Procédés automatisés : derrière l'opérateur, l'organisation

Si l'automatisation des procédés permet de réduire la gravité et la fréquence des accidents, l'opérateur en charge de la conduite reste la pièce maîtresse de la sécurité. Pourtant on voit ici que l'environnement organisationnel dans lequel il travaille est encore trop souvent inadapté à la bonne exécution de sa tâche : produire en sécurité.

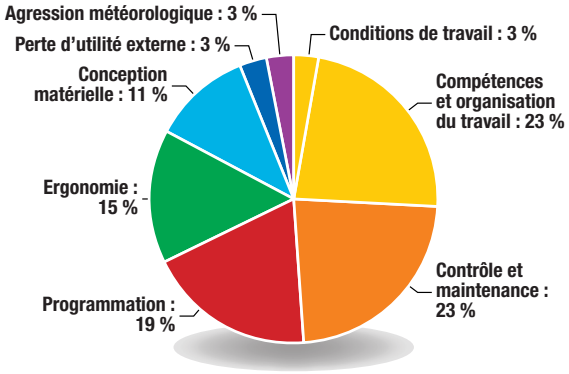
DR

Parmi les accidents de conduite des procédés automatisés répertoriés dans la base Aria, près d'un quart des causes profondes proviennent de problèmes de formation des opérateurs et d'organisation de leurs tâches. ►

L'article précédent (*Face au Risque* n° 503, mai 2014) a permis de mieux comprendre la nature des défaillances de procédés automatisés à l'origine d'accidents industriels répertoriés dans la base de données Aria. Il a montré qu'au-delà des classiques défauts matériels des composants, la majorité des défaillances apparaissent en salle de contrôle sous la forme d'une erreur commise par l'opérateur de conduite lorsque son processus cognitif est perturbé.
Des alarmes acquittées sans qu'il en résulte la moindre action corrective, des opérateurs de conduite qui aggravent une situation dégradée au lieu de la rattraper. Autant de symptômes qui montrent la nécessité de mieux comprendre les causes profondes des accidents de conduite des procédés automatisés. L'analyse de 275 accidents de ce type sélectionnés dans la base Aria permet ainsi d'identifier huit familles de causes profondes à l'origine de tous

ces accidents (voir figure 1). Cinq d'entre elles peuvent être regroupées en deux grandes catégories représentant chacune environ 45 % de toutes les causes identifiées sur l'échantillon : celles liées aux conditions d'exploitation (compétences, contrôle et maintenance, conditions de travail) et celles liées à l'automate lui-même (ergonomie, programmation, conception). Ces causes profondes méritent donc d'être présentées plus en détail.

Fig. 1 – Répartition des causes profondes des accidents de conduite automatisée



Une organisation du travail défaillante dans la moitié des accidents

La moitié des causes d'accidents sont liées aux mauvaises conditions d'exploitation du procédé automatisé. Les problèmes de formation des opérateurs de conduite et l'organisation de leurs tâches représentent presque un quart de toutes les causes profondes répertoriées dans l'échantillon d'accidents. Ce type de problème diminue la capacité de l'opérateur de conduite à interpréter la situation en cours ou à prendre la bonne décision. Ce dernier ne peut donc appliquer les bonnes actions pour rattraper la situation dégradée survenant sur le procédé (voir l'accident « Alarmes ignorées faute de consignes » page suivante).

Les défaillances de contrôle et de maintenance des composants de l'automate représentent elles aussi presque un quart de toutes les causes répertoriées. Elles provoquent bien sûr des défaillances techniques du système automatisé, mais aussi, et par ricochet, des difficultés de perception par l'opérateur de conduite. En effet, celui-ci ne dispose pas des informations nécessaires à une action adaptée quand les paramètres critiques de conduite ne sont pas ou plus disponibles en salle de contrôle (voir l'accident « Un défaut de maintenance provoque une pollution » page suivante et la vidéo « Alerte toxique en salle de contrôle » sur le site Internet du Barpi).

