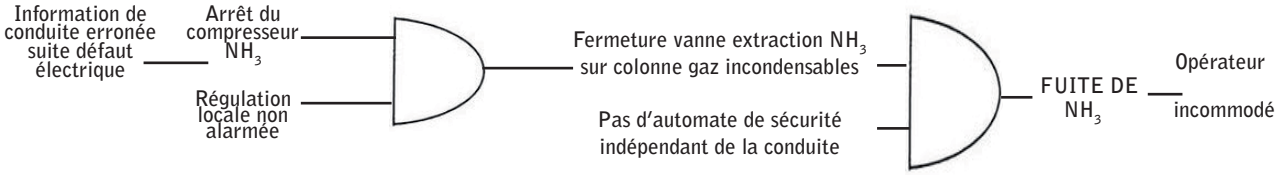


La répartition de ces accidents dans le temps (fig. 1) fait apparaître que leur nombre moyen a triplé entre 1992-2001 et 2002-2012. La généralisation de la centralisation des donnée de conduite des procédés industriels depuis le début des années 2000, grâce à l'apparition d'équipements informatiques et de réseaux de communication plus performants et moins coûteux, peut expliquer ce résultat. Une étude menée en 2002 par le *Health and Safety Executive* sur un pannel de 107 grands sites industriels anglais montrait que 81 % des sites disposaient déjà d'une conduite automatisée à distance de leurs procédés [5]. L'analyse des cas retenus permet aussi de constater que l'accident est survenu ou a été aggravé par l'absence d'un automate dans 16 % des cas (50 accidents depuis 1992). Des exemples d'accident de ce type sont présentés en page 7.

INDUSTRIE MANUFACTURIÈRE ÉQUIPEMENT INSUFFISANT (ARIA 42730) 10/09/2012

Dans une usine de panneaux de bois, un opérateur intervient vers 1 h sur une chaudière de fluide caloporteur destiné à chauffer des presses. Le vase d'expansion d'huile thermique à 274°C est plein à 72 % alors que la consigne de travail précise un taux compris entre 40 et 50 %. L'opérateur vidange une partie du vase d'expansion dans un réservoir qui contient de l'huile à 60°C. Après avoir déversé 2,5 m³ de produit, l'opérateur appelle la salle de commande qui lui confirme que la vidange peut être arrêtée. Alors qu'il s'apprête à redescendre dans la rétention en tournant le dos à la cuve, des vapeurs chaudes d'huile s'enflamment et le brûlent gravement aux membres inférieurs, au cou et au visage. Il portait ses EPI. Les vapeurs provenant d'un évent coudé du réservoir sont retombées dans la rétention. Une traînée de feu se propage du fond de la cuve au local des pompes de circulation puis s'éteint d'elle-même. Le chef d'équipe alerte les secours, un SST prend en charge la victime. Les circuits de fluide thermique sont vidangés suivant la procédure d'urgence. Le blessé est héliporté dans un service spécialisé. L'exploitant modifie l'évent du réservoir en ajoutant une évacuation en toiture, **installe un capteur d'hydrocarbures et une extraction d'air dans la rétention ainsi qu'une caméra pour éviter aux opérateurs de descendre dans la cuve lors des contrôles visuels. La motorisation ou la commande à distance des vannes est envisagée.**

CHIMIE - ÉQUIPEMENT INSUFFISANT (ARIA 28776) 01/08/1997



Dans une unité de production d'ammoniac (NH_3), une fuite d'ammoniac liquéfié se produit sur une colonne utilisée pour éliminer les gaz résiduels incondensables (argon, méthane...) dissous dans l'ammoniac. Incommodé par l'odeur, l'opérateur en salle de contrôle donne l'alerte. Une vanne manuelle est fermée et un rideau d'eau est mis en place autour de la flaque d'ammoniac pour limiter la propagation du nuage d'aérosol. Une défaillance électrique est à l'origine de l'accident : l'information erronée d'arrêt du compresseur d'ammoniac provoque la fermeture de la vanne d'extraction de l'ammoniaque liquide sur la colonne. Celle-ci s'est donc remplie et le système de régulation local d'évacuation des gaz incondensables a laissé échapper l'ammoniaque liquide. L'installation est modifiée pour améliorer la sécurité : remplacement du système de régulation local du niveau de la colonne **par un dispositif centralisé avec alarme** permettant un diagnostic plus rapide, **remplacement du système d'information sur la marche du compresseur par un automatisme de sécurité indépendant de l'automate de conduite,** amélioration du confinement de la salle de contrôle...

VOIR AUSSI

automate absent : Aria 24436, 25156, 26430, 28745, 34410, 38674 / automate insuffisant : Aria 2137, 19964, 26430, 30323, 31367, 32841

RAFFINAGE - ÉQUIPEMENT INSUFFISANT (ARIA 34351) 16/03/2008

Lors du chargement de 31 000 m³ de fioul de soute dans un navire, une fuite sur une canalisation de transfert d'une raffinerie occasionne un important épandage dans l'estuaire de la Loire. A 16h10, une personne sur une barge constate la présence d'hydrocarbures à la surface de l'eau et donne l'alerte. Vers 16h45, un rondier localise et isole la fuite située à 500 m en amont du lieu de détection. Le POI est déclenché à 17 h et l'inspection des installations classées est prévenue. Un navire récupérateur est positionné à l'embouchure du fleuve et 2 chalutiers collectent les boulettes d'hydrocarbures dans l'estuaire. L'exploitant envoie un communiqué de presse et annonce la prise en charge des dommages, des coûts de dépollution et l'indemnisation des professionnels touchés pour un montant de 50 Meuros. La fuite n'a été décelée qu'après 5 heures de délai ; 478 t de fioul se sont déversées, dont 180 t dans la Loire. Plusieurs actions et mesures complémentaires sont demandées à l'exploitant, dont **une surveillance permanente avec dispositif de détection de fuite et report d'alarme en salle de contrôle pour les canalisations proches du fleuve...**

VOIR AUSSI

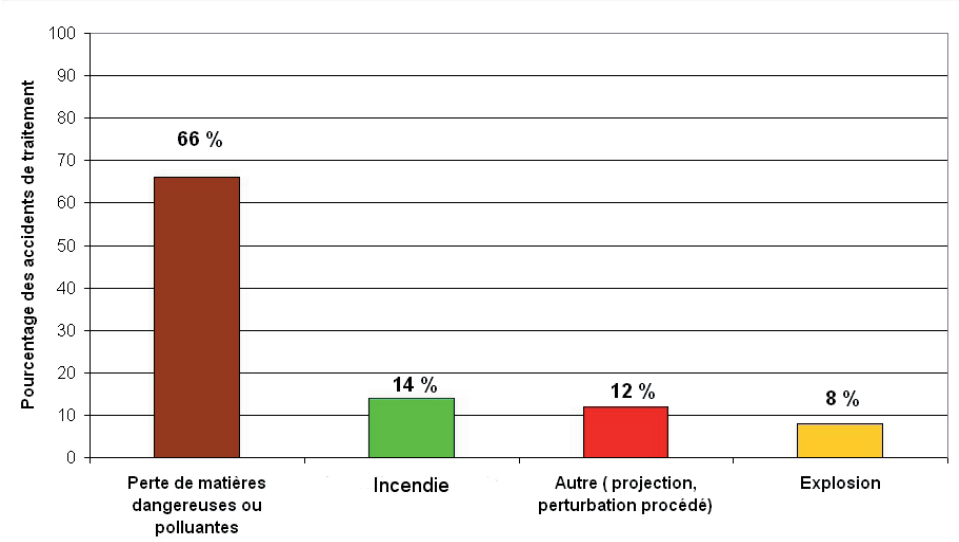
automate absent : Aria 10131 / automate insuffisant : Aria 26186, 29903, 31441

1.2 Accidentologie détaillée

1.2.1 Types d'événements

Les accidents provoqués ou aggravés par une défaillance de la fonction traitement ont une typologie semblable à celle des accidents de capteurs [1] : Les rejets de matières dangereuses prédominent, loin devant les incendies et les explosions (fig. 2).

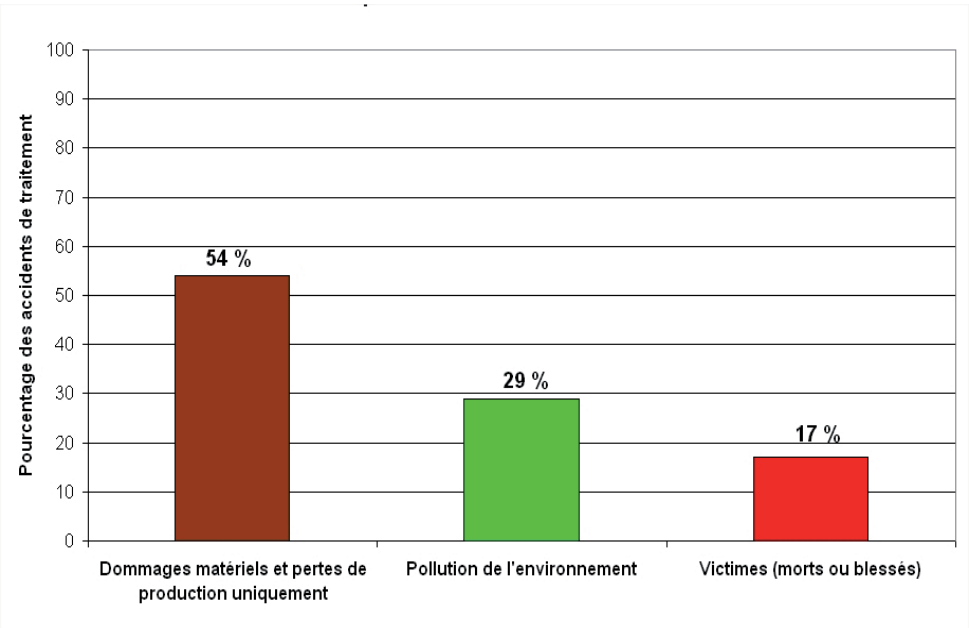
Figure 2 *Répartition des accidents de traitement par type d'événement*



1.2.2 Conséquences des accidents

Si une majorité des accidents étudiés a des conséquences uniquement économiques, près de 3 accidents sur 10 sont à l'origine d'une pollution de l'environnement (fig. 3), résultant de la fréquence des pertes de matières dangereuses ou polluantes. Les victimes sont le plus souvent des employés se trouvant à proximité de l'unité accidentée (voir ARIA 28776 page 7 et ARIA 32640 page 25 par exemple).

Figure 3 *Répartition des accidents de traitement par conséquence principale*

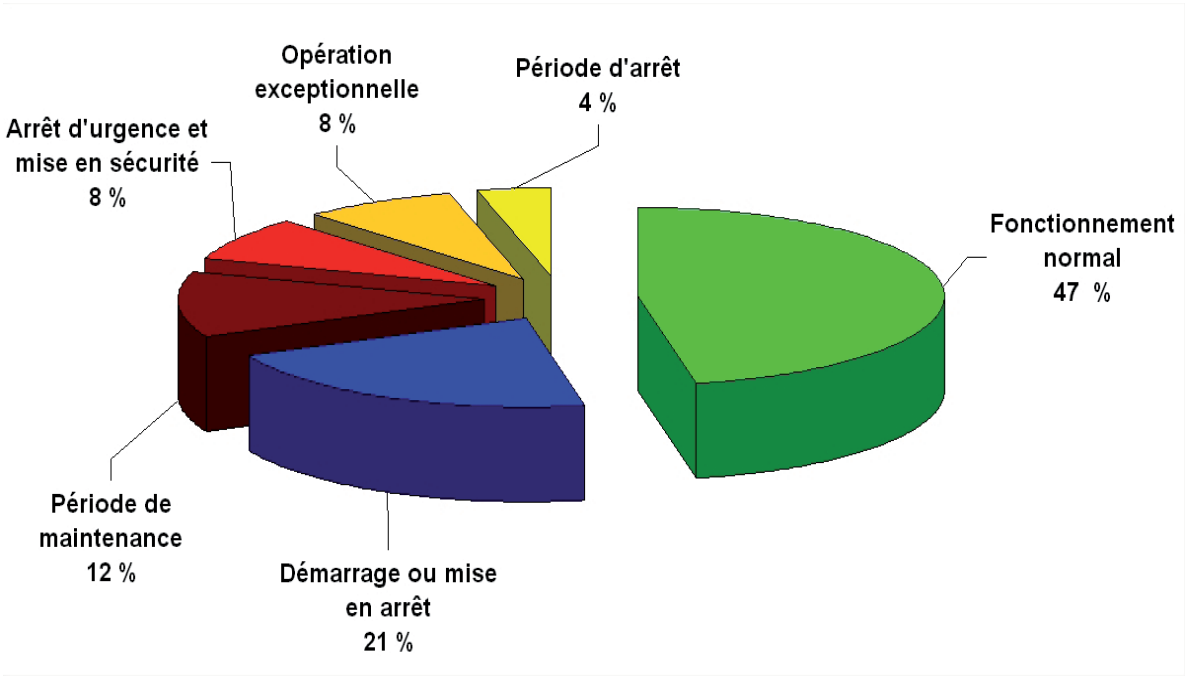


1.2.3 Circonstances des accidents

L'examen des circonstances des accidents de traitement (fig. 4) révèle une prédominance de leur survenue en dehors des phases normales de fonctionnement. Se pose alors la question de l'adaptation matérielle de la fonction traitement aux phases de fonctionnement inhabituelles, telles que les périodes d'entretien, les redémarrages, mais aussi celle de la présence et de la réaction des opérateurs lors de ces phases (voir chapitre 2.2).

Plus de la moitié des accidents impliquant la fonction traitement surviennent en dehors des phases normales de fonctionnement.

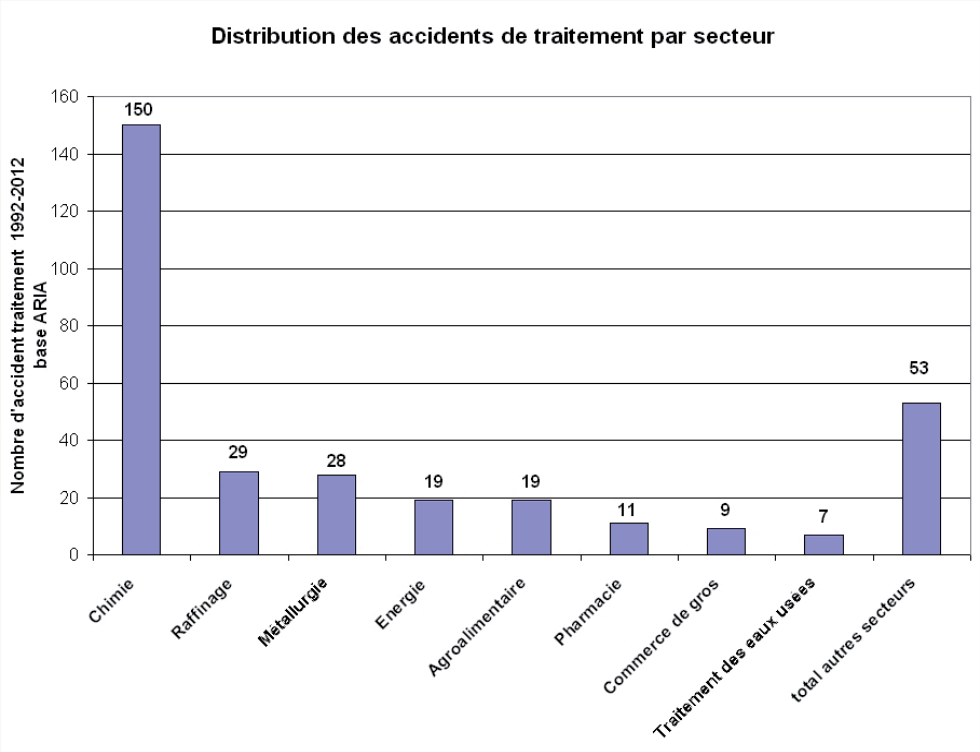
Figure 4 *Répartition des accidents de traitement par circonstances*



1.2.4 Secteurs d'activité concernés

Huit secteurs d'activité se distinguent dans l'échantillon d'accidents étudié avec plus de 6 cas enregistrés (fig. 5). La chimie est en tête avec plus de 54 % des accidents recensés (150 cas). Ce résultat s'explique par un fort taux d'automatisation des procédés chimiques, par leur diversité et par le nombre élevé de sites de production en France, ce secteur étant aussi le plus représenté de manière générale dans la base ARIA (12 % des accidents d'installations classées entre 1992 et 2012). De nombreuses installations sont polyvalentes pour fabriquer des produits divers, ce qui favorise la survenue de situations accidentelles non prévues lors de la conception du système automatisé ou résultant de décisions de conduite erronées. Dans ce secteur, une meilleure intégration de la fonction traitement aurait permis d'éviter ou de réduire l'accidentologie dans 21 % des cas, taux légèrement supérieur au taux moyen de l'ensemble des secteurs (16 %). Un accident de ce type est présenté au milieu de la page 7.

Figure 5 *Répartition des accidents de traitement par secteur d'activité*



A contrario, le secteur du raffinage est nettement moins représenté que celui de la chimie dans l'échantillon d'accidents, malgré un taux d'automatisation important : il occupe malgré tout la 2ème position avec 11 % des cas tout en ne représentant que 2,1 % de l'ensemble des accidents de la base ARIA. Les volumes de produits et de matières premières manipulés, ainsi que l'usage de procédés continus faisant appel à de nombreux équipements se prêtent particulièrement bien à l'automatisation des procédés et à la conduite centralisée des unités, ce qui peut expliquer ce constat. De plus, contrairement à la chimie, les installations de raffinage sont en nombre limité (un maximum de13 sites en activité en France sur la période étudiée) et les procédés de raffinage paraissent aussi plus standardisés. Cet état de fait laisse moins de place aux situations inhabituelles pour les automatismes en période de fonctionnement normal.

La chimie représente 54 % des accidents « traitement » de l'échantillon, le raffinage 11 %, les autres secteurs 10 % ou moins chacun.

La métallurgie arrive en 3ème position avec 10 % des accidents de traitement, bien que cette activité ne représente que 3,5 % de l'ensemble des accidents de la base. Les procédés sont là encore relativement homogènes d'un site à l'autre.

Le secteur de l'énergie (centrales thermiques et hydroélectriques) est le 4ème le plus concerné (7 %) du fait d'un niveau d'automatisation important et d'une conduite fortement centralisée : contrôle à distance des turbines et chaudières, pilotage des stockages...

Enfin, le secteur de l'agroalimentaire arrive également en 4ème position (7 %). Bien que moins automatisé que l'industrie lourde, il comprend de nombreux sites répartis sur le territoire national et met en œuvre des procédés très diversifiés qui utilisent fréquemment des matières dangereuses ou polluantes comme l'ammoniac pour la réfrigération, les hydrocarbures pour le chauffage et la cuisson... et rejette des effluents organiques potentiellement polluants. Les autres secteurs industriels suivis dans la base ARIA représentent chacun moins de 4 % des accidents de traitement recensés et ensemble moins du tiers du total des cas.

1.2.5 Composants impliqués

L'examen des 275 accidents impliquant des défaillances de composants de la fonction traitement fait apparaître l'implication de la partie matérielle (calculateur, carte électronique) dans 49 % des accidents, puis celle des interfaces homme machine (IHM) dans 41 % des cas. Les composants liés à la transmission au sein de l'automate (bus de données, relais) sont impliqués dans 14 % des cas. Ces résultats traduisent l'importance du rôle de la supervision centralisée des procédés (voir chapitre 2.2) et la criticité des pannes des composants matériels de la fonction traitement.

Chaîne automatisée d'embouteillage de gaz industriels (source : Emerson Process)

1.2.6 Fonctions de conduite et de sécurité

Les traitements automatisés liés à la conduite sont impliqués dans 80 % des cas contre 25 % pour ceux dédiés à la sécurité, plusieurs accidents impliquant les 2 fonctions à la fois quand l'automate assure ces fonctions simultanément. Par contre, les accidents de traitement liés à un manque d'intégration de la fonction traitement impliquent presque à parts égales traitements de procédés (53 %) et traitements de sécurité (47 %). Cet équilibre se retrouve surtout dans le secteur de la chimie.

80 % des accidents de traitement impliquent une fonction de conduite des procédés et 25 % une fonction de sécurité. Pour le secteur de la chimie, les accidents liés à un niveau d'intégration insuffisant de la fonction traitement concernent à parts égales la conduite et la sécurité.

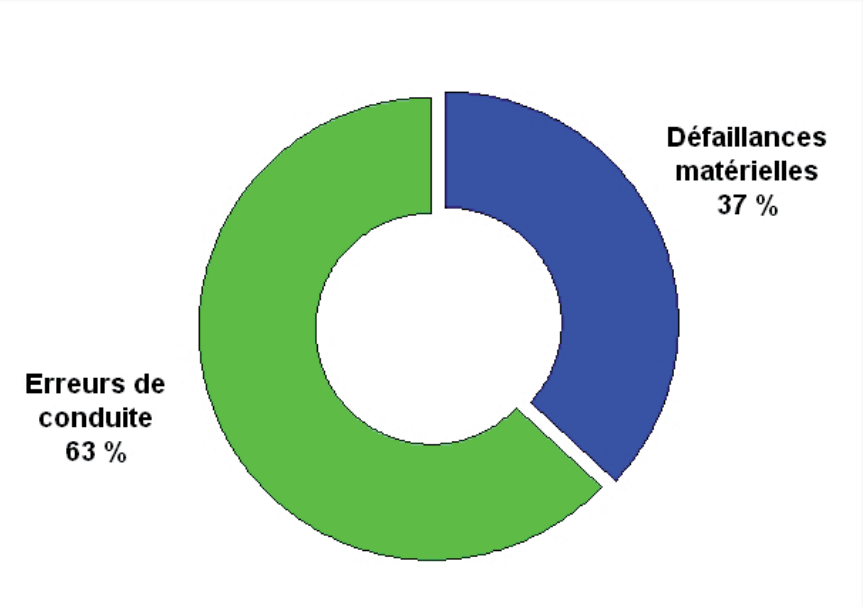
2. Analyse des causes premières des accidents

Ce chapitre analyse plus précisément les causes dites « premières » des défaillances de la fonction traitement. Il s'agit des causes immédiates ou encore des « symptômes visibles » de l'accident qui apparaissent en première analyse. Pour mémoire, 85 % des accidents de traitement analysés, soit 275 cas, relèvent d'une défaillance de cette fonction tandis que 15 % (50 cas) relèvent d'un niveau d'intégration ou d'équipement insuffisant. Ces causes se partagent en 2 catégories :

- **Les défaillances matérielles :** elles recouvrent les accidents où une panne / un dysfonctionnement d'un composant matériel / logiciel de la fonction traitement est à l'origine de l'accident ou de son aggravation. Pour ces accidents, au moins un composant matériel ou logiciel de la fonction traitement n'a pas fonctionné comme prévu. Le chapitre 3 développe les causes profondes de ces accidents, qui relèvent aussi bien de problématiques organisationnelles que de facteurs externes aux installations.

- **Les erreurs de conduite ou de supervision :** cette catégorie ne concerne que les procédés automatisés conduits ou supervisés à distance, et où au moins une erreur de l'opérateur chargé de traiter les informations remontées par l'automate en salle de contrôle de l'unité ou de l'usine est à l'origine de l'accident ou de son aggravation. Le chapitre 3 détaille les causes profondes de ces accidents, presque exclusivement organisationnelles.

Figure 6 *Les causes premières des accidents de la fonction traitement*



La figure 6 montre une prédominance des erreurs de conduite sur les défaillances matérielles des composants. Ce résultat confirme l'importance croissante des systèmes automatisés de conduite à distance dans les sites industriels [5], mais aussi que le dysfonctionnement matériel d'un composant de la chaîne de traitement reste encore une source non négligeable d'accident.