Les erreurs de programmation à l'origine d'un accident sur cinq

Les processus de spécification et de conception du système automatisé représentent la deuxième grande catégorie de causes profondes de ces accidents. Les défauts de la programmation recouvrent à eux seuls 1/5 de toutes les causes recensées. Ils traduisent en général les difficultés à réaliser un programme couvrant les différents états du procédé, tout en s'adaptant aux pratiques d'exploitation en vigueur. En effet, le prestataire extérieur ne connaît pas toujours bien les différents états du procédé, surtout dans les situations dégradées et inhabituelles. Comme elles sont rares et difficiles à anticiper, ces situations sont souvent oubliées ou mal décrites dans les documents de spécification.

Les conséquences d'un défaut de programmation de l'automate peuvent se limiter à des défaillances matérielles, comme le montre l'accident « Programmation en cause dans la rupture du disque » (voir page suivante). Mais ce défaut contribue souvent à perturber l'opérateur de conduite, car des paramètres importants ne sont finalement pas - ou mal - exploités par le système.

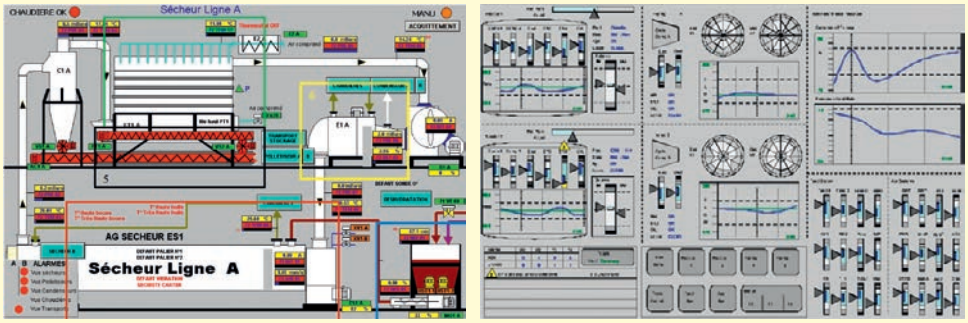
Des interfaces de conduite essentielles à la sécurité !

L'ergonomie représente également une cause importante de cette deuxième catégorie. Elle est souvent liée à l'absence de prise en compte des spécificités physiologiques et mentales de l'opérateur humain. Lors des processus de spécification

BEAUTÉ PEUT NE PAS RIMER AVEC SÉCURITÉ

Si attirante qu'elle soit, l'interface graphique de gauche se contente de reprendre le synoptique du procédé et est trop chargée et colorée. À cause de cela, un opérateur n'a pas perçu une situation dangereuse (voir l'accident n° 42156 dans la base Aria).
L'interface de droite est conforme aux bonnes pratiques ergonomiques : affichage de l'historique temporel des paramètres et des plages de fonctionnement, couleurs réservées aux alarmes critiques rendues de ce fait plus visibles, etc.

Fig. 2 – Ergonomie des interfaces



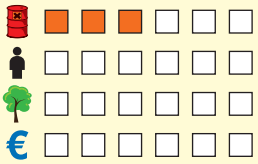
et de conception d'un nouveau procédé automatisé, les efforts sont focalisés sur les performances techniques et sur la réduction des délais de mise en service.
On demande rarement leur avis aux opérateurs de terrain lors de la définition des nouvelles interfaces de conduite. Pourtant ce sont les principaux utilisateurs, et ils vont passer des milliers d'heures devant ces interfaces !
La figure 2 illustre ainsi les marges de progression qui existent encore dans le domaine de l'ergonomie des interfaces. La différence est frappante entre une interface de conduite d'inspiration purement technique (en haut) et une interface dont l'ergonomie a été pensée pour aider l'opérateur de conduite dans sa tâche quotidienne (en bas). Logiquement, les défauts ergonomiques entraînent des perturbations cognitives de l'opérateur : soit il n'arrive pas à percevoir les paramètres importants pour la situation en cours, soit il a du mal à les interpréter correctement (voir l'accident « Une interface confuse retarde la détection… » page suivante).