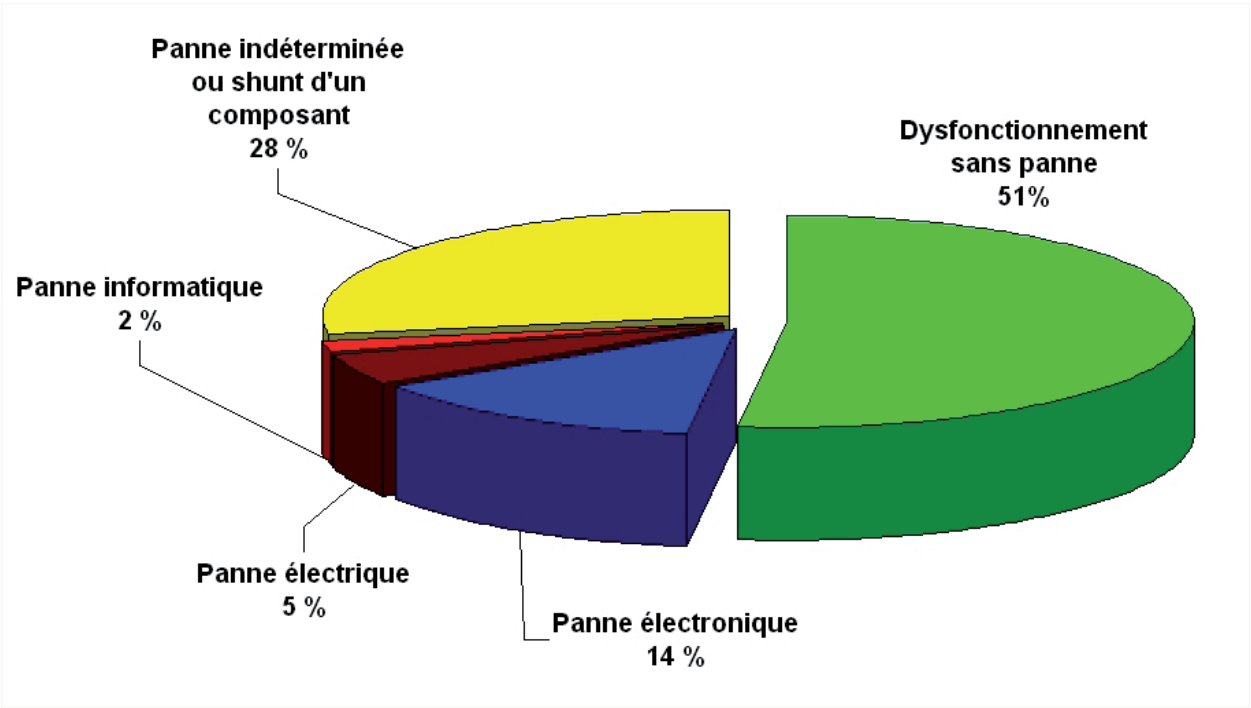
Les causes directes des accidents impliquant la fonction traitement sont aux 2/3 liées à des erreurs de conduite, les défaillances de composants « hardware » ou « software » représentant 1/3 des accidents répertoriés.

2.1 Les défaillances matérielles

Les défaillances matérielles représentent la première cause directe des défaillance de la fonction traitement (102 cas). Si cette fonction est moins exposée aux environnements des procédés que les capteurs et les actionneurs (risques d'encrassement, de corrosion et de blocage mécanique), elle est fortement dépendante de la programmation des automates, qui peut engendrer des dysfonctionnements sans que l'automate tombe franchement en panne. Ces facteurs expliquent l'importance des dysfonctionnements sans panne dans la répartition des défaillances matérielles (fig.7).

Ce constat montre aussi que la détection de tels dysfonctionnements peut être difficile pour les opérateurs d'un système automatisé, d'où l'importance de leur formation et entraînement. De plus, les potentialités de pannes matérielles des différents équipements se cumulent : cartes électroniques, relais de communication, câblage, alimentation électriques, écrans d'affichage, unités centrales, systèmes d'avertissement sonore, etc.(voir les accidents illustratifs page 14).

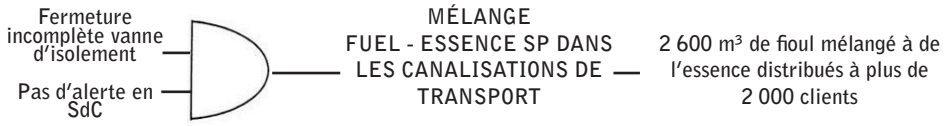
Figure 7 *Les types de défaillances matérielles de la fonction traitement*



Les dysfonctionnements sans panne franche représentent plus de la moitié des défaillances matérielles de la fonction traitement.

Certain de ces équipements présentent d'ailleurs des vulnérabilités similaires aux capteurs, comme le shunt ou la perte d'alimentation électrique. Leur technologie les expose enfin plus particulièrement aux pannes électroniques, source de 14 % des défaillances matérielles de cette fonction.

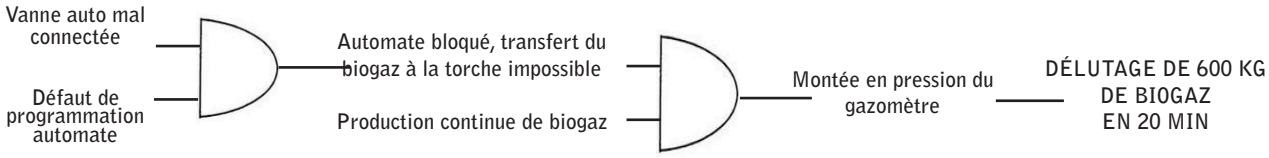
DYSFONCTIONNEMENT (ARIA 35774) 15/01/2009



Dans la nuit, 4 900 m³ de fioul domestique non conforme (contenant 17 % d'essence sans-plomb) sont livrés par une raffinerie à une société réalisant du stockage en vrac («stockeur») puis partiellement distribués les jours suivants à plusieurs milliers de consommateurs via des entreprises de distribution de 11 départements du nord-ouest de la France. Le mélange fioul-essence sans plomb ainsi constitué à un point éclair de 22°C (contre 55°C pour du fioul « pur »), le rendant facilement inflammable et susceptible de former une atmosphère explosive en milieu confiné (cuve de stockage...). Ce même jour, une petite explosion se produit lors du remplissage d'un camion de livraison dans une entreprise de commerce de combustibles ; les 2 gérants sont légèrement brûlés au niveau du front, mais ne font pas appel aux secours : 2 600 m³ au total ont été distribués à 2 070 entreprises ou particuliers.
Un défaut d'étanchéité entre les canalisations reliant la raffinerie à 2 « stockeurs » est à l'origine de l'incident. **Une vanne censée isoler 2 pipelines livrant simultanément 2 « stockeurs » en essence et en fioul ne s'est pas correctement fermée tout en donnant une information erronée en salle de contrôle.**

VOIR AUSSI Aria 8885, 18339,38617, 40986, 41305 , 41736, 41849, 42156

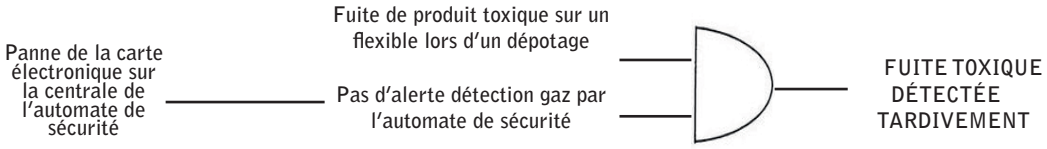
PANNE DUE À UN ACTIONNEUR (ARIA 38485) 23/03/2010



Dans une installation de production de biogaz classée Seveso, un délutage se produit à 1h15 au niveau d'un gazomètre. Le délutage est une émission de biogaz au niveau d'un gazomètre due à un déséquilibre entre ses débits entrant et sortant. Lorsque la capacité maximale du gazomètre est atteinte, le biogaz s'échappe par la garde hydraulique de l'ouvrage. Le phénomène peut être anticipé par suivi du niveau. **Le jour de l'accident, une défaillance matérielle (problème de connectique) sur la fin de course d'une vanne neutralise l'automatisme gérant les configurations d'exploitation, bloquant ainsi les possibilités de transfert ou de torchage du biogaz.** Le biogaz non extrait du gazomètre est alors dégazé.
Ne pouvant agir à distance, l'exploitant actionne manuellement sur place le jeu de vannes du réseau de transfert pour rétablir la situation. L'une d'elle, « dure » à manœuvrer, demande plusieurs minutes d'intervention sous ARI . Le « retour à la normale » a lieu 25 minutes plus tard ; 600 kg de biogaz (composé à 65 % de méthane, 34 % de CO_2 et d'impuretés dont de l'H_2S à 50 ppm) ont été émis à l'atmosphère.
Cet incident révèle la fragilité des dispositifs de fins de course. L'exploitant décide de les modifier pour les fiabiliser et d'allonger leur plage de détection. Les vannes « dures » seront remplacées pour les rendre plus aisées à manoeuvrer manuellement en cas de besoin.

VOIR AUSSI Aria 5989, 27060, 33423, 43146

PANNE DE CARTE ÉLECTRONIQUE (ARIA 42931) 02/05/2012



Lors d'une livraison de méthoxyméthane (DME) dans une usine de produits cosmétiques, un flexible de transfert gonfle au niveau du raccord vers l'installation fixe et fuit en raison d'une incompatibilité entre le matériau du flexible et le produit livré. L'opératrice constate la fuite et alerte le chauffeur qui ferme la vanne de fond de cuve et coupe le moteur du camion. Le bouton d'arrêt d'urgence est actionné pour déclencher la mise en sécurité du poste de dépotage et l'évacuation de l'usine par précaution durant 20 min. **L'accident met en évidence une détection gaz qui s'est révélée inopérante à cause d'un défaut matériel des cartes électroniques de la centrale de traitement (cartes datant de 2001)**. Les capteurs, rapidement saturés, sont passés en signal « hors échelle » ; signal qui a été traité comme « défaut de capteur » sans action particulière (alors que le « hors échelle » doit normalement déclencher les procédures de sécurité).
Le fabricant de la carte aurait identifié le risque potentiel de dysfonctionnement depuis 2008 et remédié à la situation (par changement des cartes et mise à jour du logiciel). Toutefois, l'ensemble des cartes concernées n'avaient pas été rappelées ou mises à jour. L'exploitant de l'usine chimique remplace l'ensemble de ses cartes.

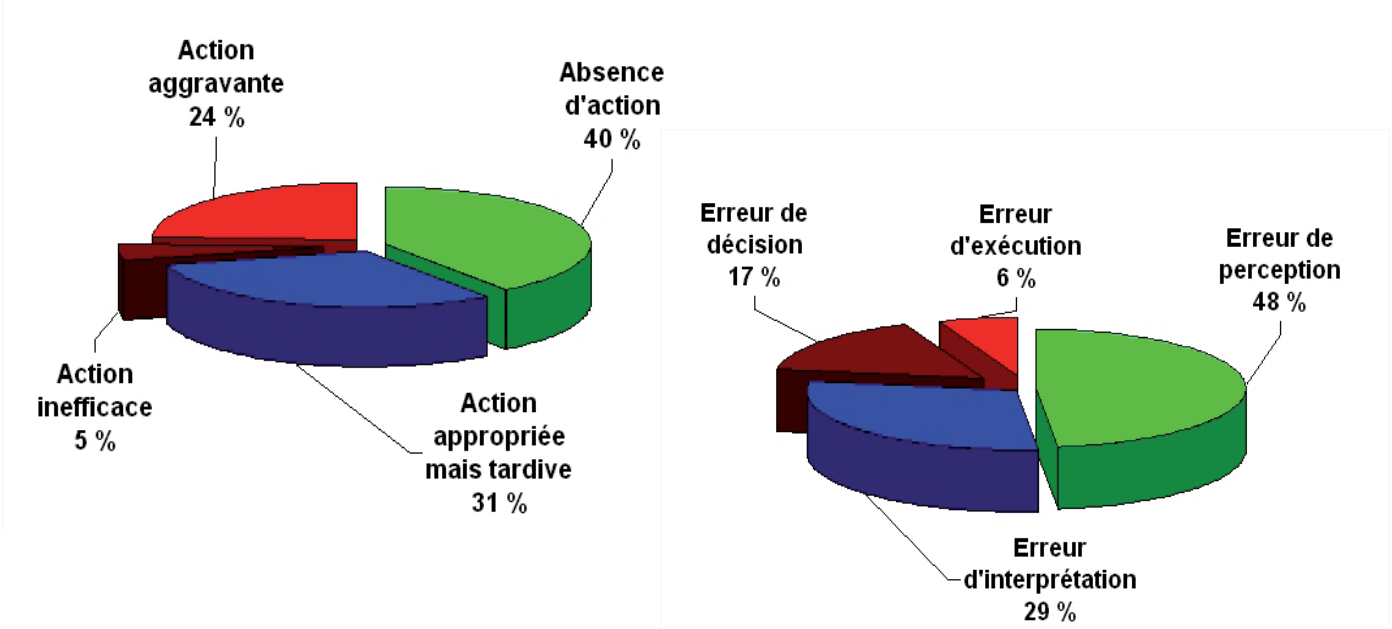
VOIR AUSSI Aria 3536, 7172, 10064, 21466, 27060, 32624, 39321, 43437

2.2 Les erreurs de conduite

Dans un contexte de développement des systèmes de conduite centralisée, le rôle des opérateurs de conduite et des chefs de quarts est essentiel au bon fonctionnement et à la sécurité des installations. Dans le milieu du raffinage, une question circule ainsi en boutade : « *Combien de minutes une raffinerie fonctionnerait sans incident ou accident si on évacuait tous les employés ?* ». Les erreurs de conduite constituent la cause directe de 63 % des accidents impliquant une défaillance de la fonction traitement (173 cas). Ces erreurs se traduisent le plus souvent par une absence ou un retard de réaction de l'opérateur confronté à une situation inhabituelle (fig. 8, à gauche), traduisant des causes profondes liées à la conception du système de conduite, à la charge de travail et à la formation de ces opérateurs (voir chapitre 3).

70 % des erreurs de conduite se traduisent par une absence de réaction ou une réaction trop tardive de l'opérateur face à une situation inhabituelle.

Figure 8 *Symptômes (à g.) et catégories (à dr.) des erreurs de conduite*



Pour mieux appréhender leur nature, les différentes erreurs de conduite rencontrées ont été classées en 4 catégories (fig. 8, à droite) :

- **L'erreur de perception*** **:** l'opérateur n'a pas ou mal perçu les informations envoyées par l'automate sur l'état du ou des procédés dont il assure la conduite.
- **L'erreur d'interprétation :** l'opérateur a bien perçu les informations disponibles, mais ne comprend pas correctement l'état dans lequel se trouve le(s) procédé(s).
- **L'erreur de décision :** l'opérateur a bien compris l'état du ou des procédés, mais choisit d'effectuer une action se révélant inadaptée, ou de ne pas effectuer une action qui aurait été adaptée, décision menant (ou contribuant à mener) à l'accident ou à son aggravation.
- **L'erreur d'exécution :** l'opérateur a pris une bonne décision, mais se trompe lors de son exécution.

Chaque catégorie d'erreur est imbriquée dans la précédente, une erreur de perception d'un opérateur entraînant implicitement de sa part une erreur d'interprétation, puis de décision et d'exécution.

Les problèmes de perception et d'interprétation des informations par l'opérateur expliquent plus de 3/4 des erreurs de conduite.

* : La notion de perception retenue pour l'analyse se limite à la disponibilité et la présentation du signal extérieur, et non aux différents facteurs physiologiques ou mentaux qui influencent la perception de ce signal par l'opérateur (fatigue, apprentissage, capacités visuelles ou auditives...).

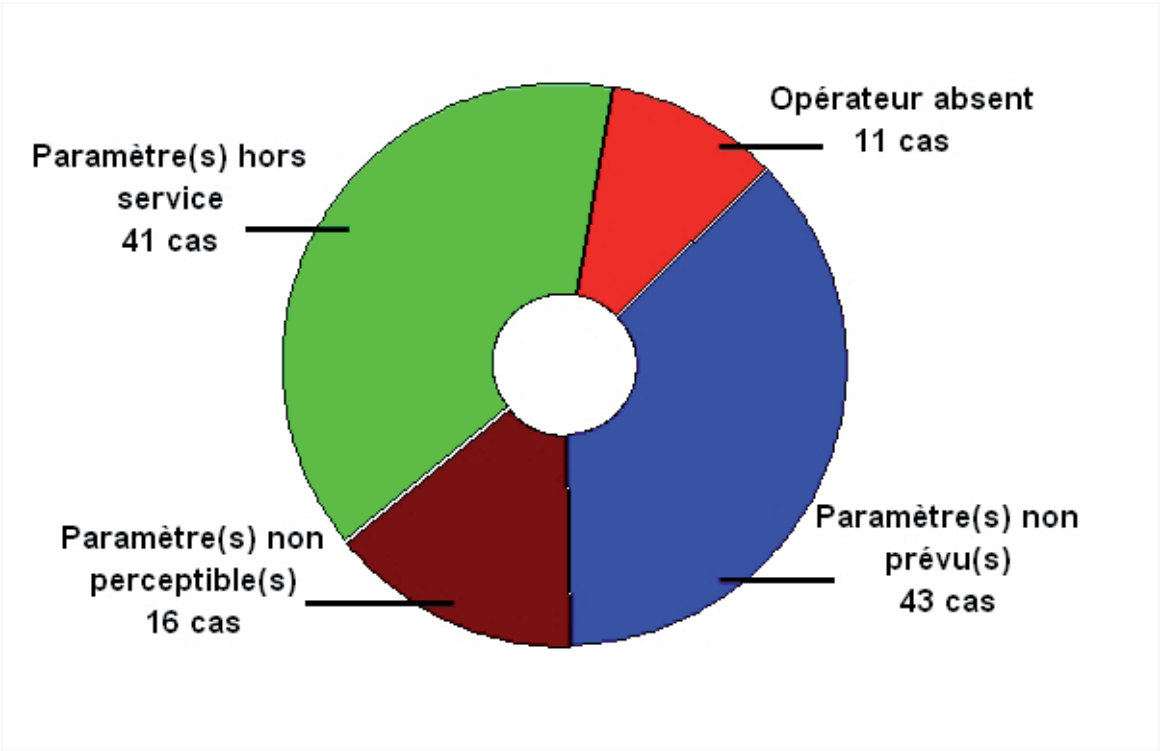
2.2.1 Erreurs de perception

La figure 8 (p. 15) montre que la perception des informations délivrées par l'automate à l'opérateur de conduite est la plus souvent mise en cause.

Les problèmes de perception expliquent à eux seuls la moitié des accidents de traitement dus à des erreurs de conduite.

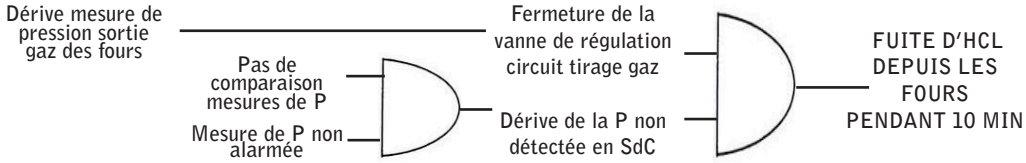
Les erreurs de perception ont été classées en 4 sous-catégories (fig. 9). Ce classement montre que la plupart des erreurs de perception ne sont pas directement imputables à l'opérateur. En effet, certains paramètres de conduite sont indisponibles lors de l'accident en raison d'une panne, ou d'un défaut de conception qui a rendu ces paramètres impossibles à percevoir dans les conditions de travail de l'opérateur, ou tout simplement parce que le suivi de ces paramètres n'était pas prévu initialement (voir chapitre 3, ARIA 42690 p. 38 et ARIA 12671 p. 43). Enfin, quelques erreurs de perception sont dues à l'absence de l'opérateur, occupé par d'autres tâches urgentes qui lui ont été assignées. Des exemples d'accident illustrant les erreurs de perception sont présentés page 17.

Figure 9 *Les différents types d'erreurs de conduite liée à la perception*



Près de 80 % des erreurs de perception de l'opérateur ont pour origine l'indisponibilité des paramètres qui lui sont nécessaires pour comprendre la situation en cours ou prendre la bonne décision.

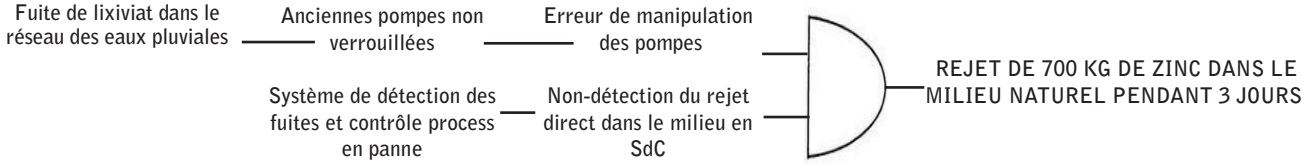
PARAMÈTRES NON PRÉVUS (ARIA 30178)
03/03/2005



Dans une usine chimique, 0,6 t de chlorure d'hydrogène (HCl) s'échappe pendant 10 min de l'ensemble des fours et évents de l'atelier de sulfate de potassium lors du nettoyage des circuits d'HCl. Un employé résidant à proximité du site alerte le poste de garde de la présence d'un brouillard provenant de l'usine. La mise en service de l'arrosage d'urgence des lavantes permet de stopper les émissions. Une dérive d'1 des 2 dispositifs de mesure de pression de la sortie de gaz des fours (sans lien direct avec l'intervention), entraînant la fermeture de la vanne de régulation du circuit de tirage des gaz, est à l'origine de l'incident : les gaz n'étant plus tirés se sont échappés des fours. **L'absence d'alarme sur ce paramètre de conduite a retardé l'intervention du personnel et l'absence d'inter-comparaison entre les 2 mesures de pression a rendu impossible la détection de la dérive du capteur**. Pour diminuer la probabilité d'un nouvel incident, une alarme de détection d'écart entre les 2 mesures de pression est installée, et une procédure identifiant les interventions délicates imposant notamment la présence de l'encadrement est rédigée.

VOIR AUSSI Aria 4582, 12671, 28389, 32841, 33310, 37825, 41945

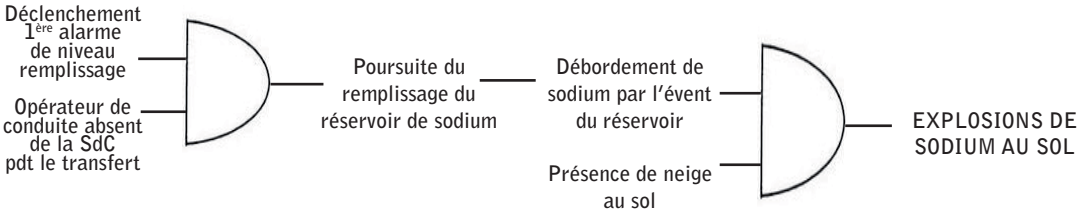
PARAMÈTRES HORS SERVICE (ARIA 26895)
21/01/2004



Dans une usine métallurgique, des eaux chargées en zinc se déversent dans un canal lors du redémarrage après un entretien périodique des ateliers de lixiviation et d'électrolyse. L'établissement dispose d'un réseau d'eaux pluviales polluées, relié à une fosse de relevage permettant leur transfert vers un bassin de stockage de 5 500 m³ et une station de neutralisation-décantation mise en service l'année précédente. Les anciennes pompes de la fosse qui permettent un rejet direct (sans traitement) dans le canal ont été maintenues en place pour être utilisées dans des situations exceptionnelles. Le jour de l'accident, des fuites sur les échangeurs de la lixiviation s'écoulent dans ce réseau d'eaux pluviales puis, à la suite d'une erreur de manipulation des pompes, sont rejetées sans traitement dans le canal durant 3 jours ; 700 kg de zinc sont ainsi déversés dans le milieu naturel. Une enquête révèle que l'erreur de manipulation a été possible en raison du maintien en place sans consignation des anciennes pompes. **L'Inspection constate également une panne du système de détection des fuites et de la chaîne de transmission du contrôle process à l'ordinateur central.**

VOIR AUSSI Aria 11665, 31376, 32579, 33306, 37041, 41207, 42690

OPÉRATEUR ABSENT (ARIA 15018)
26/02/1999



Une usine d'électrolyse ignée du chlorure de sodium comprend une partie basse pour l'électrolyse et, reliée par un sodioduc, une usine haute où sont chargées les citernes ferroviaires. Dans cette dernière, 2 réservoirs tampons de 60 m³, sous azote et équipés de 3 alarmes de niveaux, sont implantés dans un bâtiment. Le remplissage des réservoirs dure 2 h et est commandé depuis l'usine basse. **Un opérateur de l'usine haute surveille l'opération et doit informer l'usine basse lorsque la 1ère alarme sonne. Occupé ailleurs le jour de l'accident, l'opérateur n'entend pas l'alarme**. Du sodium sort par l'évent azote d'un réservoir qui débouche hors du bâtiment. Son explosion au contact de la neige alerte l'opérateur de l'usine basse qui arrête le transfert de sodium. Le POI est déclenché. Le bardage du bâtiment est endommagé. Le transfert du sodium est asservi aux alarmes, un piège froid est installé sur l'évent et des consignes sont modifiées.