Une fois en exploitation, les défauts de conception sont difficiles à détecter

Cette deuxième catégorie de causes profondes recouvre enfin les erreurs de conception matérielle de l'automate. Ces erreurs se produisent aussi bien lors de l'installation d'un nouveau procédé automatisé que lors de modifications d'un procédé existant. En fonctionnement normal, ces erreurs sont difficiles à détecter. Elles ne provoquent généralement que des dysfonctionnements mineurs car les processus automatisés essentiels au procédé ont été testés et validés.
En revanche, lors des situations anormales ou dégradées, beaucoup plus rares, les effets accidentels de ces erreurs se révèlent pleinement. Leur rapidité de déclenchement ne permet plus à l'opérateur de remettre le procédé en zone sûre (voir l'accident « Des automates incapables de gérer la dérive des conditions d'exploitation » page suivante). C'est d'autant plus

QUELQUES ACCIDENTS ILLUSTRATIFS

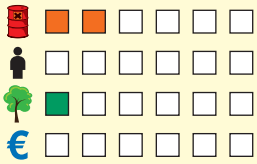
ALARMES IGNORÉES FAUTE DE CONSIGNES APPROPRIÉES



8 janvier 2007. Vers 17 h, des teneurs élevées en hydrocarbures sont relevées sur le site d'une usine chimique suite au dysfonctionnement du dispositif de chauffage d'un bac de benzène entraînant l'ébullition du produit, suivie de son émission à l'atmosphère par la soupape de sécurité : 4,4 t de benzène sont rejetées à l'atmosphère. La surchauffe du benzène est due à une défaillance du capteur de température pilotant la vanne d'alimentation en vapeur du circuit de chauffage.
L'alarme sonore de température haute, réglée à 40 °C, avait été acquittée sans réglage d'un nouveau seuil d'alarme. Les enregistrements montrent que la température du benzène dépassait 40 °C depuis plusieurs jours. Le rejet n'a été détecté que par la concentration de benzène dans l'air et non par la prise en compte des paramètres de suivi du réservoir pourtant alarmés pour certains depuis plusieurs heures en salle de contrôle.
Aucune procédure ou instruction définissant les seuils d'alarme des différents paramètres d'exploitation du réservoir et les actions à engager lors de dérive n'était définie.

> Indices accidents

UN DÉFAUT DE MAINTENANCE DE LA CHAÎNE DE DÉTECTION PROVOQUE UNE POLLUTION



21 janvier 2004. Dans une usine métallurgique en cours de redémarrage, des effluents contenant 700 kg de zinc sont déversés dans le canal voisin.
Le réseau d'eaux pluviales polluées du site se déverse dans une fosse de relevage. Ces eaux sont ensuite transférées par pompage vers un bassin de stockage. D'anciennes pompes permettant un rejet direct dans le canal sont toujours en service. Le jour de l'accident, des fuites sur les échangeurs de l'atelier de lixiviation (extraction de minéraux par circulation d'une solution aqueuse) s'écoulent dans le réseau d'eaux pluviales. À la suite d'une erreur de manipulation, les effluents sont rejetés sans traitement dans le canal. L'erreur de manipulation est due :
> à un défaut d'alerte de la salle de contrôle suite à une panne du système de détection et de transmission des fuites ;
> à la non consignation des anciennes pompes.

PROGRAMMATION EN CAUSE DANS LA RUPTURE D'UN DISQUE

28 novembre 2005. Dans une usine de matières plastiques, un disque de rupture s'ouvre sur le retour moyenne pression (RMP) d'une ligne de l'atelier Polyéthylène. Les produits évacués s'enflamment en sortie de cheminée. Trois employés sont légèrement blessés.
Des travaux sur une des trois lignes de l'atelier ont entraîné le déclenchement par les automates de l'arrêt d'urgence général.