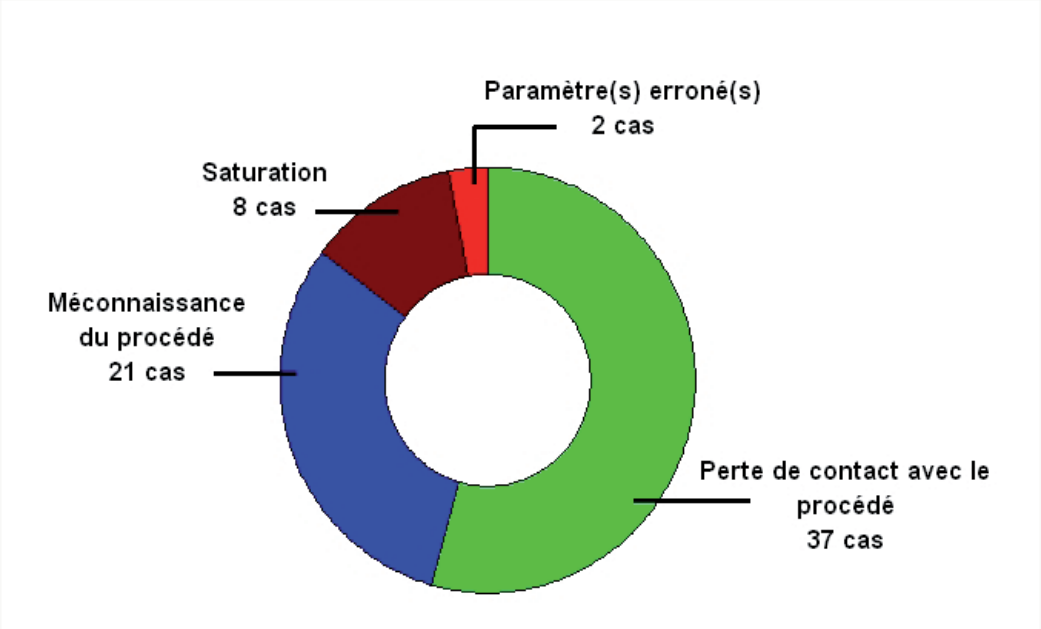
VOIR AUSSI Aria 7600, 21466, 22988, 24436, 35992, 36061

2.2.2 Erreurs d'interprétation

L'erreur de conduite qui n'est pas due à des problèmes de perception des paramètres nécessaires à l'opérateur découle souvent des problèmes qu'il rencontre pour bien comprendre la situation en cours sur le procédé qu'il supervise. Les différentes erreurs d'interprétation rencontrées ont été réparties en 4 sous-types (fig. 10) et font ressortir des causes profondes plutôt liées à la qualification et à l'implication de l'opérateur dans ses tâches de conduite (voir chapitre 3.1).

Les erreurs d'interprétation représentent plus du quart des accidents de traitement dus à des erreurs de conduite.

Figure 10 *Les différents types d'erreurs de conduite liées à l'interprétation*



- **Méconnaissance du procédé :** ce type d'erreur d'interprétation est souvent rencontré quand un procédé est automatisé ou modernisé, ou lors d'un incident inhabituel sur l'automate. Dans le premier cas, les contraintes productives conduisent parfois à une mise en service rapide alors que les opérateurs ne sont pas suffisamment habitués et formés à la conduite de l'automate. L'expérience professionnelle et le niveau de qualification des opérateurs ne les a ainsi pas toujours préparés à superviser « virtuellement » un procédé fortement automatisé, où il faudra savoir conduire des équipements depuis son siège, repérer les paramètres importants sur plusieurs écrans et établir une représentation mentale de la situation du procédé à partir de ces données. La maîtrise « terrain » qu'ils avaient du procédé est remise en cause ; ne pouvant plus s'appuyer directement sur leur expérience, ils peuvent être déstabilisés.

PAROLES DE TERRAIN

« Mon apprentissage s'est fait sur le tas [...] Untel n'a pas reçu de formation lorsqu'il a été intégré aux équipes en 4 x 8 ».

Témoignage d'un opérateur de conduite d'un site pharmaceutique français en 2008 [6]

En situation d'incident sur l'automate, la formation et l'entraînement de l'opérateur sont d'autant plus importants qu'il est amené à reprendre la main sur un procédé en situation dégradée, donc plus difficile à gérer, et doit agir rapidement pour éviter que l'incident n'évolue en accident (voir ARIA 32109 p. 22). Une étude australienne réalisée en 2005 auprès des opérateurs de salle de contrôle de réseaux ferrés, d'usines automatisées et de centrales thermiques montre que 51 % d'entre eux estiment leur niveau de formation insuffisant, dont 80 % de ceux supervisant des centrales thermiques [7]. L'étude britannique portant sur 107 sites industriels automatisés avec conduite centralisée relève que seulement 23 % d'entre eux avaient mis en place une formation spécifique des opérateurs à la conduite et aux situations d'urgence, 15 % un système d'habilitation au poste de conduite et que seulement 3 % disposaient d'un simulateur d'entraînement au poste de conduite [5].

Salle de contrôle d'une aciérie dans les années 2000

- **Perte de contact avec le procédé :** dans un procédé fortement automatisé, l'opérateur devenu superviseur isolé en salle de contrôle n'est plus en contact avec le procédé et perd ses repères sensoriels (bruit, vibration...). Il finit pas ne plus le connaître suffisamment et peut perdre sa connaissance profonde des équipements. Le procédé devient une « boîte noire » dont il ne connaît que la partie émergée virtuelle : les informations transmises par l'automate en salle de contrôle. Il doit alors construire sa représentation mentale du procédé sur la base de ces informations filtrées et peut avoir du mal à relier l'activation logicielle d'une commande avec celle matérielle d'un équipement dont il peut ignorer la localisation précise dans l'unité. Enfin, les effets de cette commande sur le procédé peuvent n'être visibles sur les écrans que plusieurs heures après la fin de son quart.

PAROLES DE TERRAIN

« Les gens prennent pour argent comptant ce qu'ils voient sur l'écran. Les jeunes ont une logique d'informatique et ne vont pas sur le terrain... ils se retranchent derrière l'outil informatique ».

Témoignage d'un ingénieur français de procédés chimiques en 2008 [6]

De plus, le « confort » relatif de la salle de contrôle (café, musique, sièges, chauffage ou climatisation...) et la disponibilité immédiate des paramètres de conduite sur les écrans ne l'incitent pas à effectuer des tournées dans l'unité pour acquérir une connaissance « terrain » du procédé, acquisition qui nécessiterait de se glisser entre des équipements salissants, bruyants ou dangereux alors que parfois il gèle ou il pleut. Il perd la connaissance des paramètres critiques, se dégage « mentalement » du procédé et finalement n'interprète qu'avec difficultés et retard les situations anormales (voir ARIA 43147 p. 22 et ARIA 12671 p.43).

Les causes profondes à l'origine de cette « perte de contact » semblent moins, comme on pourrait le croire, liées aux capacités intrinsèques de l'opérateur qu'à des facteurs organisationnels qui incitent l'opérateur à tomber dans la routine, ou perturbent sa capacité à comprendre la situation en lui présentant trop ou pas assez de paramètres pertinents (voir chapitres 3.3 et 3.4).

PAROLES DE TERRAIN

« Au départ, on devait avoir du personnel en salle et des rondiers dans l'atelier. Petit à petit, les rondiers sont venus en salle de contrôle. Et à l'heure actuelle, il y a une méconnaissance de l'atelier. On ne sait plus ce qui va se passer si on appuie sur le bouton ».

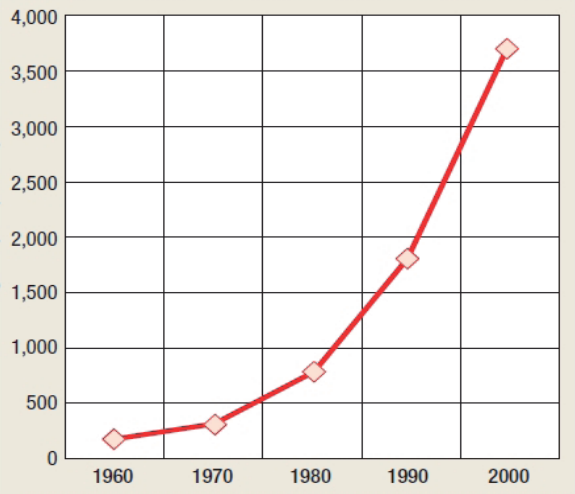
Témoignage d'un agent de maîtrise d'un site chimique français en 2008 [6]

« Depuis qu'on a amené les nouvelles technologies et mis des systèmes [automatisés] à ne plus finir, tu perds le contrôle de ce que tu fais ».

Témoignage d'un opérateur de conduite d'une raffinerie canadienne [8]

- **Saturation :** l'opérateur brutalement submergé d'informations non hiérarchisées transmises par un automate n'arrive plus à établir un diagnostic correct de la situation et finit par ignorer ces données qu'il n'arrive plus à exploiter. Le cas le plus courant est une phase de redémarrage quand beaucoup d'alarmes sonnent en salle de contrôle et sont ignorées. Ainsi, un accident dans une raffinerie nord-américaine a été aggravé par l'inaction de l'opérateur en salle de contrôle qui se trouvait confronté à plus de 300 alarmes à traiter en moins de 5 minutes [9]. En 1994, les 2 opérateurs de quart dans la salle de contrôle de la raffinerie de *Milford Haven* (GB) ont été confrontés à 275 alarmes non priorisées en 11 minutes : ils ont fini par fuir la salle de contrôle peu avant l'explosion de la raffinerie ! Un exemple de saturation des opérateurs d'une raffinerie française est présenté en bas de la page 22.

Figure 11 *Evolution du nombre d'alarmes différentes que doit gérer un opérateur de conduite de plate-forme pétrolière entre 1960 et 2005 (source : World Oil, septembre 2006)*



Les études dans le domaine de la gestion des alarmes en salle de contrôle menées depuis le début des années 2000, dont certains résultats apparaissent dans le tableau 1, montrent clairement que ce n'est pas la capacité de l'opérateur de conduite qui est en cause mais plutôt l'inflation exponentielle des alarmes au poste de conduite dont le nombre dépasse maintenant de loin les capacités de traitement des opérateurs (voir fig. 11). Un chef de projet industriel français estimait en 2011 que seulement 20 à 40 % des alarmes des postes de conduite industriels étaient vraiment nécessaires [10].

Enfin, un sondage réalisé aux États-Unis en 2012 auprès d'un panel de sites industriels à la conduite centralisée, composé à 52 % d'industrie lourde, à 33 % d'industrie manufacturière et à 15 % de sites pharmaceutiques et agroalimentaires, montrait que la moitié des sites sondés ne disposaient d'aucune méthode de gestion des alarmes de conduite alors que 70 % d'entre eux reconnaissaient que la surcharge d'alarmes avait des conséquences négatives sur la production et la sécurité des procédés [11].

La conclusion de ce sondage était que cette situation résultait plus d'un problème de culture d'entreprise et de formation du personnel que de l'absence de méthodologie, puisque de nombreuses méthodes reconnues de gestion et de hiérarchisation des alarmes existent et font même partie de certaines normes techniques internationales, comme l'ISA18.2.

	Pétrole	Chimie	Energie	Autre	Standard EEMUA 191	Standard ISA 18.2
Nombre moyen d'alarmes par jour	1200	1500	2000	900	de 150 à 300	de 150 à 300
Nombre maximal en 10 minutes	220	180	350	180	< 10	< 10 pendant 2,5 heures au maximum
Nombre moyen en 10 minutes	8	9	8	5	1 à 2	1 à 2

Tableau 1

Comparaison entre la fréquence des alarmes au poste de conduite mesurée dans différents secteurs industriels nord-américains et la fréquence recommandée par les bonnes pratiques [12]

PAROLES DE TERRAIN

« Aujourd'hui, les systèmes d'informations ajoutent quantité d'informations, trop pour permettre à l'opérateur de tout gérer ».

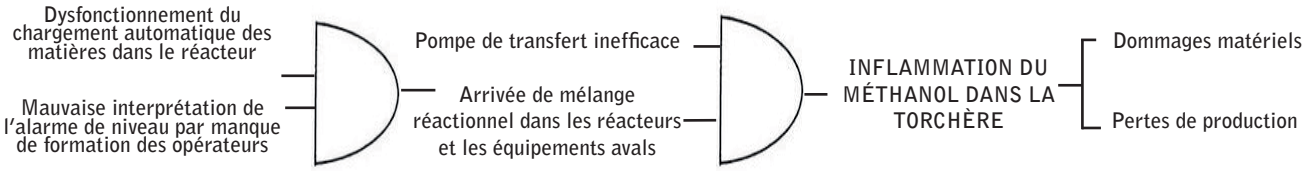
Témoignage d'un chef de projet industriel [10]

« Dans le secteur de la pétrochimie, les pertes liées à des défauts d'alarmes représenteraient de 10 à 20 milliards de $. Le coût d'un incident typique : de 100 000 à 1 million de $ ».

Témoignage d'un bureau d'études industriel nord-américain [10]

- **Paramètres erronés :** ce type d'erreur d'interprétation est beaucoup plus rare (moins d'1 erreur d'interprétation sur 10). Dans ce cas, les informations fausses dont dispose l'opérateur lors de l'accident ne lui permettent pas d'analyser correctement la situation en cours sur le procédé qu'il est chargé de surveiller (voir ARIA 35774 p.14 et ARIA 40969 p. 31).

MÉCONNAISSANCE (ARIA 32109)
12/07/2006



Dans une usine chimique, un feu se déclare vers 20h30 au niveau de la torchère d'un atelier de production de biocarburant, lors de la fabrication de diester par trans-estérification d'huile végétale par du méthanol. L'installation est mise en sécurité par coupure de l'alimentation en méthanol et en gaz. Les pompiers maîtrisent le sinistre en une dizaine de minutes. Les conséquences sont limitées à la torchère malgré l'important flux thermique généré ; l'instrumentation et la partie courant faible sont détruites, les parties métalliques (canalisations, supportages) sont atteintes. L'atelier situé à 80 m est arrêté pour plusieurs semaines et une dizaine de personnes est en chômage technique. La végétation est carbonisée dans un rayon de 20 m autour de la torchère. Un dysfonctionnement dans le processus de chargement automatique des matières premières (huile, méthanol, catalyseur) est à l'origine de l'accident ; le réacteur et tous les équipements connexes (condenseur, canalisations externes, réservoir tampon en amont de la torche...) se sont remplis du mélange réactionnel. La pompe de transfert bien que déclenchée par l'alarme de niveau haut n'a pu abaisser le niveau dans le réservoir tampon et empêcher l'arrivée dans la canalisation de transfert vers la torche du méthanol liquide qui s'est alors enflammé. De multiples défaillances ou insuffisances des dispositifs de sécurité sont en cause ; le dépassement du niveau très haut n'a pas entraîné de mise en sécurité de l'installation, mais uniquement une alarme au poste de commande, **les dysfonctionnements au poste de chargement n'ont pas été détectés, l'intervention des opérateurs fut trop lente par manque de formation...**

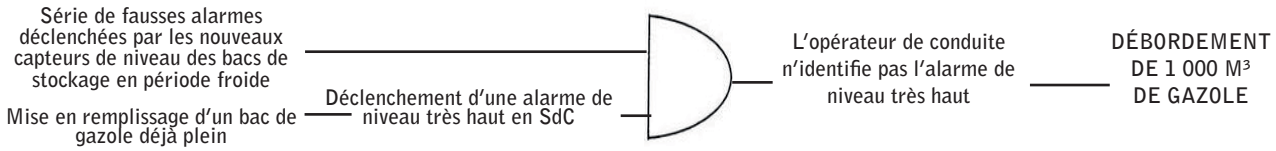
VOIR AUSSI Aria 2684, 6093, 27585, 33333, 33838, 35432, 41207

PERTE DE CONTACT AVEC LE PROCÉDÉ (ARIA 43147)
16/10/2002

Dans le cadre du redémarrage d'une centrale thermique, le turbo-alternateur est remis en service le 15/10 à 14 h et couplé sur le réseau national sans dysfonctionnement. Entre le 15/10 au soir et le 16/10 au matin, une montée en température anormale entraîne l'auto-inflammation de l'huile dans la caisse à huile et un incendie autour du turbo-alternateur. Plusieurs mesures correctives sont prises : mise en place d'une sécurité de température haute, suppression des filtres (limitant le débit d'huile), rappel aux opérateurs de conduite concernant les rondes à effectuer dans l'atelier.
La mise en place d'automatismes facilitant le démarrage et la surveillance des grosses machines pendant cette phase critique a conduit progressivement à oublier les précautions que prenaient jadis les opérateurs pendant plusieurs jours pour s'assurer que l'on avait effectivement atteint des conditions de marche stable. Les surveillances concernant les filtres, les températures diverses, de paliers notamment, les vibrations détectées à l'ouïe, permettaient généralement de prendre des mesures correctrices avant qu'une alarme annonce un état de détérioration quasi-inévitable.

VOIR AUSSI Aria 12671, 15397, 30920, 32632,41207

SATURATION DE L'OPÉRATEUR (ARIA 40584)
28/05/2011



Lors d'une ronde de changement de quart dans une raffinerie, un employé constate vers 5 h qu'un bac de stockage contenant du gazole déborde. Le remplissage est arrêté et le bac isolé ; 1 000 m³ d'hydrocarbures récupérés dans la cuvette de rétention sont transférés vers d'autres bacs, ainsi que vers le réseau d'égouts huileux pour être récupérés dans les bacs de recyclage. Le bac était plein lorsqu'il a été mis par erreur en remplissage vers 1h30. Le tableauteur a demandé à l'opérateur extérieur de fermer la vanne manuelle de coulage vers ce bac, mais l'opérateur a fermé celle de recirculation du bac. Le bac a débordé dans sa cuvette de rétention à partir de 4 h. Détectés par le système d'alarme de la conduite centralisée, ces transferts de produits non désirés n'ont pas été pris en compte à temps par le tableauteur. Les capteurs de niveau de type radar équipant les bacs du parc nord étaient en cours de remplacement suite à leur obsolescence. **Les nouveaux capteurs installés déclenchaient de nombreuses fausses alarmes en salle de contrôle en raison de la période de temps froid qui provoquait des sur-consommations nocturnes dans les bacs.** Ce problème de réglage de leurs seuils de détection était en cours de traitement quand l'accident est survenu : **le tableauteur n'a pas réussi à identifier l'alarme indiquant le débordement du bac accidenté au milieux des nombreuses fausses alarmes de niveau très haut des bacs voisins qui se déclenchaient continuellement en salle de contrôle.**

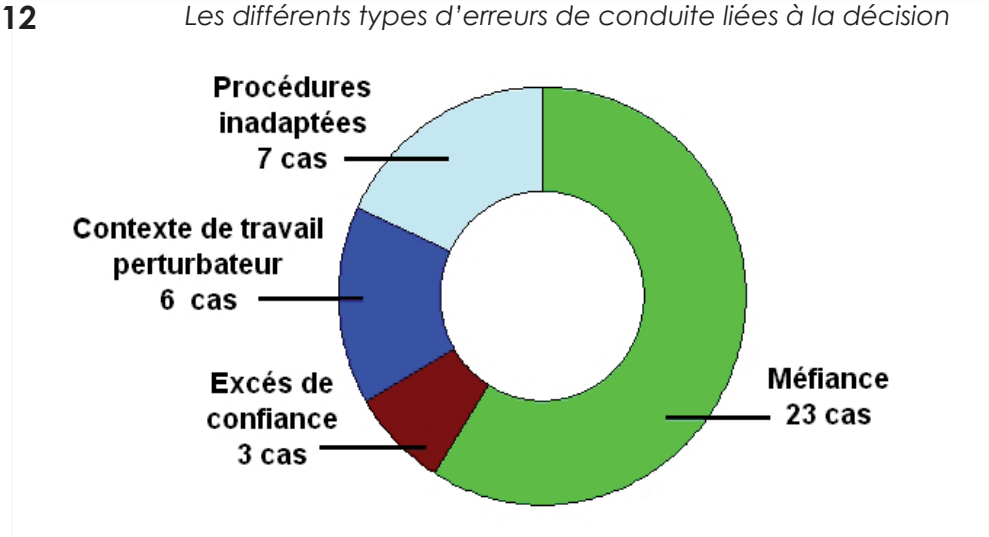
VOIR AUSSI Aria 26880, 30406, 30687, 33094, 38617, 43042, 43455

2.2.3 Erreurs de décision

Les erreurs de décision représentent une part faible des erreurs de conduite étudiées, mais mettent souvent en cause l'interaction de l'opérateur de conduite avec le système automatisé. Sur les 4 types d'erreur de décision présentés figure 12, 2 concernent en effet les biais de décision liés à l'opinion que porte l'opérateur sur le système automatisé qu'il supervise.

La majorité des erreurs de décision s'inscrivent dans un contexte de méfiance de l'opérateur vis-à-vis de l'automate.

Figure 12 *Les différents types d'erreurs de conduite liées à la décision*



- **Méfiance envers l'automate :** présent dans la majorité des erreurs de décision analysées, ce constat traduit souvent un malaise entre la « hiérarchie » qui décide l'automatisation de la conduite d'un procédé et la « base » qui subit l'arrivée d'une nouvelle méthode de travail. En pratique, l'opérateur évalue les performances de l'automate qu'il supervise. S'il estime que celui-ci n'est pas assez fiable ou efficace, il aura tendance à ne pas faire confiance aux paramètres transmis et à se fier à sa propre perception de la situation. L'accidentologie montre que cette situation se rencontre surtout en dehors des phases d'exploitation normales - démarrages, pannes d'équipements... - situations où les alarmes se déclenchent en série ou en cascade, poussant les opérateurs à les ignorer. Cette situation conduit parfois l'opérateur à « shunter » l'automate pour lancer des actions qu'il juge plus adaptées, mais qui se révèlent parfois désastreuses. C'est typique des situations où, à la suite de défauts de conception, des automates perturbent ou compliquent les tâches courantes des opérateurs (fausses alarmes fréquentes) ou entraînent des pertes de production et de rendement significatives (voir ARIA 37139 p. 25 et ARIA 33333 p. 31, ainsi que ARIA 21466 p. 41).

  Des études ont aussi montré qu'un effet pervers peut survenir quand ce shunt provoque un accident : il pousse la hiérarchie a réduire encore plus la liberté d'action de l'opérateur vis-à-vis de l'automate, créant une situation de « sur-automatisation » qui amène souvent l'opérateur a appliquer une stratégie encore plus complexe et risquée de contournement de l'automate [13]. La perte de contact avec le procédé - évoquée au chapitre 2.2.2 - peut se conjuguer à cette méfiance et inciter d'autant plus l'opérateur à shunter l'automate qu'il méconnaît les conséquences accidentelles possibles de son geste.

- **Excès de confiance :** cette erreur de décision est l'inverse de la précédente : jugeant l'automate performant et fiable, l'opérateur peut avoir tendance à relâcher son attention, à se « désengager mentalement » et à laisser l'automate « conduire » le procédé sans supervision humaine pendant des durées significatives, par exemple pour réaliser des tâches annexes, faire une petite pause ou à la suite d'une fatigue passagère. Un cercle vicieux s'engage parfois

car plus l'opérateur néglige son rôle de superviseur, moins il connaît le procédé et plus il a tendance à se « reposer » sur l'automate et à perdre son sens critique (voir ARIA 32640 p. 25). Une tendance analogue a été identifiée dans le domaine de l'aviation civile où, à la suite de plusieurs catastrophes, certains experts dénoncent « *des pilotes qui se mettent au service des automatismes, alors que les automatismes devraient être au service des pilotes* ».

« Le vrai danger n'est pas que les ordinateurs commencent à penser comme des hommes, mais que les hommes commencent à penser comme des ordinateurs ». ***Sidney J. Harris, écrivain et journaliste nord-américain***

Ce relâchement peut amener un opérateur à manquer des signaux d'alerte importants. En reprenant son rôle de superviseur, il tarde à comprendre la situation alors que la séquence accidentelle est déjà bien avancée. Cet excès de confiance peut aussi le conduire à perdre son sens critique et à se fier aveuglément à l'automate au mépris des évidences physiques (fumées, bruits anormaux, valeurs affichées contradictoires...). Cette attitude ne concerne pas que des opérateurs débutants ; une expérience effectuée en 1994 sur des pilotes de lignes expérimentés montre que la moitié d'entre eux continuaient à utiliser le pilote automatique alors que plusieurs données prouvaient que celui-ci était défaillant. Une autre étude réalisée en 1997 révèle que le taux de détection des défaillances d'un automate par des opérateurs de conduite était de 40 % en moyenne quand celui-ci avait une fiabilité constante, et de 70 % quand celui-ci avait un fonctionnement aléatoire [13].

- **Contexte de travail perturbateur :** ce type d'erreur survient lorsque un opérateur (ou un groupe d'opérateurs de conduite) doit prendre une décision face à une situation inhabituelle, donc peu fréquente. Certains éléments du contexte de travail vont perturber la prise de décision. En premier lieu le stress ressenti du fait de la nécessité de prendre dans un délai court - souvent une dizaine de minutes - une décision qui sera souvent irréversible (pas de droit à l'erreur). Puis la pression qui s'exerce sur le décisionnaire, ou qu'il se met lui-même, face aux enjeux importants liés à sa décision : risques d'aggravation de l'accident, de pertes économiques pour l'usine ou de surcharge de travail pour les collègues qui devront mettre l'unité en sécurité ou la redémarrer... (voir ARIA 28880 p. 28). Les résultats de différentes études portant sur la probabilité de prise d'une mauvaise décision par des opérateurs confrontés à une situation anormale montrent qu'elle est significative dans les 10 premières minutes suivant le déclenchement de cette situation : 70 % en moyenne, et toujours supérieure à 10 % pour des opérateurs expérimentés et bien entraînés selon la méthode *THERP* par exemple[19].

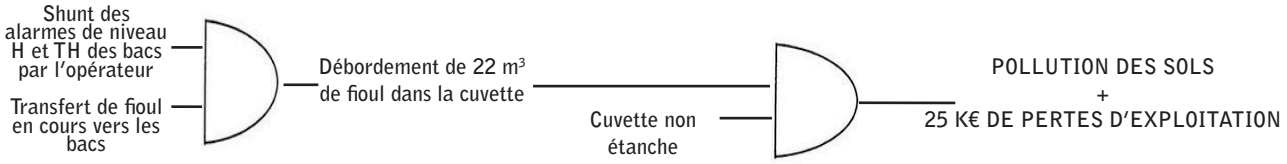
PAROLES DE TERRAIN

« C'est beau et c'est facile quand tout va bien, comme un pompier qui n'a pas de feu à éteindre… on fait des tests ou on va faire une ronde. Mais quand il arrive un problème, c'est là qu'il faut que tu prennes les bonnes décisions tout de suite, c'est là que ça devient stressant »

Témoignage d'un opérateur de conduite d'une raffinerie canadienne [8]

- **Procédures inadaptées :** lors d'une situation anormale, l'opérateur de conduite doit souvent se référer à des procédures écrites pour prendre sa décision. Mais celles-ci se révèlent parfois incomplètes ou inadaptées à la situation en cours, cette dernière n'ayant pas été envisagée lors de leur rédaction. L'opérateur va alors baser sa décision sur les préconisations de la procédure en vigueur, ou l'utiliser pour décider entre plusieurs choix possibles entre lesquels il hésite. S'il n'a pas la capacité de remettre en question la pertinence de la procédure dans la situation anormale en cours (voir le concept de « sécurité réglée » vs. « sécurité gérée » [18]), son respect de la procédure l'amène - ou contribue à l'amener - à prendre une mauvaise décision. Une étude nord-américaine menée en 2012 a montré que 40 % des erreurs opératoires survenues lors de situations anormales ou inhabituelles dans l'industrie avaient pour origine des procédures incomplètes ou mal rédigées [15](voir ARIA 24639 p. 25).

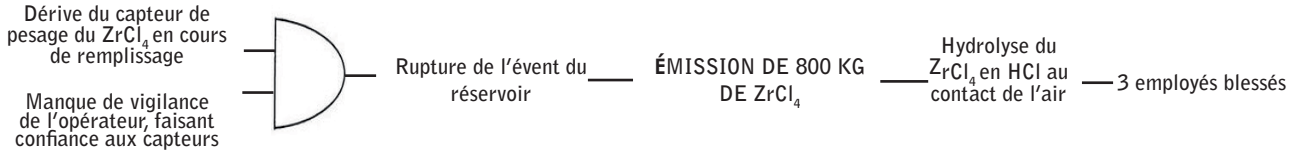
MÉFIANCE ENVERS L'AUTOMATE (ARIA 37139)
28/07/2009



Dans une centrale électrique, un transfert de fioul domestique du bac primaire (2 450 m³) vers les bacs journaliers, lancé vers 16 h, ne s'arrête pas automatiquement alors que le niveau haut est atteint. Vers 23 h, le gardien constate lors de sa ronde un débordement accidentel de fioul dans la rétention associée aux réservoirs journaliers. Le transfert est interrompu. La rétention n'étant pas totalement étanche, du fioul suinte en plusieurs endroits, polluant le sol. Près de 22 m³ de fioul ont débordé. L'exploitant estime la perte d'exploitation à 25 000 Euros. **Un opérateur avait forcé la marche de transfert du fioul en inhibant les niveaux haut et très haut des bacs journaliers**. L'inspection des installations classées constate par ailleurs l'absence de consigne pour le transfert du combustible, l'absence d'avertisseur sonore en cas de dépassement des niveaux haut et très haut et l'absence de réaction du personnel lors de l'apparition d'alarmes au niveau des systèmes de supervision sur le site et les sites déportés....

VOIR AUSSI Aria 164, 4908, 11107, 15397, 20490, 21466, 36496, 42163

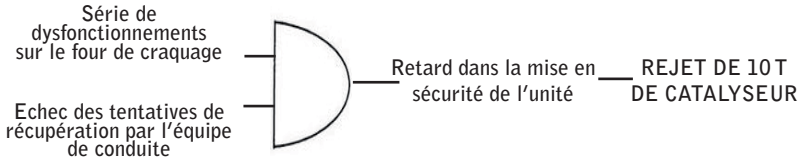
EXCÈS DE CONFIANCE (ARIA 32640)
10/01/2007



Un épandage de 800 kg de tétrachlorure de zirconium ($ZrCl_4$) a lieu vers 1 h dans l'unité de carbochloration d'un site chimique après rupture de la tuyauterie d'évent d'un réservoir de stockage. Lors du ramassage du $ZrCl_4$ épandu à l'extérieur, un nuage de chlorure d'hydrogène (HCl) se forme par hydrolyse. Le procédé met en œuvre 2 compacteuses qui alimentent 3 réservoirs de stockage de $ZrCl_4$ chacun via une conduite de transport pneumatique sous azote. Lors de l'accident, les 2 compacteuses alimentent le 1er réservoir chargé à 132 t selon les pesons tandis que les 2 autres sont vides. A 22h14, des dépassements de seuil de pression haute (90 mbar), répétés mais brefs, sur le capteur de pression du 1er réservoir entraînent l'arrêt de la 1ère compacteuse. A 0h50, le dépassement en continu du seuil de pression haute dans le réservoir indique l'éclatement de son disque de rupture. Les détecteurs d'HCl du bâtiment franchissent leur seuil d'alarme (5 ppm) 1 min plus tard. Finalement, la 2ème compacteuse ne sera arrêtée qu'à 1h50 sur intervention du personnel. Le $ZrCl_4$ s'est échappé via le disque de rupture et la canalisation d'évent en PVC rompue. Le système instrumenté associé au capteur de pression n'était couplé qu'à la 1ère compacteuse et n'avait pas d'effet sur la seconde. Le transfert de $ZrCl_4$ s'est donc poursuivi pendant 1 h après la rupture du disque et de la canalisation. Cette situation résulte d'une mauvaise gestion des modifications de l'installation. **Par ailleurs, les agents en salle de contrôle ne sont pas intervenus lors des déclenchements répétés des alarmes de pression, choisissant de faire confiance aux données du peson qui indiquait un niveau de remplissage de 132 t pour une capacité de 150 t.**

VOIR AUSSI Aria 22988, 42920

PROCÉDURES INADAPTÉES (ARIA 24639)
10/01/2003



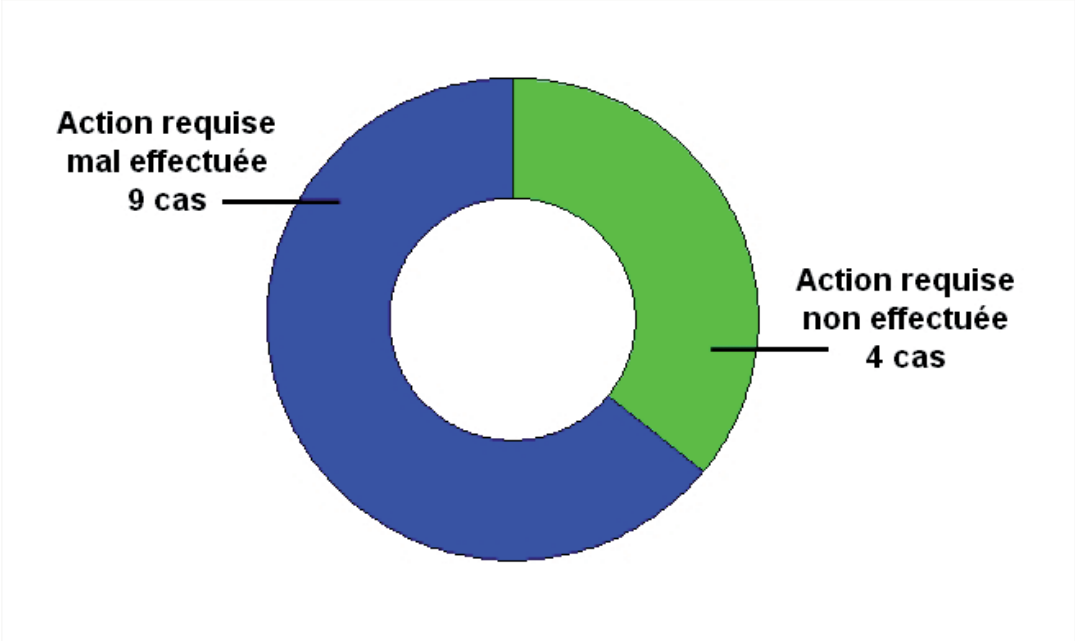
Dans une raffinerie, une série de dysfonctionnements de l'unité de craquage catalytique provoque l'envoi à la cheminée de 10 t de catalyseur. En début d'après-midi, une 1ère anomalie de fonctionnement apparaît : déclenchement d'une chaudière participant à l'alimentation en air du régénérateur. Aucune anomalie n'est détectée dans le réacteur. Une demi-heure plus tard, une baisse de la température de réaction est détectée. Simultanément, la pression au niveau du réacteur et du régénérateur baissent et la pression différentielle au niveau des cyclones augmente. L'alarme de niveau haut se déclenche sur le cyclone tertiaire. Des baisses de niveau du catalyseur se produisent ensuite dans le fond du strippeur et dans le régénérateur. L'équipe de conduite utilise toutes les variables à sa disposition pour rétablir la situation mais, devant le peu d'effet des actions, décide d'appliquer la stratégie d'urgence mise au point à la suite des incidents précédents et arrête l'unité à 18h30. Un premier bilan met en évidence un rejet de 10 t de catalyseur à la cheminée. **La recherche d'un rattrapage de la situation a fait perdre un temps précieux et provoqué un nouveau rejet de catalyseur à la cheminée. L'exploitant complète les consignes opératoires imprécises** et règle un seuil d'alarme plus bas sur la détection de niveau haut du cyclone tertiaire.

VOIR AUSSI Aria 21026, 21516, 32632, 33838, 40014, 42613

2.2.4 Erreurs d'exécution

Les erreurs d'exécution sont les erreurs de conduite les plus rares parmi les accidents étudiés. Ce constat s'explique par le fait que ces erreurs sont en bout de chaîne cognitive (voir chapitre 2.2), mais aussi parce que l'opérateur de conduite ou le « collectif de travail » arrive à rattraper la majorité des erreurs de ce type, bien qu'elle soient très fréquentes (de 70 à 80 % des erreurs humaines [18]). Dans tous les cas, ces erreurs recouvrent aussi bien la mauvaise exécution de l'action requise (erreur de geste) que sa non-exécution (oubli).

Figure 13 *Les différents types d'erreurs de conduite liée à l'exécution*



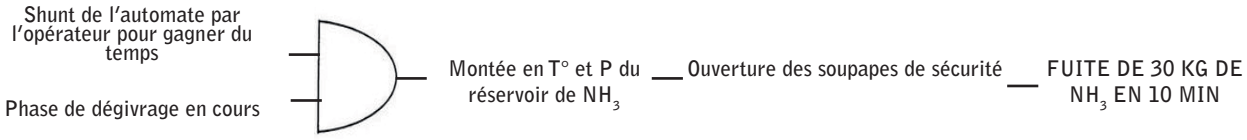
- **Action requise non effectuée :** Bien souvent, la non exécution d'une action requise est liée à une charge de stress importante pour l'opérateur. En effet, l'opérateur de conduite doit réagir correctement aux alarmes, ce qui nécessite une attention soutenue qui peut amener à l'oubli d'une action décidée parmi beaucoup d'autres à effectuer dans un temps limité. Il est d'autant plus stressé qu'il se retrouve parfois seul (quart de nuit) à gérer une situation complexe, l'automatisation ayant permis de diminuer fortement les effectifs des unités (voir ARIA 38617 p. 27).
- **Action requise mal effectuée :** ces erreurs recouvrent celles que peut commettre l'opérateur de conduite dans un cadre routinier comme des ratés (oubli de programmation, appui involontaire sur un bouton) ou la saisie involontaire d'une mauvaise valeur. Un exemple d'accident découlant de ce type d'erreur est présenté en bas de la page 27.

PAROLES DE TERRAIN

« Déclenchement... salle de contrôle : à moitié dans le coltar, il faut reprendre ses esprits à toute vitesse, le stress complet, l'adrénaline qui monte... Être efficace, éviter les fausses manœuvres. Les vérines clignotent, les alarmes carillonnent, sonnent, les imprimantes crépitent...»

Témoignage d'un opérateur de conduite (de nuit) d'un site chimique [14]

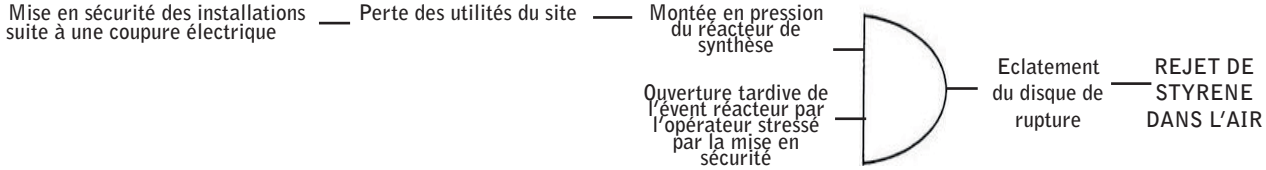
DÉCISION - CONTEXTE DE TRAVAIL PERTURBATEUR (ARIA 28880)
05/01/2005



Dans un établissement de surgelés, 30 kg d'ammoniac gazeux sont émis à 10h08 et durant 10 min par la soupape de sécurité d'une installation de réfrigération. Légèrement intoxiqués, 2 sous-traitants en intervention sont hospitalisés par précaution, 10 employés sont examinés sur place et 30 personnes sont évacuées. **Voulant accélérer une phase de dégivrage des équipements, un agent qui a suivi des stages de frigoriste et est habilité pour intervenir sur ce type d'installation avait décidé de passer en mode manuel en arrêtant les ventilateurs de refroidissement des condenseurs alimentant le réservoir haute pression (HP) de l'installation.** Le dégivrage certes plus rapide a en fait été réalisé sur une installation en régime instable : diminution du refroidissement des compresseurs, puis augmentation de la température et de la pression dans le réservoir HP jusqu'au dépassement de la pression de tarage de la soupape.

VOIR AUSSI Aria 21466, 34477, 38674, 39384, 42163

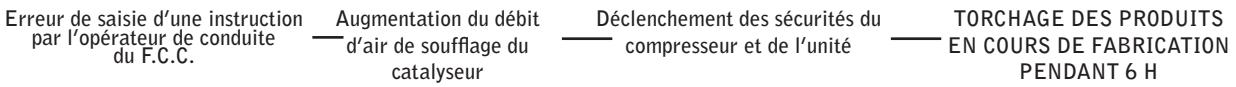
ACTION NON EFFECTUÉE (ARIA 38617)
14/07/2010



Lors d'un orage, une coupure électrique perturbe à 22h46 la production de polystyrène (PS) d'un site Seveso. Un disque de sécurité se rompt et du styrène est émis à l'atmosphère. Pour minimiser les effets des microcoupures (orages) sur la qualité des produits, l'exploitant a l'habitude de basculer l'alimentation des ateliers sur les 4 groupes électrogènes de sa centrale. La manoeuvre est réalisée à 22h20, 3 groupes étant disponibles. A 22h43, l'orage met en défaut le 1er groupe ; les 2 autres ne suffisant pas, la centrale se met en sécurité à 22h46 avec perte des utilités. Un agent tente de redémarrer la centrale, puis l'astreinte maintenance électrique, seule habilitée à basculer l'alimentation sur le réseau EDF, est appelée à 22h53. A 23h05, un réacteur de synthèse sur 1 des 3 lignes de fabrication monte en pression. Selon la procédure d'urgence, des gyromonitors démarrent à 23h15 pour abattre d'éventuelles vapeurs à l'évent du réacteur. Le site est reconnecté au réseau à 23h18, mais les unités ne démarrent qu'après un délai. A 23h20, le disque de rupture du réacteur éclate, projetant un mélange liquide de 10 t de PS et 3 t de styrène. L'emballement du réacteur est dû à la perte des utilités. **L'opérateur de la salle de contrôle n'a pas ouvert l'évent suffisamment tôt compte tenu de l'ensemble des actions à gérer pour mettre en sécurité les 3 lignes de polystyrène ainsi que le prévoyait la procédure.**

VOIR AUSSI Aria 2900, 23893, 26363, 41518

ACTION MAL EFFECTUÉE - ERREUR DE GESTE (ARIA 33334)
15/07/2007



A 21h03, **le tableauteur chargé de la section catalyse de l'unité de craquage catalytique (F.C.C.) d'une raffinerie entre une valeur d'ouverture erronée** de la vanne de mise à l'atmosphère au refoulement du compresseur insufflant l'air nécessaire à la mise en suspension du catalyseur dans le régénérateur. Cette vanne permet de détourner une partie du débit d'air au refoulement du compresseur pour protéger ce dernier des phénomènes de pompage. **Le tableauteur de quart indique puis valide une valeur de commande d'ouverture erronée de la vanne (inférieure à 10 %) alors qu'il souhaitait abaisser la valeur de 20 % à 19,5 %.** Cette instruction a pour conséquence d'augmenter le débit d'air au régénérateur et en cascade de déclencher la sécurité du compresseur, puis de l'ensemble de l'unité. Celle-ci se décomprime durant 15 min provoquant des émissions à la torche, puis son arrêt progressif. L'exploitant redémarre progressivement l'unité de 23 h à 5 h, occasionnant de nouvelles émissions à la torche. La consigne mise à jour demande au tableauteur de ne plus entrer de valeur mais d'utiliser uniquement les commandes («flèche montante» ou» flèche descendante») incrémentant la valeur initiale de 0,5 ou 1 % au maximum.

VOIR AUSSI Aria 4582, 5900, 31307, 33516, 35533

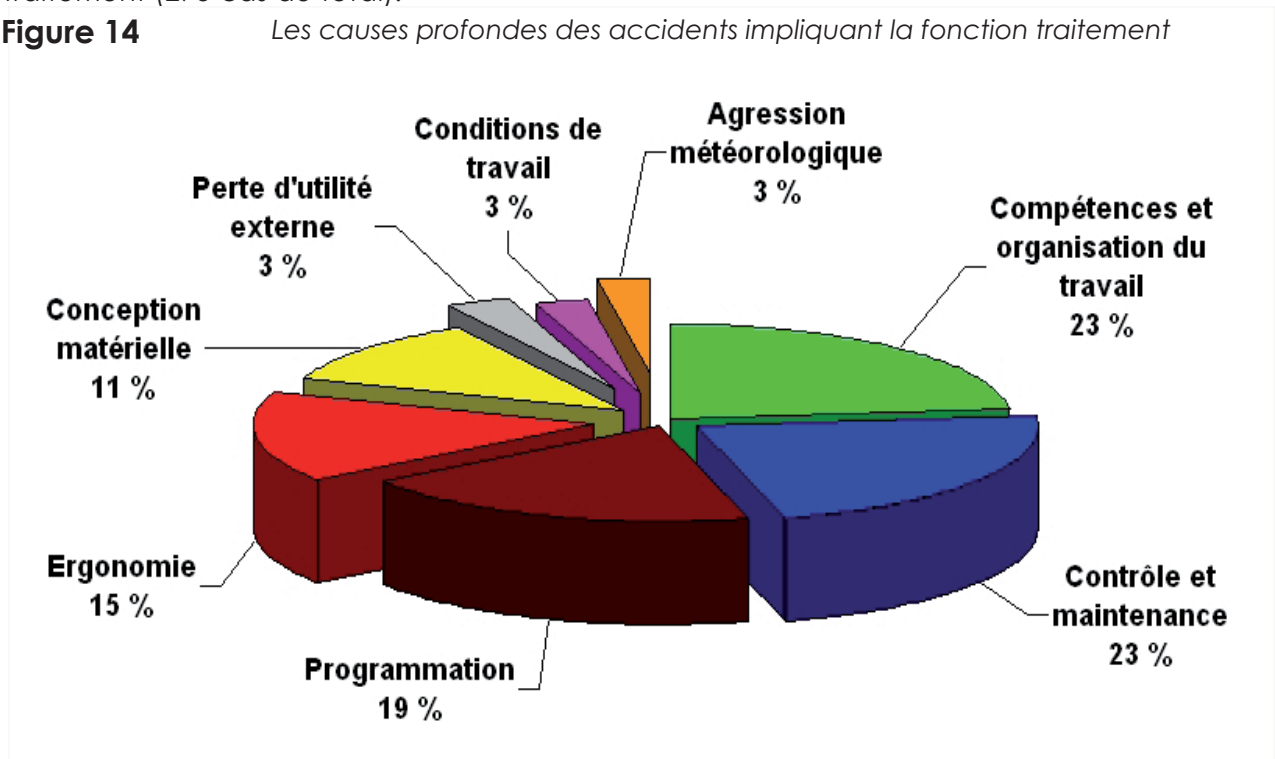
3. Analyse des causes profondes des accidents

L'analyse des causes profondes des accidents impliquant la fonction traitement conduit à les répartir en 8 grandes catégories :

- les problèmes de compétences et d'organisation du travail
- les insuffisances de contrôle et de maintenance des composants matériels
- les défauts de conception logicielle (programmation)
- les défauts d'ergonomie matérielle et des interfaces
- les défauts de conception matérielle
- la perte des utilités externes
- les conditions de travail inadaptées
- les agressions météorologiques

Un accident provoqué par une défaillance (matérielle ou de conduite) de la fonction traitement peut avoir pour origine plusieurs causes profondes (exemple d'un accident avec une défaillance matérielle causée par une insuffisance de maintenance et une erreur de conduite liée à un manque de formation). C'est pourquoi le nombre des causes profondes identifiées et présentées figure 14, soit 314, dépasse le nombre d'accidents avec défaillance de la fonction traitement (275 cas au total).