EN SAVOIR PLUS

> Synthèse Barpi « Accidentologie des automatismes industriels, partie 2/3 : La fonction traitement, de l'écran… à l'accident », 2014, 30 pages.
> Vidéo illustrative : « Alerte toxique en salle de contrôle », 2014, 15 minutes.
Téléchargeables librement sur le site Internet du Barpi : www.aria.developpement-durable.gouv.fr

regrettable que la plupart des situations inhabituelles sur un procédé sont généralement prédictibles en phase de conception. Cela suppose bien sûr de s'appuyer sur une méthodologie éprouvée d'analyse des risques (Amdec, Hazop, Lopa, etc.). Il est donc important de se donner le temps nécessaire à une conception soignée et rigoureuse du procédé automatisé.
Seule la prise en compte des causes profondes peut réduire efficacement les risques d'accident des procédés automatisés.
Le passage en revue d'un échantillon important d'accidents de procédés automatisés a montré que la défaillance technique ou l'erreur de l'opérateur en salle de contrôle ne sont généralement que les conséquences visibles de causes plus profondes. Pour améliorer la sécurité des procédés, il est essentiel de ne pas se contenter de corriger les symptômes. Il convient de traiter en priorité les causes profondes que sont les conditions d'exploitation et notamment les facteurs organisationnels, ainsi que la programmation des automates et la conception des interfaces de conduite faisant la liaison entre l'homme et la machine. ■

Didier Pitrat
Ministère de l'Écologie, du Développement durable et de l'Énergie, Bureau d'analyse des risques et pollutions industriels (Barpi)

Cette action a provoqué la montée en pression dans le circuit RMP et l'ouverture d'un disque de rupture.
La présence d'électricité statique dans la cheminée aurait provoqué l'ignition du nuage d'éthylène relâché par le disque. L'exploitant lance plusieurs actions : révision de l'analyse fonctionnelle des positions de repli des vannes de protection des circuits RMP, vérification et programmation des positions retenues dans les automates…

UNE INTERFACE CONFUSE RETARDE LA DÉTECTION D'UNE SITUATION ANORMALE

4 novembre 2011. Une élévation anormale de température est constatée dans une cellule en béton d'un silo, lors d'un contrôle du suivi thermométrique sur le logiciel du poste de supervision des installations. Une hétérogénéité de l'humidité du produit stocké est à l'origine de l'auto-échauffement. En outre, les prises horaires d'échantillons en sortie de séchoir n'ont pas permis de constater l'anomalie.
L'absence de détection de l'anomalie de température par le personnel, malgré le suivi thermométrique muni d'alarmes visuelles, est due selon l'exploitant à trois facteurs : manque de vigilance, paramétrage perfectible et mauvais affichage du niveau de remplissage de la cellule qui fausse les alarmes, visualisation partielle des courbes en fonction des échelles de temps ou température utilisées.

DES AUTOMATES INCAPABLES DE GÉRER LA DÉRIVE DES CONDITIONS D'EXPLOITATION

12 juillet 2006. Vers 20 h 30, un feu se déclare au niveau de la torchère d'un atelier de production de biocarburant. 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.
La soupape de sécurité du réacteur de l'atelier est reliée à la torchère par l'intermédiaire d'une cuve tampon. Le jour de l'accident, un dysfonctionnement du processus de chargement automatique des matières premières a conduit au sur-remplissage du réacteur. Le surplus de matière a débordé vers la cuve tampon. Le dépassement du niveau haut de cette cuve entraîne une alarme. Lorsque l'opérateur se rend sur place, le mélange réactionnel a atteint la flamme de la torchère et s'est enflammé.
À l'origine de l'événement :
> le défaut de chargement du réacteur n'a été détecté ni par l'automate de conduite, ni par l'opérateur en salle de contrôle ;
> le dépassement du niveau très haut de la cuve tampon n'a pas entraîné de mise en sécurité de l'installation par l'automate de sécurité, mais uniquement une alarme au poste de commande ;
> la cohabitation de deux automates ne permet pas d'avoir une vision intégrée des sécurités et du procédé. Les informations disponibles n'ont pas permis une intervention suffisamment rapide des opérateurs.