Figure 14 *Les causes profondes des accidents impliquant la fonction traitement*



Deux groupes de causes contribuant chacune à plus de 10 % de toutes les causes profondes recensées se distinguent à parts égales : le groupe de celles liées aux phases de spécification et de conception de la fonction traitement (conception matérielle, programmation et ergonomie), et le groupe de celles liées aux conditions d'exploitation courantes de l'automate (compétences et organisation du travail, contrôle et maintenance).

Le 1er groupe, lié à la spécification et la conception, représente 45 % des causes profondes (alors qu'il représentait au maximum 31 % des causes d'accidents impliquant des capteurs dans les grands secteurs industriels fortement automatisés [1]). Ce constat confirme que, pour réduire le risque d'accidents de la fonction traitement, qui est le véritable « cerveau de l'automate », il est indispensable de soigner la spécification et la conception de tous ses composants : alimentation, câblage, électronique, logiciels, interfaces de conduite.

Le 2ème groupe est lié aux conditions d'exploitation de l'automate et représente 46 % des causes profondes, alors qu'il représentait de 60 à 90 % des causes d'accidents impliquant des capteurs selon les secteurs industriels [1]. Le fait d'être moins exposé aux environnements des procédés et la prédominance des composants électroniques sur ceux mécaniques pourraient contribuer à réduire les problèmes liés à des défauts de maintenance et de contrôle des composants.

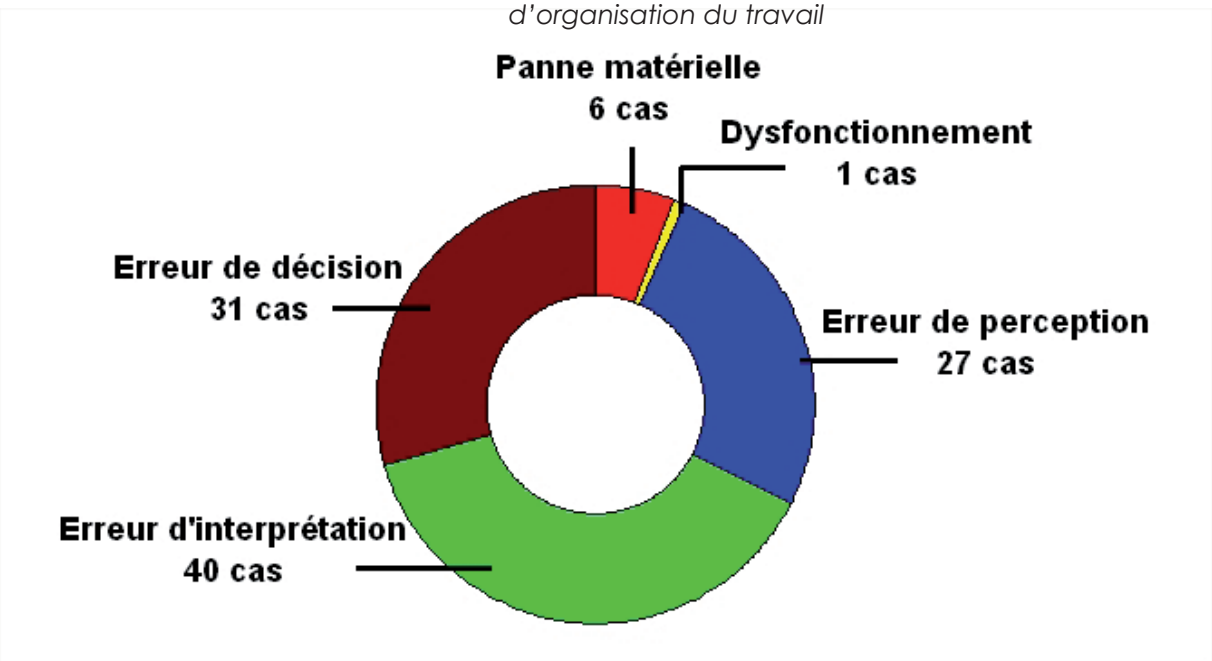
90 % des causes profondes d'accidents de la fonction traitement se répartissent à parts égales entre l'exploitation de l'automate : organisation, contrôles, maintenance et sa conception : choix du matériel, programmation, ergonomie.

3.1 Compétences et organisation du travail

La cause profonde « compétences et organisation du travail » concerne en premier lieu les accidents de traitement provoqués par un manque de formation et d'entraînement des opérateurs de conduite. Ces derniers sont alors souvent amenés à ne pas prêter attention aux informations importantes ou, s'ils les ont bien perçues, à mal les interpréter ou prendre une mauvaise décision en raison d'une maîtrise insuffisante du fonctionnement du procédé et de la signification des paramètres de conduite importants (voir fig. 15 et ARIA 33333 p. 31). D'autre part, une mauvaise organisation du travail peut amener à confier à l'opérateur de conduite des tâches annexes qui le détournent de sa mission principale ou le contraignent à s'absenter de la salle de contrôle, ce qui le conduit à détecter tardivement ou à ne pas détecter des situations anormales (voir ARIA 15018 p.17). L'enquête réalisée par le HSE en 2002 sur 107 sites industriels anglais où la conduite était automatisée montrait que 37 % des salles de contrôle n'étaient pas occupées en permanence ; et que dans 90 % de celles qui l'étaient, le ou les opérateurs de quart la quittaient fréquemment pour effectuer d'autres tâches [5]. Enfin, l'étude nord-américaine menée en 2012 a rappelé le rôle des procédures incomplètes ou mal rédigées dans la survenue d'accidents[15].

Les problèmes de formation des opérateurs et d'organisation de leurs tâches représentent presque 1/4 des causes profondes des accidents de traitement et se traduisent principalement par des erreurs de conduite.

Figure 15 *Les causes premières ayant pour origine des problèmes de compétence et d'organisation du travail*

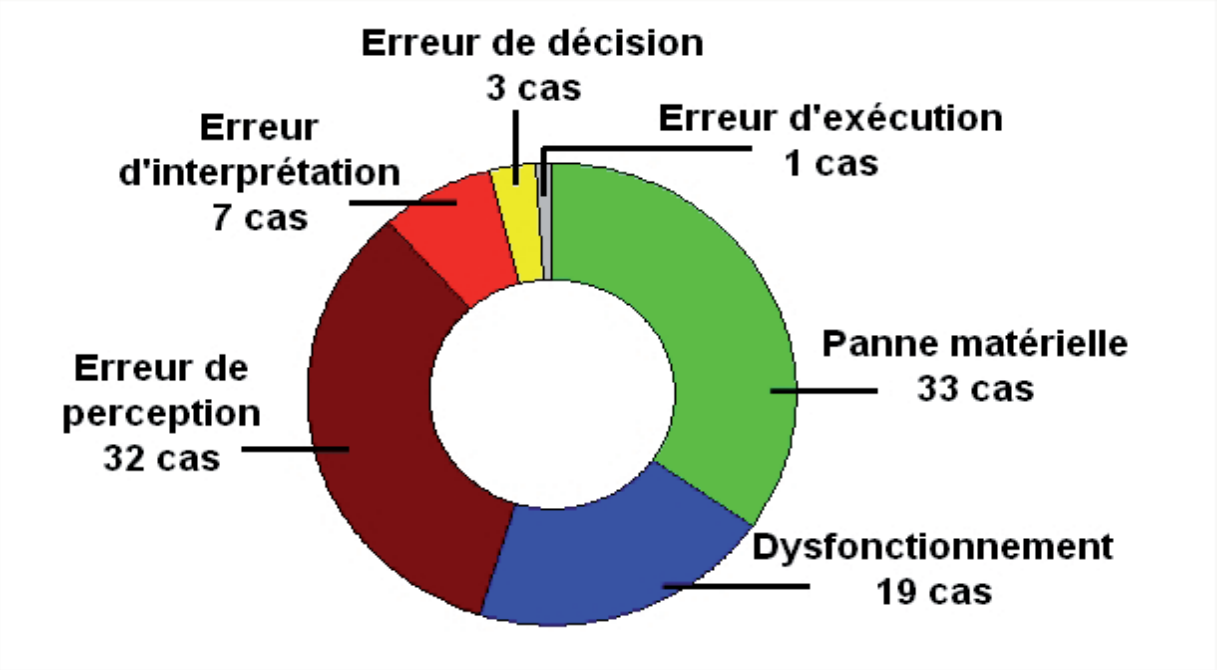


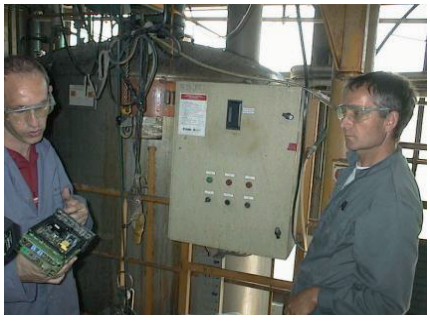
3.2 Contrôle et maintenance

Les insuffisances de contrôle et de maintenance constituent l'autre cause profonde la plus fréquente mais, contrairement aux problèmes de compétence et d'organisation du travail, elles donnent surtout lieu à des défaillances matérielles en provoquant des pannes et dysfonctionnements (fig. 16). Elles peuvent aussi conduire indirectement à des erreurs de conduite quand les paramètres nécessaires à l'opérateur ne sont plus disponibles et qu'il ne peut les percevoir : panne de transmission de données... Cette cause profonde interroge l'efficacité de l'organisation responsable du contrôle et du suivi des composants matériels de l'automate, et souligne la vulnérabilité de la fonction traitement à ce type de défaut organisationnel. Des exemples d'accidents où de telles insuffisances ont été relevées sont présentés page 31 (ARIA 22404 et 40969).

Les défauts de contrôle et maintenance représentent 1/4 des causes profondes, et génèrent essentiellement des défaillances de composants matériels de l'automate et des erreurs de perception.

Figure 16 *Les causes premières ayant pour origine des problèmes de contrôle et de maintenance*





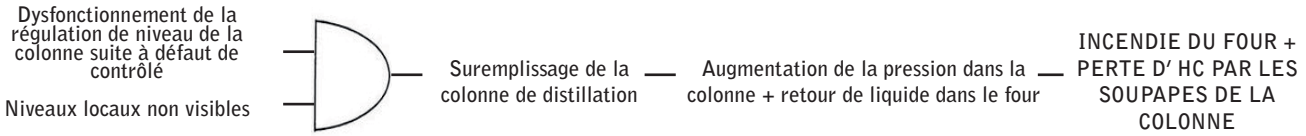
Panne d'une carte d'automate ayant provoqué un accident

COMPÉTENCES ET ORGANISATION DU TRAVAIL (ARIA 33333)
01/10/2005

Dans une raffinerie, un feu se déclare sur un four à la suite d'une rupture de tube. Le système d'arrêt d'urgence est déclenché, l'unité se dépressurise par le tube rompu à l'intérieur du four. Lors de l'incident, l'unité était en phase de retour à son débit nominal. Environ 24 h avant la rupture, à la suite d'un incident, l'unité de reformage a opéré à un débit très bas pendant 3 h. **La sécurité bas débit avait été bipassée sans mise en place de mesures compensatoires. L'information ne fut pas non plus communiquée le lendemain au personnel de jour.** Cette situation anormale conduit un cokage rapide des tubes et accélère leur fluage. L'incendie provient donc d'une surchauffe des tubes liée à un cokage interne, lui-même dû à un fonctionnement à débit insuffisant et est lié à un non-respect des règles de sécurité. L'incident de la veille ayant été sous-évalué, l'équipe suivante a été peu ou pas informée. L'inspection demande le renforcement des règles de gestion des sécurités et la vérification de leur application stricte, la finalisation de la mise en place de la gestion et de la rationalisation des alarmes (« alarm management »). **Elle demande également de formaliser les ressources à alerter en cas d'incident process en dehors des heures ouvrées, de formaliser les règles de gestion des arrêts non planifiés et redémarrages associés, de revoir les règles de réception des tests périodiques des sécurités, de renforcer le programme de formation et de recyclage via l'utilisation de nouveaux outils du groupe, en ciblant notamment les fours et la gestion des incidents.**

VOIR AUSSI Aria 9652, 26880, 30406, 31441, 32109, 32632, 32640, 35432, 38674, 42163, 42920

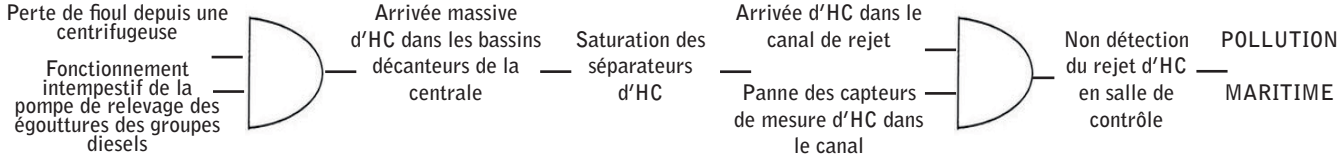
DÉFAUT DE CONTRÔLE (ARIA 22404)
13/08/2009



Un feu se déclare sur l'unité de distillation dans une raffinerie lors de son arrêt. L'unité avait redémarré la veille, après réception des travaux, d'autres chantiers étant encore en cours sur le site. Une remise en chauffe avait été lancée dans la nuit, l'unité était en phase de montée en puissance. Vers 9h15, on observe une épaisse fumée noire à la cheminée (incendie dans le four) et des flammes au niveau des trappes d'explosion qui s'ouvrent. Cette situation est précédée de coups de bélier dans les tuyauteries et d'une montée en pression dans la colonne dont les soupapes s'ouvrent : des hydrocarbures se répandent vers l'extérieur. Après enquête, il s'avère que des indications erronées sur des indicateurs de niveaux ont entraîné un sur-remplissage de la colonne puis le retour de liquide dans le four par le circuit de mise sous vide (reflux des incondensables). Les niveaux locaux n'étaient pas lisibles, **la chaîne associée aux niveaux de régulation du fond de colonne n'avait pas été complètement vérifiée (carte),** la configuration du circuit, notamment des niveaux de soutirage, n'était pas correcte.

VOIR AUSSI Aria 7577, 16213, 18051, 29722, 31441, 34923, 36660, 37525, 42557

DÉFAUT DE MAINTENANCE (ARIA 40969)
22/09/2011



A 6 h, l'équipe de quart d'une centrale électrique thermique détecte des hydrocarbures dans le canal de rejet à la mer. Le chargé d'exploitation ordonne la fermeture des vannes de la partie aval du canal pour contenir la pollution. La pompe de relevage d'un puisard de récupération des égouttures des groupes diesel ne s'est pas arrêtée à son niveau bas, continuant à fonctionner jusqu'à son débrochage par les agents de quart. Une centrifugeuse a également dysfonctionné et rejeté massivement du fioul. Ces deux avaries ont entraîné une arrivée massive d'hydrocarbures dans les bassins décanteurs dont les séparateurs ont été saturés, laissant s'écouler des polluants vers les bassins de traitement et dans le canal de rejet. **Aucune anomalie n'a été détectée en salle de commande car les 2 cabines de surveillance par mesure en continu des teneurs d'hydrocarbures dans le canal de rejet étaient inopérantes depuis le 15/09**.L'exploitant remet en état les équipements défectueux, effectue un audit de l'installation de traitement des eaux industrielles et sensibilise l'ensemble de son personnel.

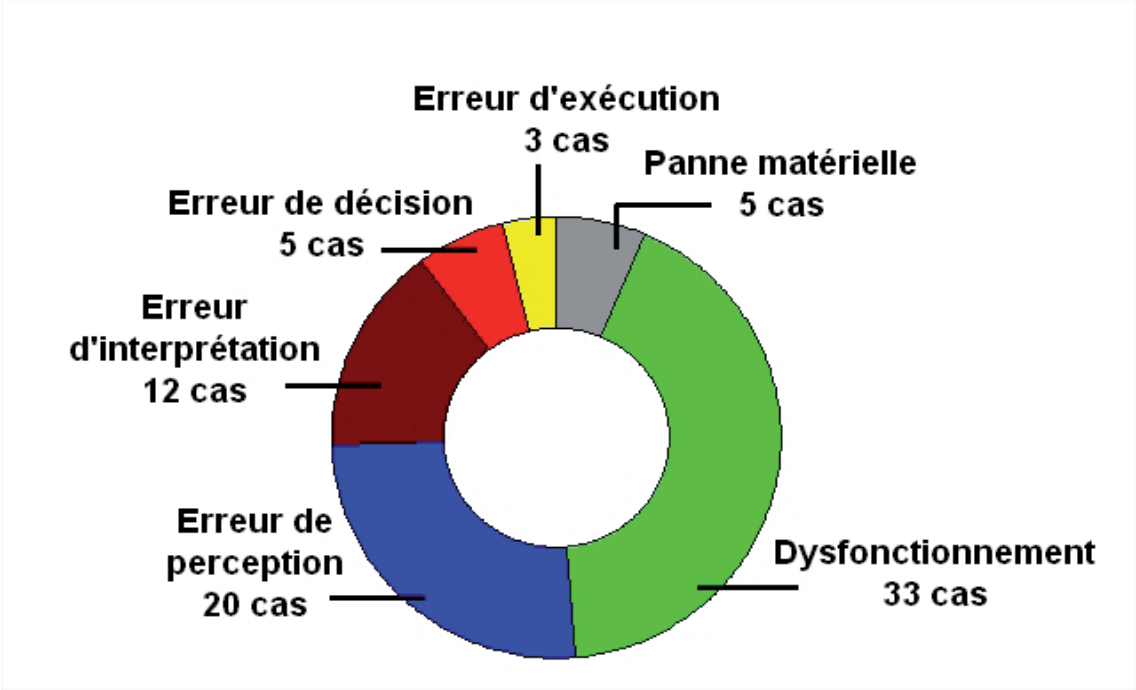
VOIR AUSSI Aria 6645, 14247, 26895, 34319, 35774, 36193, 41541, 42235, 42931

3.3 Programmation

Si la programmation est au cœur de la performance d'un système automatisé, c'est aussi un domaine que les exploitants ont plus de mal à maîtriser en interne, tant au niveau de la spécification et de la conception (ce n'est pas leur cœur de métier technique) que de l'entretien (mise à jour et modification des codes nécessitant un savoir-faire rarement disponible en interne).
Les erreurs de programmation donnent lieu à parts égales à des défaillances matérielles - plutôt des dysfonctionnements que des pannes - et des erreurs de conduites surtout liées à des problèmes de perception et d'interprétation (fig. 17).

Les défauts de programmation représentent 20 % des causes profondes d'accidents de traitement ; ils provoquent aussi bien des défaillances matérielles de l'automate que des erreurs de l'opérateur de conduite.

Figure 17 *Les causes premières ayant pour origine des défauts de programmation*



Certaines défaillances matérielles découlent parfois d'erreurs imputables au seul programmeur : bug informatique, séquence d'activation sur le mauvais équipement, saisie de seuils d'activation erronés, action programmée inverse de celle demandée, etc. Cependant, les défaillances matérielles et les erreurs de conduite provoquées par des défauts de programmation ont souvent pour origine une mauvaise compréhension du cahier des charges ou une connaissance incomplète des particularités et des risques du procédé par les prestataires choisis pour la spécification et la programmation de l'automate : situations non prévues, traitement d'infor-

PAROLES DE TERRAIN

« On nous a demandé de modifier en catastrophe et on a voulu fabriquer trop vite. On nous a demandé de modifier les recettes en produisant alors qu'il aurait fallu arrêter ».

Témoignage d'un technicien à l'occasion de la modification d'un automate [6]

mations contradictoires, oubli de certains paramètres de conduite, pas de remontée d'alarmes vers la fonction traitement, activation inappropriée de certains équipements dans des circonstances particulières (mauvaise position de vanne, pompes créant des coups de bélier, seuils d'alarme inadaptés, voir les exemples p. 34 et ARIA 42690 p. 38*)*. Par ailleurs, des contraintes productives peuvent amener à abréger les phases de validation souvent longues et complexes et à ne pas détecter ces erreurs de programmation (voir ARIA 36437 p. 34).

En phase de spécification et de conception, il semble essentiel de prévoir des temps d'échange entre la direction, les chef d'ateliers, les opérateurs de conduite et le programmeur « extérieur » pour que celui-ci comprenne bien le principe de fonctionnement attendu de l'automate et les particularités du procédé. Etant donné l'importance de l'automate dans la conduite et la sécurité du procédé, il est aussi nécessaire de prévoir du temps pour tester l'automate après toute modification, surtout pour les séquences inhabituelles de fonctionnement telles que les mises à l'arrêt, les démarrages et les fonctionnements en mode dégradé.

En phase d'exploitation, un degré d'intervention sur la programmation de l'automate est souvent laissé à l'opérateur de conduite. Il est important de bien évaluer ce degré, car il peut aussi pousser l'opérateur à des erreurs de conduite :

- Trop important, l'opérateur pourra librement modifier le paramétrage de l'automate et shunter - par confort ou maladresse - des seuils importants pour la sécurité ou la qualité du procédé, tels que des alarmes (voir ARIA 37139 p. 25).

PAROLES DE TERRAIN

« Du point de vue de l'encadrement, ce système était trop ouvert, trop dangereux… les opérateurs sont embêtés parce qu'ils ont pris de mauvaises habitudes, et je ne sais pas s 'ils connaissent les conséquences potentielles en cas d'erreur ».

Témoignage d'un responsable d'atelier à l'occasion du remplacement d'un automate [6]

- Trop restrictif, l'opérateur ne pourra pas rattraper un incident en exploitant pleinement son expérience et ses capacités de jugement, car il devra agir selon les règles de fonctionnement et les délais imposées par l'automate qui ne sont pas toujours adaptés à la cinétique et aux spécificités de la situation anormale en cours (voir ARIA 38617 p. 27*)*.

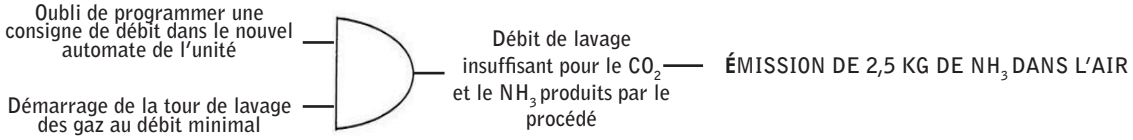
PAROLES DE TERRAIN

« C'est le système qui prend le contrôle, tandis qu'avant on by-passait quelques équipements et on s'organisait pour reprendre en main la situation ».

Témoignage d'un opérateur de raffinerie [8]

Programmation d'un automate (source : Control Engineering Asia)

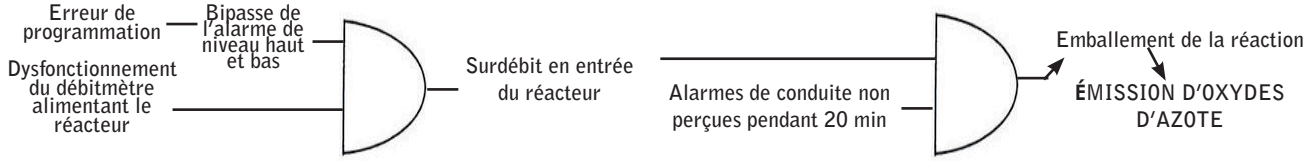
PROGRAMMATION INCOMPLÈTE (ARIA 36437)
03/07/2009



Dans une usine chimique classée Seveso, environ 2,5 kg d'ammoniac sont émis à l'atmosphère vers 13h15 à la suite du dysfonctionnement d'un laveur de gaz, provoquant une nuisance olfactive. Une personne extérieure à l'établissement donne l'alerte. L'appareil est stoppé puis remis en service. Aucune personne n'est incommodée et la production n'est pas perturbée. **L' incident est survenu à la suite du changement de système de conduite du procédé. En effet, la consigne de débit des eaux salées utilisées dans le laveur de gaz de la tour de carbonatation n'a pas été reprise dans le nouveau système.** A la mise en service de celui-ci, le débit d'eau salée s'est calé à son niveau minimal correspondant au niveau de fonctionnement nominal de l'atelier. Compte tenu de la production en cours, ce débit était insuffisant pour un lavage complet des gaz (CO_2 et NH_3) d'où l'émission d'NH_3.

VOIR AUSSI Aria 11181, 16080, 23589, 25057, 25204, 36437, 42921

PROGRAMMATION INADAPTÉE (ARIA 21994)
19/02/2002

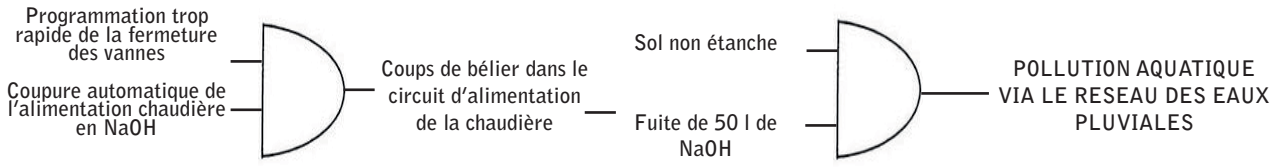


Une émission d'oxydes d'azote (NOx) dans une usine chimique génère un nuage roux qui se déplace sur le site avant de se dissiper en présence d'un vent fort. Ce rejet de NOx a pour origine une valeur erronée donnée par un débitmètre placé sur la ligne d'alimentation en acide nitrique de l'un des réacteurs d'un atelier de fabrication d'acide glyoxylique. D'autres dysfonctionnements concomitants sont également observés. Ainsi, **à la suite d'une erreur de programmation, le bipasse d'une alarme de niveau bas entraînait également le bipasse de l'alarme de niveau haut, débit supérieur à la plage de mesure du débimètre**. Enfin, l'opérateur n'a pas vu 3 ou 4 alarmes durant 20 min de conduite des installations. Ces différentes défaillances ont provoqué l'ouverture d'une vanne sur la ligne de production alors qu'elle aurait dû se fermer, la quantité d'acide nitrique dans le réacteur étant suffisante à ce moment de la réaction. Cette dernière étant exothermique, le réacteur est monté en température déclenchant une dilution du milieu réactionnel à l'eau et la mise en sécurité de l'appareil : vidange du réacteur dans une capacité à pression atmosphérique vide prévue à cet effet et dégazage de celle-ci. Aucun blessé n'est à déplorer. Tous les débitmètres de l'atelier sont vérifiés.

VOIR AUSSI

Programmation des alarmes absente ou inadaptée :	Aria 12671, 21994, 28389, 30178, 31376, 32632, 37825, 42628, 42690, 43455
Séquence de fonctionnement inadaptée à la situation en cours :	Aria 13297, 25057, 26199, 31150, 37041, 39384
Position inadaptée des équipements pilotés :	Aria 16080, 18563, 31307, 42920, 43271

PROGRAMMATION ACCIDENTOGÈNE (ARIA 28911)
21/09/2004



Une fuite de 50 l de soude (NaOH) se produit sur l'alimentation de l'unité de déminéralisation d'une chaudière dans une usine de fabrication de colles. Le sol détérioré sous les colonnes de déminéralisation facilite l'écoulement des eaux de lavage chargées de soude dans un ancien réseau pluvial se rejetant dans la SORGUE. L'élévation du pH provoque la précipitation du carbonate de calcium, entraînant un important trouble blanchâtre de la rivière. Ce dernier disparaît 1 h plus tard. **L'entreprise prévoit** la réfection et l'étanchéification du sol de l'unité, la réparation de la tuyauterie, **la modification du programme de l'automate pour éviter les coups de bélier lors de la fermeture des vannes et une réduction de la temporisation de discordance.**

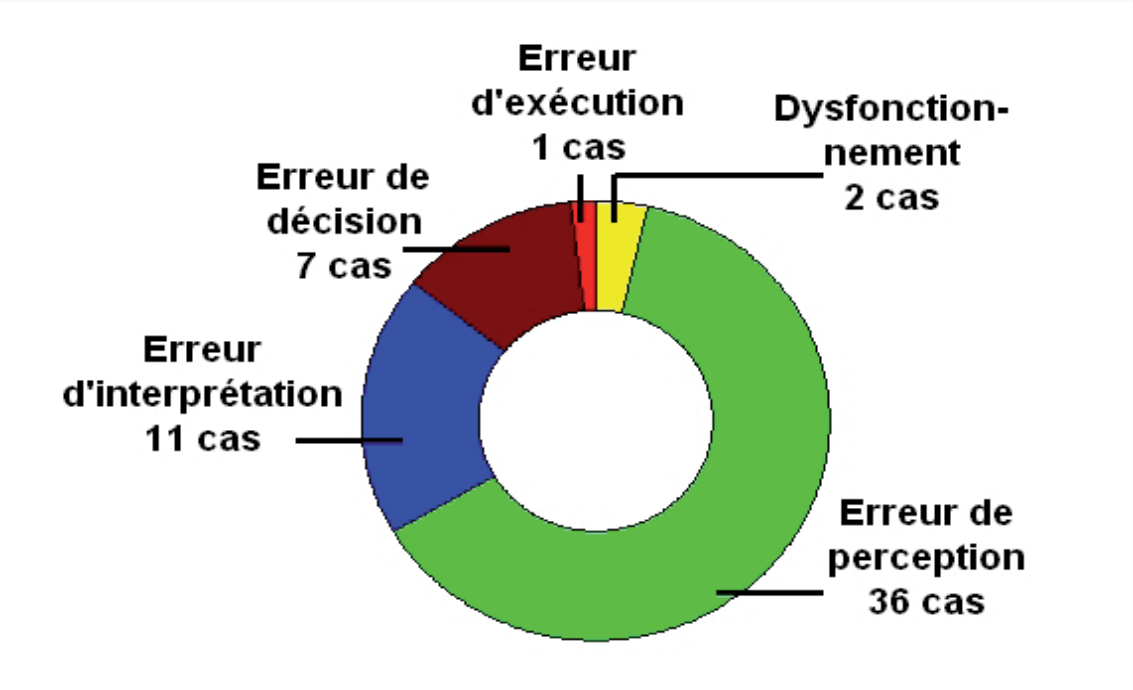
VOIR AUSSI Aria 5989, 16072, 28911, 30417, 32109, 31691, 40522, 41736, 42038, 42921

3.4 Ergonomie matérielle et des interfaces

Etant donné le rôle fondamental joué par l'opérateur de conduite dans la fonction traitement, l'ergonomie constitue logiquement une cause profonde d'accident non négligeable, essentiellement impliquée dans les erreurs de conduite (fig. 18). Si les défauts d'ergonomie concernent majoritairement des erreurs de perception en raison de paramètres importants non visibles, d'alarmes de conduite ou de sécurité inaudibles ou noyées dans des bandeaux d'affichage, de surcharges d'alarmes, etc. (voir ARIA 40584 p. 22), elles sont aussi la source d'erreurs d'interprétation et de décision (voir ARIA 23893 p. 38) et parfois même d'exécution (voir ARIA 33334 p. 27). Enfin, quelques accidents provoqués par un dysfonctionnement ont pour cause profonde un défaut plus rare d'ergonomie matérielle (voir ARIA 27903 p. 38).

Les défauts d'ergonomie se traduisent par des erreurs de conduite qui soulignent le rôle essentiel de la supervision humaine et l'intérêt du soin à apporter à l'ergonomie des interfaces hommes-machines.

Figure 18 *Les causes premières ayant pour origine des défauts d'ergonomie*



Trop souvent, les prescripteurs et les concepteurs d'automates industriels se focalisent sur la performance technique ou économique du système automatisé sans se préoccuper suffisamment de la façon et des conditions dans lesquelles l'opérateur de conduite va l'utiliser. Ce dernier devra ensuite « faire avec » et compenser au quotidien les défauts ergonomiques des interfaces et commandes de l'automate, au prix d'efforts d'attention supplémentaires, avec le risque de favoriser un accident le jour où cette attention se relâche.

PAROLES DE TERRAIN

« La place de l'homme dans la conduite étant sous-estimée, les fonctions dévolues à l'imagerie le sont également ».

« Cette maquette a été sévèrement critiquée par les opérateurs de conduite... leur point de vue n'avait pas été intégré dans cette première version des IHM ».

Témoignages d'ergonomes industriels [16 et 17]

Une étude menée en 1991 sur l'ergonomie de 5 salles de contrôles de sites industriels français dans 3 secteurs d'activité (agroalimentaire, papeterie, extraction minière) a montré la récurrence de plusieurs défauts [16] :

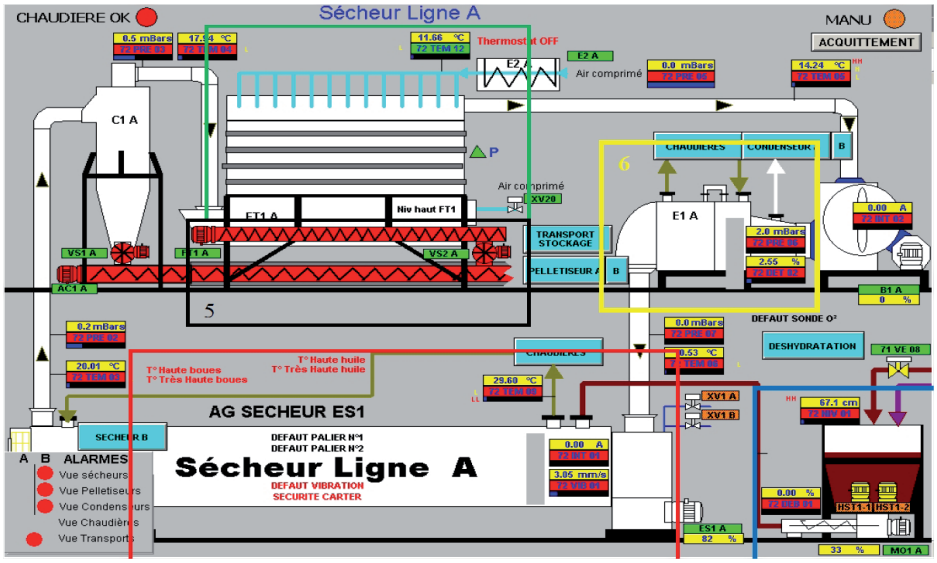
- interfaces conçues pour un fonctionnement normal, mais inadaptées aux situations anormales (pas de vue élémentaire des défauts d'équipements, accès aux informations critiques trop lent...) ;
- écrans saturés par des images synoptiques, surcharge d'informations affichées dont certaines sont caduques ou inutiles pour la phase en cours ;
- peu ou pas d'animation des images synoptiques (ex : remplissage d'un réservoir, ouverture de vanne) ;
- peu de retour (*feedback*) renseignant les opérateurs sur le résultat de leurs actions ;
- pas de représentation de l'état des équipements conduits manuellement malgré leur importance dans le procédé ;
- représentation graphique des équipements non cohérente avec leur taille relative ou leur localisation dans l'unité, utilisation de couleurs illogiques par rapport à l'état du procédé et des équipements.

PAROLES DE TERRAIN

« Ignorée lors du processus d'achat, et tardivement prise en compte lors de l'installation du SNCC, la conception de l'imagerie est assez souvent bâclée par les installateurs, ceux–ci étant entièrement mobilisés par l'échéance du démarrage, sur laquelle plane l'ombre des pénalités de retard ».

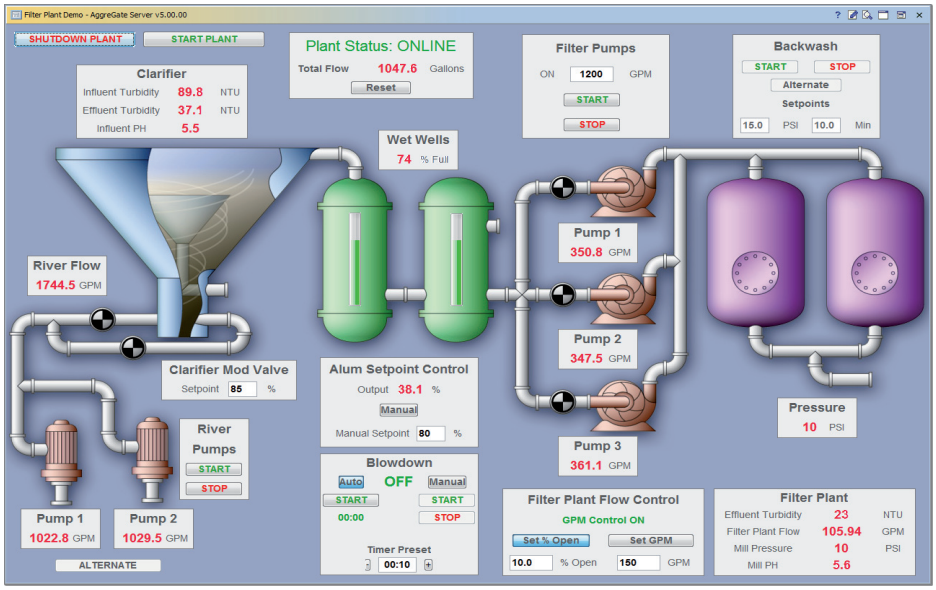
Témoignage d'un ergonome industriel [16]

Evolution des salles de contrôle des procédés industriels depuis les années 1960

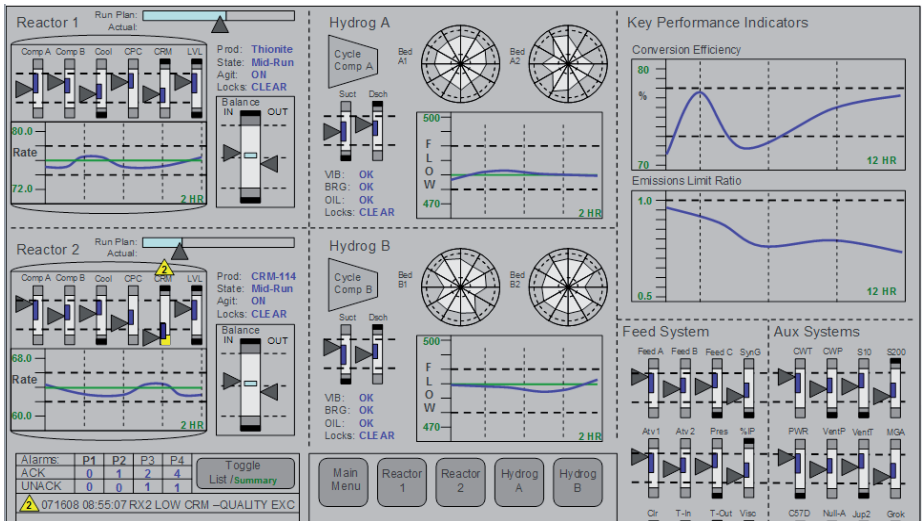


Exemples illustrant l'importance de l'ergonomie des interfaces de conduite

Interface surchargée, les données d'état sont peu lisibles, le fonctionnement de l'unité est difficile à comprendre et les couleurs vives fatiguent la vision de l'opérateur. Cette interface est à l'origine de la non détection d'une situation accidentelle par un opérateur (Aria 42156).

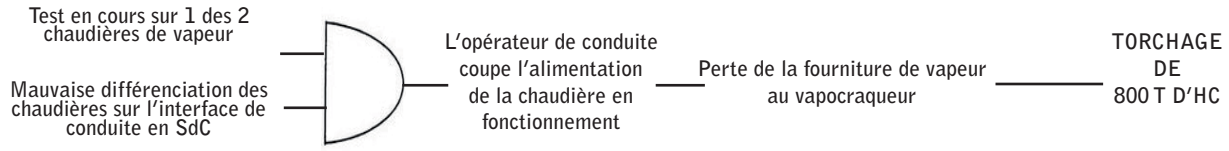


Interface plus sobre, le fonctionnement de l'unité est plus compréhensible et les changements d'état sont clairement signalés (couleur et On / Off), mais la compréhension des valeurs affichées est perfectible (détection des dérives).



Bonne ergonomie des interfaces, les valeurs sont représentées dans leur plage normale de fonctionnement et avec un historique temporel, ce qui facilite la détection de situations anormales ; les couleurs vives sont réservées aux alarmes graphiques qui sont priorisées, seules les données relatives aux équipements importants et aux phases en cours sont affichées en permanence (extrait de « *The high performance HMI handbook* »).

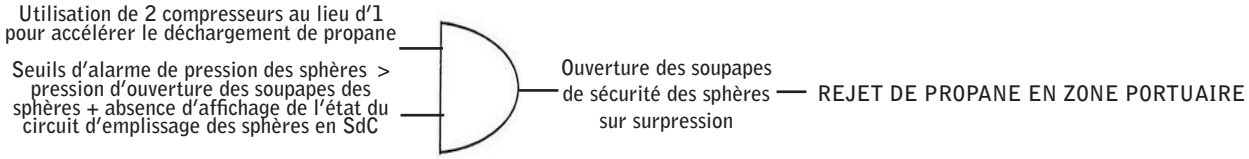
INTERFACES CONFUSES (ARIA 23893)
09/11/2002



Dans une unité pétrochimique, un problème de fourniture de vapeur au niveau de la centrale de production de vapeur du site provoque le déclenchement du compresseur des gaz craqués. Le vapocraqueur est aussitôt passé en repli et les gaz sont acheminés dans le réseau torche, entraînant le brûlage sur la torche de l'unité de 800 t d'un mélange d'hydrocarbures entre le samedi soir et le dimanche en fin d'après-midi. La fourniture de vapeur de l'unité est assurée par 2 chaudières, l'une assurant le secours de l'autre. Lors de l'incident, l'une des 2 chaudières était à l'arrêt pour maintenance, une seule chaudière restait donc en service. La chaudière à l'arrêt faisait l'objet de nombreux tests de sécurité, dont un qui prévoyait la fermeture de la vanne d'alimentation. **La personne réalisant l'essai a, par erreur, fermé la vanne d'alimentation en combustible de la chaudière en service, depuis les pupitres de commande,** provoquant une baisse importante et brutale de fourniture vapeur aux unités. Le vapocraqueur étant aussitôt passé en repli, les installations sont dégazées et le réseau torche utilisé en secours pour le brûlage des hydrocarbures. Afin de réduire ce type d'erreur, **l'exploitant améliore la différenciation des chaudières sur ses interfaces graphiques en salle de commande.**

VOIR AUSSI Aria 10131, 25216, 35432, 33516, 36722, 41207, 42156

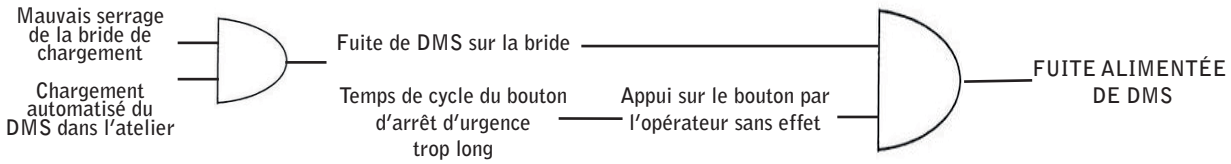
PARAMÈTRES DE CONDUITE NON PRÉVUS (ARIA 42690)
11/08/2012



Un navire de propane décharge à 6h55 sa cargaison dans 2 sphères sous-talus d'une société classée Seveso. A 20h50, le déchargement de la phase liquide s'achève et les pompes du propanier sont arrêtées. Le déchargement de la phase gazeuse via les compresseurs du bateau débute quelques minutes plus tard. A 21h35, les 2 soupapes de l'une des sphères s'ouvrent à leur seuil de tarage (10,9 bar) pendant 30 secondes. Le pompiste de surveillance arrête le transfert et interconnecte les 2 sphères pour baisser la pression qui s'équilibre à 9,8 bar. Le chef de centre et le responsable du navire décident l'arrêt du déchargement et une surveillance de la pression des 2 réservoirs est mise en place toutes les demi-heures. Selon l'exploitant, la montée en pression de la sphère de 9,2 à 10,9 bar en 35 minutes serait due à l'utilisation simultanée des 2 compresseurs du propanier pour accélérer le déchargement. Le contrôle des installations montre que les seuils d'alarme de pression de la sphère étaient réglés à une valeur supérieure à la pression de tarage des soupapes. **A la suite de l'incident, les niveaux de pré-alarme (visuel et sonore) et d'alarme des sphères sont respectivement tarés à 10,4 et 10,7 bar**, valeurs inférieures au seuil de déclenchement des soupapes. **La bonne fermeture de la vanne d'emplissage de la sphère et de l'ouverture de la vanne de barbotage sont affichées sur le synoptique de supervision.**

VOIR AUSSI Aria 2900, 13850, 14619, 19533, 23231, 33333, 37139, 34597, 40993, 42746

ERGONOMIE MATÉRIELLE (ARIA 39900)
28/01/2009



Une fuite de sulfate de diméthyle (DMS) se produit vers 11 h dans une usine chimique lors de son chargement. La connexion du conteneur de DMS au poste de chargement consiste à démonter les brides pleines, remplacer le joint par un neuf et à reconnecter les brides du conteneur aux brides de canalisations de l'atelier. Après avoir lancé le chargement de DMS en salle de contrôle, l'opérateur descend vérifier le conteneur et identifie une fuite sur la bride de liaison entre le conteneur et la canalisation de chargement. Il déclenche la sirène et le gyrophare d'alerte, puis appuie sur le bouton d'arrêt d'urgence... Le lendemain, l'exploitant conclut que la fuite est due à un mauvais serrage de la bride de chargement lors de la connexion du conteneur au poste de chargement. De plus, **l'automate d'arrêt d'urgence ne s'est pas déclenché car l'impulsion donnée sur le bouton poussoir a été trop brève par rapport au temps de cycle de celui-ci (1/10e de seconde). Les boutons poussoirs des arrêts d'urgence sont remplacés par des boutons à enclenchement sur l'ensemble du site.**

VOIR AUSSI Aria 3536, 27903, 33334, 42077

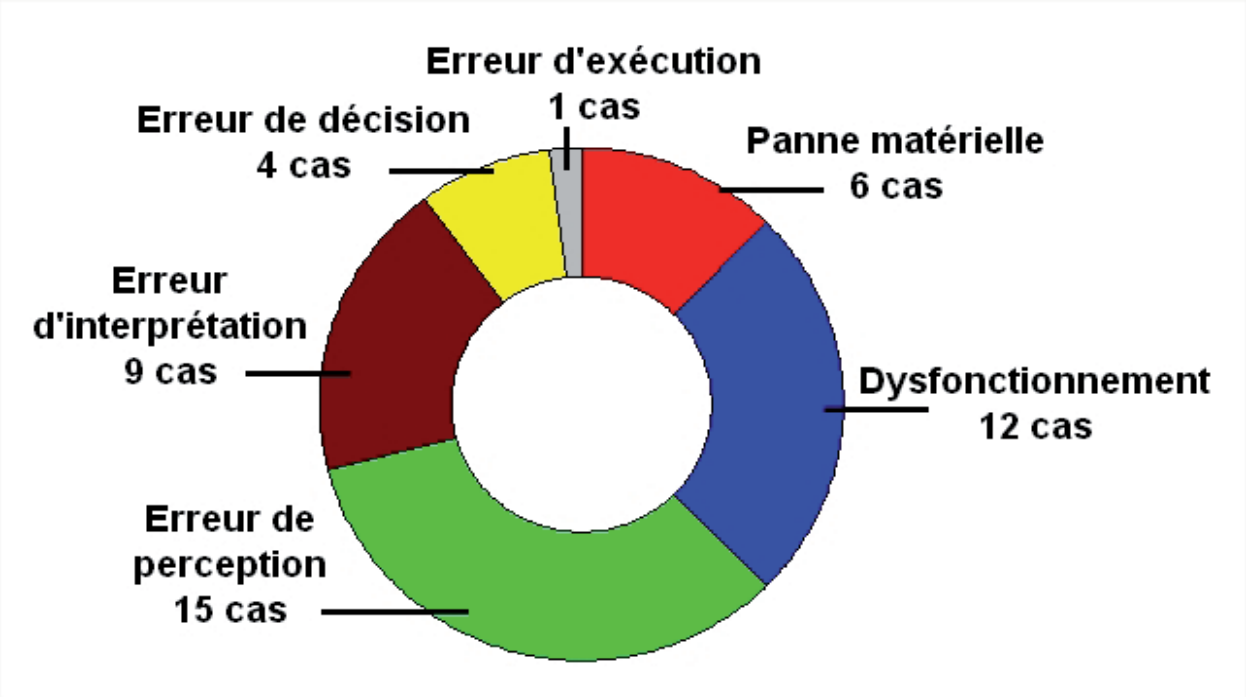
3.5 Conception matérielle

Les défauts de conception matérielle restent l'une des principales causes profondes identifiées des accidents de traitement (fig. 14 p. 28). Ils concernent aussi bien l'installation de nouveaux automates que la modification d'automates existants (voir ARIA 38676 p. 41). L'automatisation d'un procédé, surtout quand il est complexe ou polyvalent comme dans le secteur de la chimie fine et de la pharmacie, suppose d'avoir étudié en détail les différents scénarios de fonctionnement et de dysfonctionnement les plus probables et les plus graves. Bien que des méthodologies adaptées à ce genre d'études existent depuis longtemps, comme les méthodes AMDEC, HAZOP ou LOPA, les accidents de traitement étudiés font trop souvent ressortir que des situations inhabituelles comme les phases transitoires, les redémarrages ou arrêts d'urgence ont été mal prises en compte lors de la phase de conception. En particulier, il est fréquent que les séquences de mise en sécurité d'un procédé automatisé transforment un simple incident technique en un accident grave (voir ARIA 32109 p. 22).

Les défauts de conception matérielle restent une cause profonde significative d'accidents de traitement, tant au niveau des défaillances matérielles que des erreurs de conduite. Elles sont par contre plus difficiles à détecter et à prévenir une fois l'automate en service.

Contrairement aux problèmes de conception dans les accidents impliquant des capteurs [1], les défauts de conception matérielle se traduisent surtout par des dysfonctionnements et des erreurs de conduite mais rarement par des pannes franches (voir fig. 19 et ARIA 31691 p. 41). Ce constat montre que les défauts de conception sont des causes profondes d'accidents difficiles à détecter une fois l'automate en exploitation, et qui souvent ne se révèlent qu'une fois la situation anormale enclenchée. Il semble donc important de les prévenir en amont par un processus rigoureux de spécification et de conception.

Figure 19 *Les causes premières ayant pour origine des défauts de conception matérielle*



Des accidents surviennent aussi après des modifications, en particulier quand un système automatisé remplace un système manuel ou coexiste avec lui alors que les interactions entre les deux « hors marche normale » sont mal identifiées (voir ARIA 21466 p. 41). Une mauvaise conception crée aussi des défaillances de mode commun en cas de panne, quand le même automate pilote le système de conduite et celui de sécurité, quand la panne de l'automate redondant se propage à l'automate principal ou encore quand la perte d'alimentation électrique neutralise également l'automate de secours qui ne peut plus mettre le procédé en sécurité ou empêcher/détecter le développement d'un accident (voir ARIA 38676 p. 41). La panne est d'autant plus grave que les opérateurs n'ont plus aucun moyen d'apprécier correctement l'état réel du procédé ou d'actionner des systèmes de sécurité (voir ARIA 38485 p. 14) et doivent agir à l'aveugle (voir ARIA 12671 p. 43).

« Les ordinateurs n'amènent pas de nouveaux types d'erreurs. Ils amènent des occasions nouvelles et plus faciles de refaire les vieilles erreurs.»

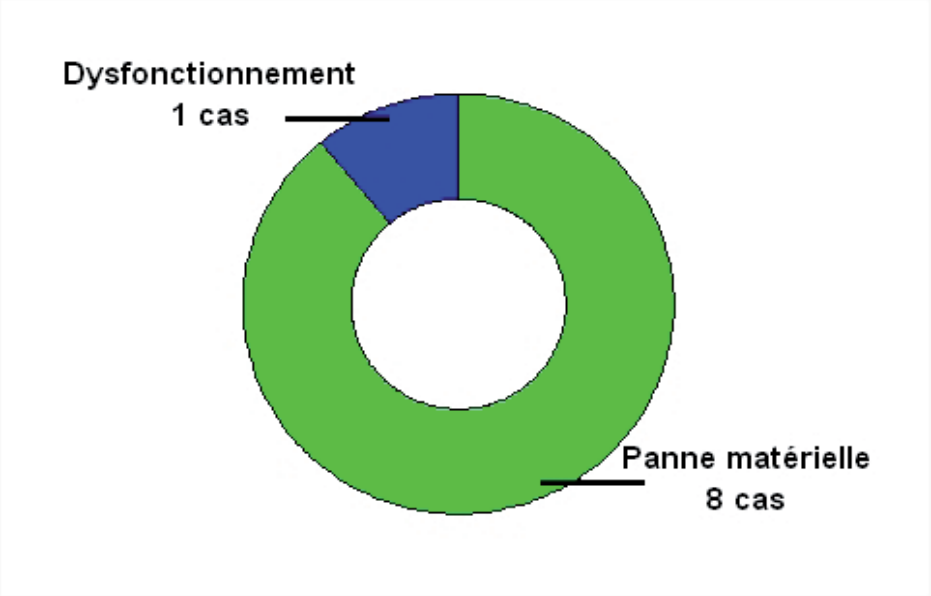
Trevor KLETZ - ingénieur chimiste et expert anglais de la sécurité industrielle - « Wise after the event »

3.6 Perte d'utilité externe

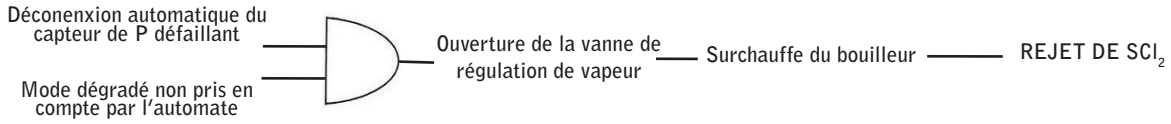
La perte d'utilité fournie par le réseau électrique apparaît comme une cause profonde d'accident assez marginale pour la fonction traitement, plutôt à l'origine de pannes franches de l'automate que de dysfonctionnements (fig. 14 p. 28 et fig. 20). L'automate étant souvent identifié comme un équipement stratégique pour la production et la sécurité, des alimentations de secours ou redondantes sont généralement prévues pour garder la conduite fonctionnelle le temps nécessaire à la mise en sécurité des équipements du procédé. Les quelques cas d'accident répertoriés dans cette étude relèvent de phénomène plus rares, comme des effets dominos à la suite de la défaillance d'autres équipements (voir ARIA 28416 p. 43).

La perte d'utilité est une cause profonde assez rare, traduisant sans doute un bon niveau de protection des systèmes automatisés.

Figure 20 *Les causes premières ayant pour origine des pertes d'utilité électrique*



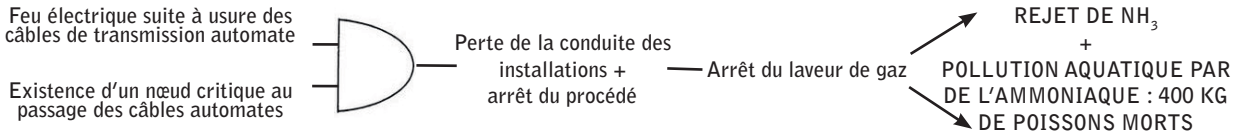
DÉFAUT DE CONCEPTION (ARIA 31691)
26/04/2006



Dans une usine chimique, une fuite de bichlorure de soufre sur une canalisation équipant le bouilleur d'une colonne de distillation s'hydrolyse produisant une forte émission de chlorure d'hydrogène (HCl). Une concentration de 50 ppm en HCl est mesurée dans le bâtiment. Les pertes d'exploitation internes liées aux 18 jours d'arrêt de l'unité de synthèse en aval sont évaluées à 270 keuros. L'accident a lieu lors de la maintenance d'un capteur de pression. Celui-ci a été diagnostiqué défaillant après avoir indiqué une pression de 108 mbar en sortie de bouilleur, déclenchant la fermeture de la vanne d'alimentation SCl_2 et de la vanne de régulation vapeur du système de chauffage du bouilleur. Le capteur n'étant pas à sécurité positive, sa déconnexion électrique provoque l'ouverture de la vanne de régulation de vapeur et le chauffage du bouilleur dont la température passera de 24 à 120°C en 30 min, entraînant l'émission de SCl_2. Les mesures prises au titre du retour d'expérience concernent notamment la mise en place d'une boucle à sécurité positive indépendante de la régulation interdisant tout redémarrage automatique après franchissement du seuil de pression haute... **Au-delà, cet accident montre qu'un système de régulation d'un procédé ne constitue aucunement un système de sécurité et ne peut être retenu comme tel. En particulier, les automates programmables de production répondent à une logique et des critères qui ne sont pas tous connus des équipes d'intervention et qui ne prennent pas forcément en compte modes dégradés et situations de consignation.**

VOIR AUSSI Aria 18563, 27060, 28389, 32640, 40986

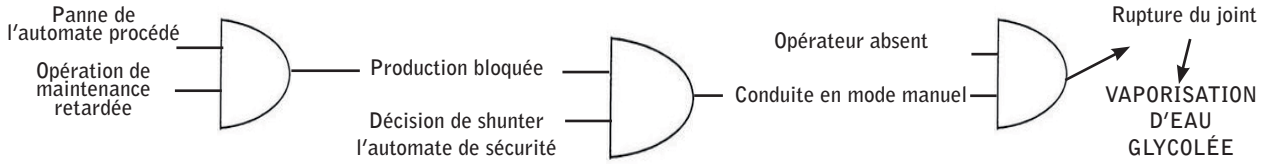
MODE COMMUN DE DÉFAILLANCE (ARIA 38676)
24/07/2010



Dans un établissement produisant du carbonate et du bicarbonate de sodium, un feu se déclare à 7 h dans une armoire électrique regroupant les câbles de transmission des automates de commande de la partie liquide du procédé. L'incendie entraîne une perte complète des commandes pendant 2 h et l'arrêt du process à l'origine d'une émission de 2 à 8 kg d'ammoniac (NH_3) gazeux à l'atmosphère à la suite de l'arrêt brutal du laveur des gaz et une émission d'eaux ammoniaquées dans le bassin de rétention des pollutions accidentelles de l'usine à la suite du refoulement d'un bac de saumure ; ces eaux sont rejetées à la MEURTHE en raison de la perte de maîtrise des installations de contrôle et de pilotage du bassin de rétention. Ce rejet est à l'origine d'une mortalité de 400 kg de poissons. Selon l'exploitant, un échauffement des câbles électriques serait à l'origine de l'événement. Cet échauffement serait dû à une perte d'isolation de ceux-ci par usure. **Le système de commande, constitué par des postes de commandes, un bus de liaison, et des automates chargés de piloter le procédé, disposait d'un point critique sous forme de « nœud », existant depuis la création du 1er système de commande du site (26 ans auparavant), par lequel passent les différents câbles des automates. Alors que les alimentations des équipements électriques sont par ailleurs toutes redondantes, tous les câbles de commande passent dans une seule et même goulotte dans l'armoire électrique.**

VOIR AUSSI Aria 3536, 11665, 36660, 36767, 41305, 42557

COEXISTENCE CONDUITE MANUELLE ET AUTOMATIQUE (ARIA 21466)
12/09/2000



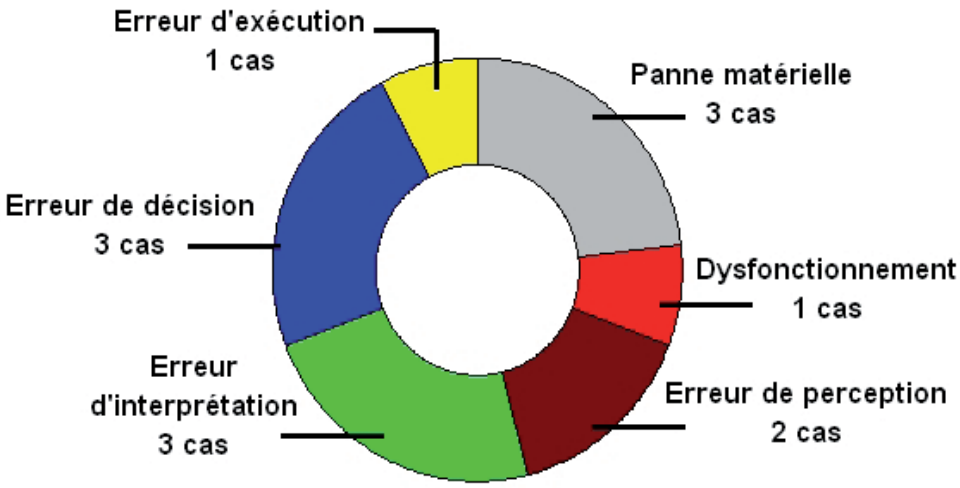
Une fuite d'eau glycolée a lieu sur un site chimique après rupture d'un joint sur une conduite. Un opérateur note à 2 h une baisse de température du caloporteur (150 °C) empêchant de poursuivre des opérations de séchage sous vide. L'astreinte diagnostique une perte de communication entre l'automate des utilités et le système de conduite (SNCC) de l'atelier. Un spécialiste du SNCC confirme la défaillance d'une carte sur l'automate utilités dont le remplacement est reporté au **lendemain matin. Le spécialiste parti et croyant bien faire, le technicien d'astreinte décide de relancer l'ensemble. Il court-circuite toutes les sécurités concernant le fluide chaud scrutées par le superviseur et reprend en manuel les régulations correspondantes.** Appelé par un autre atelier 1 h plus tard, il s'absente 30 min. A son retour, le fluide chaud dépasse 180 °C et un bruit semblable à une détonation retentit dans l'atelier. Après rupture du joint, l'eau glycolée s'est vaporisée dans l'atelier qui est arrêté aussitôt.

VOIR AUSSI Aria 21316, 25156, 40522

3.7 Conditions de travail

Les conditions de travail inadaptées se traduisent surtout par des erreurs de conduites (fig. 21). Ces erreurs sont la conséquence de situations où les opérateur sont confrontés à un événement complexe à gérer dans un environnement qui va perturber leurs capacités de perception, d'interprétation et de décision comme lors d'une phase de démarrage ou quand une situation anormale provoque des anomalies en série sur le procédé (voir ARIA 12671 p. 43).

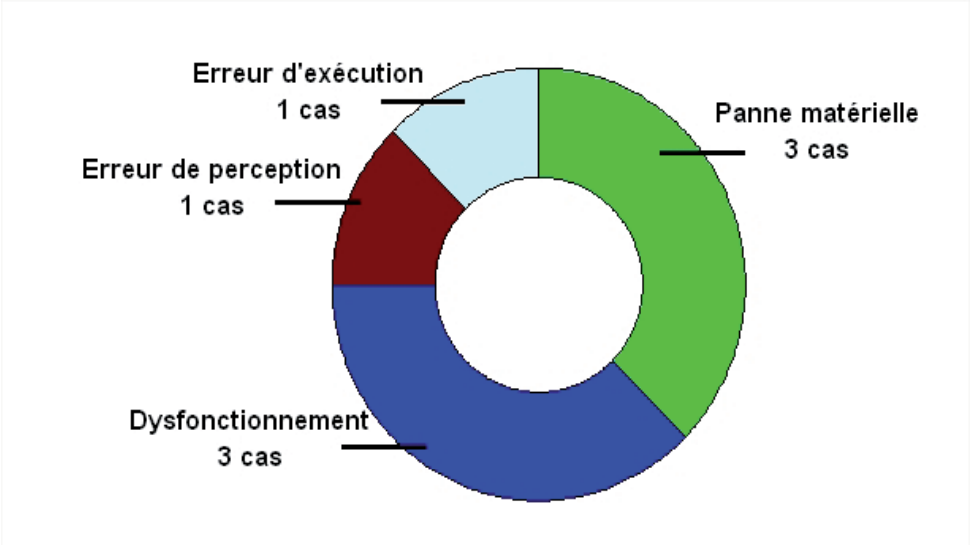
Figure 21 *Les causes premières ayant pour origine de mauvaises conditions de travail*



3.8 Agressions météorologiques

Les agressions météorologiques sont la source de quelques accidents en provoquant principalement des pannes et des dysfonctionnements de la fonction traitement (fig. 22), résultant souvent de phénomènes orageux générateurs de perturbations électriques ou électromagnétiques qui vont toucher les composants matériels de l'automate (voir ARIA 32624 p. 43).

Figure 22 *Les causes premières ayant pour origine des agressions météorologiques*

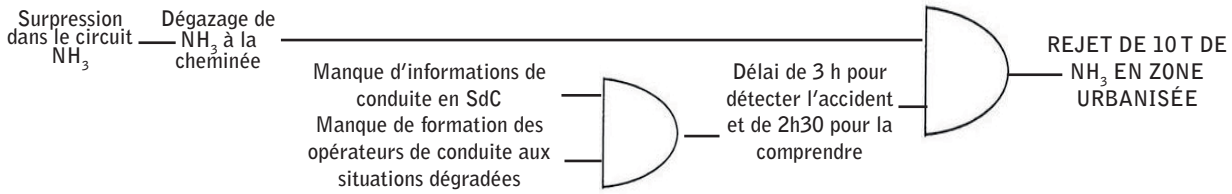


PERTE D'UTILITÉ EXTERNE (ARIA 28416)
25/10/2004

Dans une usine chimique classée Seveso, un feu se déclare à 12h59 dans un poste électrique alimentant une unité d'hydrate d'hydrazine. Un défaut électrique sur une pompe d'eau de refroidissement génère un court-circuit généralisé sur une colonne électrique. L'alarme incendie se déclenche à 13 h. L'incendie se propage aux autres colonnes du tableau par le sous-plancher. Le disjoncteur 400 V en amont, grippé, ne fonctionne pas. Le courant de défaut passe dans le transformateur 13 000 / 400 V ; une surpression et une fuite d'huile se produisent, puis un défaut homopolaire « côté primaire » entraînant l'ouverture du disjoncteur 13 kV. **L'absence de tension** déclenche le groupe diesel, mais le basculement vers ce système de secours échoue, l'automatisme étant endommagé par l'incendie. La fumée se répand dans le local onduleur dont la porte est restée ouverte. **L'onduleur s'arrête à température haute provoquant la perte du contrôle commande.** Les équipements se mettent en sécurité. **Faute d'alimentation électrique, le système de refroidissement, l'agitation et la sirène POI/PPI ne sont plus opérationnels.** La réaction en cours étant exothermique, le réacteur monte en température et en pression. A 14h10, une soupape de sécurité s'ouvre sur une colonne de l'unité d'hydrazine et 280 kg d'ammoniac (NH_3) sont émis à l'atmosphère. Plusieurs mesures sont prises : étude d'un circuit de refroidissement de secours, amélioration de la maintenance des disjoncteurs, sectorisation des salles onduleurs, tableaux électriques et groupe électrogène...

VOIR AUSSI Aria 8885, 26199, 38676, 41460, 42235

CONDITIONS DE TRAVAIL (ARIA 12671)
27/03/1998



Sur un échangeur tubulaire, un disque se rompt sur un quart de sa section à 4h50 lors d'une surpression dans le circuit ammoniaque (NH_3) reliant des stockages d'NH_3 à un atelier d'urée en marche stable. L'NH_3 est en partie entraîné vers une cheminée de dégazage de 100 m de haut. **Le rejet a lieu à l'insu des opérateurs interprétant mal plusieurs alarmes**. Diagnostic fait, l'appareil est isolé à 6h25. **L'exploitant n'a conscience de la gravité de l'événement qu'à partir de 8 h, 2h30 sont ensuite nécessaires pour en déterminer origine et causes probables**. Evaluée à 1 t d'NH_3 puis à 10 t quelques jours plus tard, la fuite à fort impact médiatique est due à une succession de défaillances matérielles, organisationnelles et humaines :

- manque de dispositifs de détection d'anomalies et de mise en sécurité automatique, **informations mises à disposition des opérateurs en salle de contrôle insuffisantes ;**
- **mauvais diagnostic / prise de décisions sans vérifications suffisantes malgré plusieurs signaux précurseurs ;**
- consignes de sécurité incomplètes.

Le mauvais diagnostic explique la non prise en compte des variations du bac d'eau ammoniacale, le retard pour isoler le circuit déficient et l'impact potentiel du rejet. De longs délais s'écoulent entre début de l'accident, alerte et activation du POI, identification de l'origine, des causes et circonstances du rejet, puis sa quantification définitive.

VOIR AUSSI Aria 8885, 26199, 38676, 41460, 42235

AGRESSION MÉTÉOROLOGIQUE (ARIA 32624)
26/07/2006

Un orage se déclare à proximité d'un dépôt de liquides inflammables protégé par un paratonnerre à dispositif d'amorçage (PDA). **Les effets indirects de la foudre ont endommagé l'une des 4 cartes d'interface de l'ordinateur**. Cette carte était interfacée avec le réseau bus rapatriant les alarmes de sécurité de niveau haut des réservoirs des dépôts. L'exploitant détecte le dysfonctionnement au moyen de la supervision du dépôt lui indiquant le défaut de communication. **L'exploitant ne dispose pas de carte de secours** et ne peut la remplacer rapidement. Il décide d'en informer l'ensemble des personnels d'exploitation et demande le renforcement de la vigilance lors du suivi des feuilles de cadence. L'exploitation se poursuit ainsi pendant 5 jours avant le remplacement effectif de la carte d'interface de l'ordinateur. La carte endommagée n'était pas protégée contre les effets indirects de la foudre. Après cet incident, l'exploitant conserve une carte supplémentaire en secours et met en place les recommandations de l'étude des effets indirects de la foudre réalisée en avril 2006 consistant en la protection, principalement au moyen de parafoudre, de l'ordinateur de supervision, des centrales de regroupement des alarmes, des capteurs et des locaux techniques, des pompes incendie de 3 dépôts, du groupe électrogène de 2 sites.

VOIR AUSSI Orage: Aria 8885, 20835, 32016, 38617 / Forte pluie : 32579, 36496 / Inondation : 35167

1

Cette synthèse confirme le rôle positif des automates industriels pour la sécurité des installations et la prévention des accidents. Si la fonction traitement se montre moins accidentogène que la fonction capteur, sa défaillance reste un facteur d'accident critique dans les secteurs d'activité fortement automatisés et utilisant des matières et équipements dangereux.

2

Les facteurs organisationnels et humains jouent un rôle fondamental dans l'accidentologie de la fonction traitement : meilleure fiabilité matérielle et plus faible exposition aux environnements agressifs des procédés que pour les capteurs et actionneurs, rôle essentiel des opérateurs de conduite.

3

La prédominance des erreurs de conduite par rapport aux défaillances matérielles dans les causes premières identifiées souligne l'importance de placer l'opérateur, et non la machine, au centre de la démarche de spécification de l'automate et de l'analyse des risques associées. En particulier, l'ergonomie de la conduite doit lui permettre d'appréhender facilement l'état du procédé, d'avoir un retour sur les effets de ses actions et de percevoir rapidement les alarmes vraiment importantes, afin de garantir son efficacité dans les situations anormales ou dégradées pour lesquelles son rôle devient irremplaçable et prépondérant.

4

Enfin, la formation et la qualification des opérateurs de conduite doivent être régulièrement vérifiées et entretenues, sous peine de leur faire perdre le contact avec un procédé qui risque de devenir progressivement une « boîte noire » fermée à leurs yeux.

Les pages suivantes associent aux 5 principales causes profondes d'accidents de la fonction traitement identifiées dans cette synthèse (voir chapitre 3) une série de recommandations de prévention.

- **Pour chacune des causes de ces causes profondes, l'importance relative des deux grandes catégories de causes premières - défaillances matérielles et erreurs de conduite, voir chapitre 2 - est notée sur une échelle de 0 à 5 :**

de ☆☆☆☆☆ **:** ***cause première jamais ou rarement rencontrée***

à ★★★★★ **:** ***cause première systématiquement rencontrée***

- **Chaque recommandation est classée en fonction de sa complexité de mise en œuvre, de l'importance des ressources en interne qu'elle est susceptible de mobiliser et enfin de son coût estimé en cas de recours à un prestataire externe. Ce classement utilise l'échelle suivante :**

☆ **:** ***négligeable à faible***

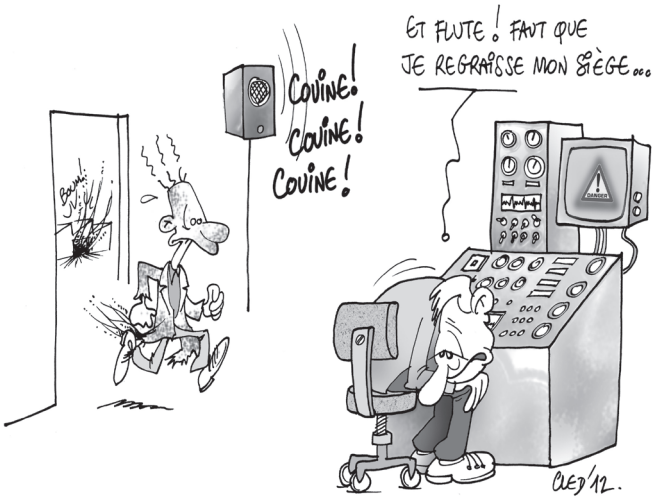
★ **:** ***faible à modéré***

★★ **:** ***modéré à important***

★★★ **:** ***important à élevé***

COMPÉTENCES ET ORGANISATION DU TRAVAIL				
Causes premières provoquées	**Défaillances matérielles**	☆☆☆☆☆		
	Erreurs de conduite (principalement d'interprétation)	★★★★☆		
Recommandations		**Complexité**	**Ressources internes**	**Coût**
Définir les pré-requis de capacités et de connaissances pour le poste d'opérateur de conduite (connaissances fondamentales, expérience professionnelle, connaissance des procédés et des risques de l'activité, capacité d'analyse...).		★	★	☆
Formaliser et mettre en œuvre un cursus de formation à la conduite, aboutissant sur une habilitation, avec des recyclages réguliers et des vérifications périodiques des acquis.		★★	★★	★ à ★★★
Equilibrer les charges de travail entre les opérateurs de conduite. Favoriser la rotation et la polyvalence entre opérateurs de conduite pour stimuler leur vigilance et leur compréhension globale du procédé à surveiller.		★★★	★★	☆
Définir clairement les actions autorisées ou interdites selon le niveau d'habilitation atteint par l'opérateur : bypass d'équipements ou de dispositifs de sécurité, acquittement d'alarmes prioritaires, situations pour lesquelles il faut consulter la hiérarchie avant de prendre une décision.		★	★	☆
Insister sur le fait qu'une décision allant dans le sens de la sécurité ne sera jamais sanctionnée, même si elle se révèle *a posteriori* inutile et qu'elle a engendré des pertes de production ou une surcharge de travail pour l'équipe.		★★	★	☆
Prévoir un entraînement régulier des opérateurs aux situations dégradées et inhabituelles, si possible sur un simulateur dédié reproduisant fidèlement le fonctionnement de l'automate (délais...) et les interfaces.		★★	★★	★ à ★★
Au cours de la formation initiale ou du recyclage, favoriser la compréhension de l'état du procédé par l'opérateur : paramètres importants, plages de fonctionnement normales et inhabituelles, sur quels paramètres jouer pour ramener le procédé dans sa zone de contrôle...		★★	★	☆
Au cours de la formation initiale ou du recyclage, favoriser la compréhension de l'effet des sécurités automatisées : conditions de déclenchent, effets sur le procédé, délai et dans quelles situations seront-elles moins efficaces ou inefficaces...		★★	★	☆
Inciter les opérateurs de quart à avoir une attitude interrogative et échanger entre eux sur les situations inhabituelles pour confronter leurs avis.		★	★	☆
Vérifier que les éventuels problèmes de ressources internes (congés, maladie, collègue en formation...) n'obligent pas l'opérateur de conduite à effectuer des tâches qui ne sont pas de son ressort et le distraient, même momentanément, de ses activités de supervision, et que les effectifs en salle de contrôle sont toujours suffisants pour traiter une situation dégradée.		★★	★★	☆
Vérifier que les procédures de conduite et de sécurité mises en place : • couvrent les différents modes de fonctionnement de l'unité (y compris les modes dégradés, situations d'urgence / arrêt), les différents risques identifiés et les différentes configurations de travail possibles en salle de contrôle (effectifs réduits, intérimaires, personnel en cours de formation...) ; • définissent clairement les rôles et les responsabilités de chacun ; • établissent un « balisage » pour guider l'opérateur vers la bonne décision, sans être excessivement directrices mais en gardant des « points de passages» obligatoires (cf. [20]) ; • correspondent aux pratiques de travail des opérateurs de conduites en les associant à leur rédaction ; • ont été testées et sont compréhensibles par le personnel de conduite (vocabulaire utilisé, illustrations évocatrices, pas d'ambiguïté...) ; • sont mises à jour régulièrement en cas de : 1- demande de modification pertinente formulée par un opérateur ou un groupe d'opérateurs 2 - modification technique ou organisationnelle de l'unité, même mineure comme l'ajout d'un paramètre ou d'une alarme (processus de gestion des modifications) 3 - exploitation d'un retour d'expérience interne ou externe sur incident ou accident ; • sont facilement et rapidement accessibles aux postes de conduite ; • font l'objet de tests de connaissance et de bonne compréhension auprès des opérateurs dans le cadre de leur formation / recyclage.		★★★	★★	☆

CONTRÔLE ET MAINTENANCE				
Causes premières provoquées	**Défaillances matérielles**	★★★★☆		
	Erreurs de conduite (principalement de perception)	★★☆☆☆		
Recommandations		**Complexité**	**Ressources internes**	**Coût**
Définir une politique de maintenance préventive (contenu et fréquence) pour chacun des composants critiques de l'automate selon l'expérience, les recommandations du fabricant et les bases de données fiabilistes disponibles (*Oreda, Eireda, PDS*...).		★★	★	★
Définir la nature et la périodicité des tests à effectuer sur les différents composants de l'automate : vérification fonctionnelle et visuelle, vérification des conditions environnementales...		★★	★	☆
Afficher (manuellement ou automatiquement) en salle de contrôle un état de fonctionnement actualisé des principaux composants de l'automate, pour que les opérateurs de conduite en soient informés : actifs, indisponibles, en dérangement, shuntés...		★	☆	☆ à ★
Définir des procédures de maintenance de l'automate en identifiant les composants critiques, les délais maximaux de réparation à respecter (notion de *Mean Time To Repair*) et les mesures compensatoires à mettre en œuvre pendant leur indisponibilité. Assurer une traçabilité de ces procédures et leur accessibilité aux équipes de conduite et de maintenance sur le lieu de travail.		★★	★★	☆
Mettre en place des indicateurs pour détecter d'éventuelles dérives de la maintenance : temps moyen de réparation, délais d'approvisionnement, disponibilité des stocks et des outillages, taux de panne des composants...		☆	★	☆
Vérifier que la communication entre les équipes de conduite et de maintenance fonctionne bien et soit régulière (cahier de suivi, réunions...)		★	★	☆
Veiller à la disponibilité rapide des composants de rechange de l'automate, notamment pour ceux qui tombent souvent en panne (ex : cartes d'entrée - sortie, relais...). Mettre régulièrement à jour la documentation.		☆	★	☆ à ★
En cas de risque d'obsolescence (arrêt du suivi par le fabricant), étudier l'intérêt de changer de génération d'automate ou à défaut, avoir la capacité de disposer rapidement des composants de rechange qui ne sont plus distribués par le fabricant (stocks de 1re et 2de urgence sur site ou hors site, cannibalisation, refabrication sur commande...).		★★	★	★ à ★★★
S'assurer de toujours disposer, en interne ou en externe, de personnes compétentes et rapidement disponibles (proximité géographique) pour assurer la maintenance sur site des différents composants de l'automate et échanger régulièrement avec les équipes de conduite.		★	★	★★



PROGRAMMATION				
Causes premières provoquées	Défaillances matérielles (principalement des dysfonctionnements)	★★★☆☆		
	Erreurs de conduite (principalement de perception)	★★★☆☆		
Recommandations		**Complexité**	**Ressources internes**	**Coût**
Lors de la spécification de l'automate, impliquer les agents d'encadrement et les opérateurs de conduite pour vérifier que toutes les fonctions attendues et les modes opératoires utilisés dans l'unité sont prévus dans le cahier des charges.		★★	★★	☆
Vérifier que le prestataire qui procède à la programmation de l'automate a bien compris les principes de fonctionnement de l'unité et de ses sécurités instrumentées, faire régulièrement des points d'étape et des tests avec lui avant la mise en service de l'automate.		★	★	★
Dans le planning d'installation d'un nouvel automate, prévoir du temps pour les phases de test et d'essais, ne pas précipiter la mise en service si l'on pense que l'automate n'est pas tout à fait au point.		★	★★	★ à ★★
Dans les tests à réaliser avant la mise en service, inclure les phases de fonctionnement inhabituelles du procédé (démarrage, arrêt prolongé, arrêt d'urgence) ainsi que les principaux modes dégradés prévisibles (panne ou consignation de certains équipements, perte d'utilité...).		★★	★	★
Si la conduite de l'unité peut se faire à la fois de façon manuelle et automatisée (cas des retrofits par exemple), examiner les « effets de bord possibles » entre ces deux modes de conduite et programmer l'automate afin de les éviter ou les minimiser.		★★★	★	☆ ★ à
Vérifier que les procédures de gestion des modifications du site prennent aussi en compte les modifications à apporter à la programmation de l'automate (modifications matérielles intervenues sur le procédé telles qu'un changement d'équipement, l'ajout de nouvelles fonctionnalités ou de paramètres de surveillance).		★	★	★★
S'assurer qu'un support informatique soit disponible pour faire évoluer la programmation selon les difficultés rencontrées par les équipes de conduite et les évolutions nécessaires identifiées au fil du temps.		☆	★	★

ERGONOMIE				
Causes premières provoquées	Défaillances matérielles	☆☆☆☆☆		
	Erreurs de conduite (principalement de perception)	★★★★☆		
Recommandations		**Complexité**	**Ressources internes**	**Coût**
Les interfaces de conduite doivent être conçues de manière à faciliter la perception, la bonne compréhension et la vigilance de l'opérateur de conduite. Pour cela, il convient de soigner particulièrement (cf. norme EEMUA 201, [16] et [20]) : • l'animation des synoptiques de conduite (remplissage, ouverture...) ; • la cohérence des représentations graphiques des équipements avec leur taille ou leur localisation dans l'unité ; • l'utilisation de couleurs pour limiter la fatigue visuelle et apporter un bon contraste, et l'adéquation des couleurs avec leurs standards ou stéréotypes (ex : rouge : haute priorité, jaune : priorité moyenne, etc.) ; • l'existence d'un retour donné aux opérateurs sur les résultats de leurs actions ; • l'affichage prioritaire des paramètres critiques avec leur plage de fonctionnement normal et un historique temporel ; • l'affichage des alarmes prioritaires : perception facile et rapide, sans interférence d'autres éléments du synoptique... • l'affichage d'un synoptique courant favorisant la perception globale de l'état de l'unité, et de synoptiques plus spécifiques pour la visualisation en détail de l'état de certaines parties ou équipements du procédé ; • l'exploitation aisée du bandeau des alarmes (pas de navigation complexe entre plusieurs écrans) ; • les termes et symboles affichés, qui doivent être naturels, standards et homogènes avec ceux employés par les opérateurs de conduite et dans les procédures en vigueur ; • la taille des caractères et des symboles affichés qui doivent être facilement perceptibles depuis le poste de travail des opérateurs.	★★	☆	★ à ★★
Pratiquer un prototypage des interfaces de conduite et recueillir l'avis des opérateurs de conduite pour que l'interface soit la plus adaptée possible à leurs pratiques acceptables de « terrain ».		★	★	★
Intégrer les aspects d'ergonomie matérielle et logicielle de la salle de contrôle dans les procédures de gestion des modifications en vigueur.		☆	★	☆
Prendre en compte l'ergonomie matérielle de la salle de contrôle pour que les conditions de travail des opérateurs soient les plus adaptées possibles : claviers et écrans, mobilier, postures de travail, facteurs d'ambiance et leur variabilité temporelle (lumière, bruits...), déplacements dans la salle de contrôle, communication verbale et visuelle entre les opérateurs de quart, moyens de communication avec les opérateurs d'exploitation... (cf. norme ISO 11064 et [20]). Cette approche doit favoriser la communication entre les opérateurs, minimiser les risques de distraction, de mauvaise perception et d'erreurs de geste (saisie d'une valeur erronée, appui sur le mauvais bouton...).		★	☆	★ à ★★

CONCEPTION MATÉRIELLE				
Causes premières provoquées	**Défaillances matérielles**	★★☆☆☆		
	Erreurs de conduite (principalement de perception)	★★★☆☆		
Recommandations		**Complexité**	**Ressources Internes**	**Coût**
Analyser et classer les différents composants de la chaîne de conduite automatisée selon leur criticité vis-à-vis de la sécurité : capteurs, actionneurs, calculateurs, cartes et réseaux de communication, interfaces de conduites, logiciels...		★★	★	☆
Pour les composants classés critiques : • définir le comportement qu'ils doivent avoir en cas de panne, perte d'utilité ou de dysfonctionnement de l'automate (ex : *fail safe*, alimentation de secours) ; • privilégier les équipements standards et à long cycle de vie pour minimiser le risque de panne et faciliter leur maintenance ; • choisir des composants facilement testables et, si possible, dotés de capacités d'auto-diagnostic (capteurs, calculateurs...) ; • privilégier le choix de composants dont la maintenance est possible sans arrêter (totalement) l'unité et sans compromettre la sécurité.		★★★	★	☆
Analyser les conditions de service et environnementales auxquelles seront soumis ces composants pour définir les contraintes qu'ils doivent être capables de supporter sans dysfonctionner : température, humidité, poussière, atmosphère corrosive, vibrations, chocs mécaniques, décharges électrostatiques...		★★	★	☆ à ★
Lors du choix des composants et de l'architecture de l'automate, se baser sur une méthodologie d'analyse des risques reconnue, en minimisant les risques de modes communs de défaillance et en favorisant l'identification des redondances jugées nécessaires pour les composants critiques (*Hazop,* concept de sécurité intrinsèque...).		★★★	★	★
Pour la conception d'une chaîne de sécurité automatisée, vérifier la compatibilité des composants choisis avec les attendus en termes d'indépendance, de fiabilité et de temps de réponse (niveau de SIL atteint globalement par la chaîne complète).		★★	★	☆ à ★
Si la conduite de l'unité peut se faire à la fois de façon manuelle et automatisé, identifier les « effets de bord possibles » entre ces 2 modes de conduite et en tenir compte dans le choix de l'architecture de fonctionnement.		★★★	★	☆ à ★
Mettre en place une méthodologie de gestion des alarmes : • identification des alarmes existantes en situation normale et en situation dégradée, mesure de leurs flux ; • interview des opérateurs sur les alarmes existantes : pertinence, importance du flux, priorité dans l'affichage, pratiques de traitement des alarmes en situation normale et dégradée, pratique de shunt de certaines alarmes jugées « nuisibles », délai de traitement jugé suffisant ? • examen de l'utilité réelle et de la priorité de chaque alarme selon la situation en cours ; • examen de la pertinence des seuils des alarmes pour minimiser les risques d'oscillation et d'alarmes nuisibles ; • examen des redondances entre alarmes (plusieurs alarmes signalant le même problème ou se déclenchant à répétion pour la même raison) ; • définition des taux d'alarme cibles en situation normale et en situation dégradée qui soit compatible avec les capacités de traitement des opérateurs (cf. normes ISA 18.2 ou EEMUA 191) ; • différenciation des alarmes selon leur nature et priorité (tonalité, modulation, vibrations...) ; • faciliter l'acquittement des alarmes depuis le poste de conduite (minimum de déplacement, accès rapide au synoptique) ; • sélection des alarmes à afficher pour respecter les taux d'alarmes cibles et définition de leur niveau de priorité (3 niveaux maximum) ; • définition d'une stratégie de gestion des alarmes pour les futurs projets automatisés et pour les modifications des alarmes.		★★	★★	★ à ★★

- [1] DGPR/BARPI . « Le capteur, un allié de la sécurité ? ». Accidentologie des automatismes industriels, partie 1/3, juin 2012. Disponible sur : ***http://www.aria.developpement-durable.gouv.fr/syntheses/par-theme/accidentologie-des-automatismes-industriels-le-capteur/***
- [2] BAINBRIDGE, L. « Ironies of automation ». Automatica, 19, pp. 775-779, 1983.
- [3] DGPR/BARPI. « Inventaire 2013 des accidents technologiques ». Disponible sur : ***http://www.aria.developpement-durable.gouv.fr/inventaire-2013/***
- [4] Dossiers de sécurité fonctionnelle. « Instrumentation : des équipements à surveiller de près ». Mesure, n° 813, mars 2009.
- [5] HEALTH AND SAFETY EXECUTIVE. « Human factors aspects of remote operations in process plants ». Contract research report, 432 / 2002, ISBN 0 7176 2355 6.
- [6] COLLMELLERE, C. « Quand les concepteurs anticipent l'organisation pour la maîtrise des risques : deux projets de modifications d'installations sur deux sites classés Seveso 2 ». Thèse de doctorat de sociologie, Université technologique de Compiègne, 566 p., 2008.
- [7] MOULTON, B. ; FORREST, Y. « Accidents will happen : safety critical knowledge and automated control systems ». New Technology, Work and Employment 20:2, ISSN 0268-1072.
- [8] BARIL, R. « Les transformations du travail des opérateurs de raffinerie de pétrole : le passage des cadrans aux écrans ». Pistes, vol n° 1, novembre 1999.
- [9] CHARETTE, R. N. « Automated to death ». IEEE Spectrum, décembre 2009. Disponible sur : ***http://spectrum.ieee.org/computing/software/automated-to-death***.
- [10] Repères. « Alarmes et diagnostics : des composants essentiels ». Jautomatise, n° 77, pp. 44-47, juillet-août 2011.
- [11] « Alarm management best pratices: are you following them ? ». Automation world, 8 février 2012. Disponible sur : ***http://www.automationworld.com/operations/alarm-management-best-practices-are-you-following-them***.
- [12] STAUFFER, T. et al. « Managing alarm using rationalization ». Control engineering, 3 mars 2011. Disponible sur : ***http://www.controleng.com/single-article/managing-alarms-using-rationalization/13efb381a8d417b6f7d16b3140799f29.html***.
- [13] PARASURAMAN, R. ; RILEY, V. « Humans and Automation : Use, Misuse, Disuse, Abuse ». Human factors, 39, pp. 230-253, 1997.
- [14] LEVARAY, J.P. « Putain d'usine ». Editions de l'insomniaque, 94 p., 2002, ISBN 2 9087 4445 7.
- [15] RALEIGH, P. « Operating procedure key to process safety ». Process engineering, 16 juillet 2012. Disponible sur : ***http://processengineering.theengineer.co.uk/operating-procedure-key-to-process-safety/1013172.article***.
- [16] FANCHINI, H. « Imagerie de conduite industrielle : le choix des images, le poids des maux ». Le travail humain, tome 54, n°3, 1991.
- [17] Repères. « L'opérateur : le maillon faible ? ». Jautomatise n° 53, pp. 52-57, juillet-août 2007.
- [18] DANIELLOU, F., SIMARD, M., BOISSIERES, I. « Facteurs humains et organisationnels de la sécurité industrielle, un état de l'art ». Numéro 2012-02 des *Cahiers de la sécurité industrielle*, ICSI, Toulouse, 2010, ISSN 2100-3874
- [19] SWAIN, A.D., GUTTMANN, H.E. « Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications ». NUREG/CR-1278, USNRC,1983.
- [20] DANIELLOU, F. « L'opérateur, la vanne, l'écran. L'ergonomie des salles de contrôle ». Edition de l'ANACT, Collection outils et méthodes, avril 1986, ISBN 2-03540-34-9.

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 du Développement durable 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.
Souslesrubriquesgénérales,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.

Plus de 250 fiches techniques détaillées et illustrées présentent 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, automatismes industriels...

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, plus de 40 000 accidents sont en ligne et de nouvelles analyses thématiques verront régulièrement le jour.

Cette synthèse constitue le deuxième volet d'une étude approfondie de l'accidentologie des automatismes industriels dans la base ARIA. Consacrée à la fonction « traitement », elle présente les enseignements tirés de l'analyse détaillée de 325 accidents sélectionnés dans cette base.

Ces enseignements et recommandations ont pour objectif de sensibiliser toutes les personnes impliquées dans la sécurité des installations industrielles. Cette synthèse montre en effet que les défaillances de la fonction traitement d'un automate industriel, ayant provoqué ou aggravé un accident, ont majoritairement pour cause directe des erreurs humaines liées à des causes organisationnelles profondes.

Voir aussi :

Accidentologie des automatismes industriels, partie 1/3 :
« Le capteur, un allié de la sécurité ? »

Accidentologie des automatismes industriels, partie 3/3 :
« vannes et actionneurs » (à paraître)

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

Bureau d'analyse des risques et pollutions industriels
5 place Jules Ferry
69006 Lyon
Téléphone : 04 26 28 62 00
Email : barpi@developpement-durable.gouv.fr

Direction générale de la Prévention des risques
Ministère de l'Écologie, du Développement durable et de l'Énergie

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Ministère de l'Écologie, du Développement durable et de l'Énergie