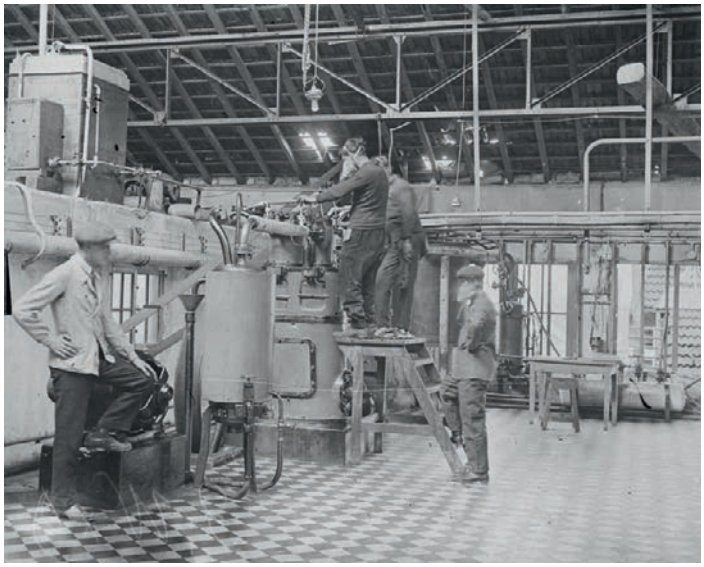
Procédés automatisés : la carte ou l'opérateur ?

Si, dans l'industrie, les systèmes automatisés permettent de mieux protéger les travailleurs et d'améliorer les dispositifs de sécurité, l'analyse de leur accidentologie met en relief les défaillances d'origine technique mais aussi humaine.



DR

◄ **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 sa surveillance sont pilotés depuis une salle de contrôle.**

Dans les processus industriels, la fonction de traitement des automates de conduite et de sécurité constitue le véritable « cerveau » de l'automate, car elle est située entre les capteurs (amont) et les actionneurs (aval). Les défaillances de cette fonction sont susceptibles de provoquer ou d'aggraver des accidents sur les sites industriels dont la production et la sécurité repose largement sur ces systèmes automatisés. Comme tout équipement industriel, ces défaillances peuvent être d'origine matérielle, mais aussi humaine, le développement des procédés conduit à distance depuis une salle de contrôle ayant fait apparaître une nouvelle vulnérabilité de cette fonction : les erreurs commises par les opérateurs en charge de la supervision.

L'étude des accidents de la base de données Aria montre que ceux qui sont provoqués ou aggravés par une défaillance de la fonction traitement représentent une vingtaine d'accidents par an et ont doublé depuis 20 ans. Ils touchent un grand nombre de secteurs d'activité. En effet, si la majorité des accidents étudiés sont survenus dans l'industrie lourde (chimie, raffinage, métallurgie), ils le sont aussi dans des secteurs où se développe le contrôle des procédés à distance comme celui de l'énergie (non nucléaire) et de l'agroalimentaire. Si la plupart des accidents étudiés ne présentent pas un caractère de grande gravité, fuites de matières dangereuses avec dommages matériels et pertes de production, leurs circonstances sont, en revanche, plus révélatrices. 53 % d'entre eux sont survenus en dehors des périodes de fonctionnement normal : démarrage, maintenance, arrêt d'urgence…

La fonction traitement repose sur des composants matériels comme des cartes électroniques, des calculateurs,

mais aussi sur l'intervention des opérateurs de quart devant leurs écrans en salle de contrôle. Cette dualité se retrouve dans les défaillances matérielles et humaines à l'origine des accidents.

LA MOITIÉ DES DÉFAILLANCES MATÉRIELLES SONT DES DYSFONCTIONNEMENTS SANS PANNE

Une analyse des causes directes menée sur 275 accidents a montré que 37 % d'entre eux avaient pour origine la défaillance matérielle d'un des composants. En regardant de plus près la nature de ce type de défaillance (voir figure 1), on constate que plus de la moitié sont des dysfonctionnements sans panne franche de l'automate. Ceux-ci s'avèrent difficiles et plus longs à détecter, donc propices à créer ou aggraver une situation accidentelle. La figure montre aussi la faible part des pannes informatiques par rapport aux pannes matérielles et, en particulier, par rapport aux pannes électroniques (voir l'accident « Panne de carte électronique » page 16).

L'OPÉRATEUR AGGRAVE LA SITUATION DANS UN ACCIDENT SUR QUATRE !

Les autres causes directes sont constituées par les erreurs de conduite commises par les opérateurs en salle de contrôle, qui représentent la majorité des défaillances (63 %). Les « symptômes » les plus fréquents de ces erreurs sont l'absence de réaction de l'opérateur, ou une réaction inefficace face à une situation dégradée du procédé supervisé (voir figure 2). Mais, plus inquiétant, dans presque une situation sur quatre, l'opérateur a aggravé la situation au lieu de la corriger ! Un examen plus détaillé de la nature de ces erreurs (voir figure 3) permet de constater que la majorité d'entre elles a pour origine un problème de perception des informations importantes ou d'interprétation correcte de la situation en cours.

DIFFICULTÉS DE PERCEPTION ET ERREURS D'INTERPRÉTATION

Les difficultés de perception sont à l'origine de presque la moitié des erreurs de conduite et traduisent les situations où l'opérateur n'a pas ou a mal perçu les informations envoyées par l'automate. La plupart de ces problèmes ont pour origine l'indisponibilité de ces informations en salle de contrôle, suite à une panne de capteurs/actionneurs ou un défaut de conception de l'automate rendant ces paramètres impossibles à percevoir (voir l'accident « Paramètres de conduite non prévus » page 17).

Les erreurs d'interprétation restent aussi très fréquentes (29 %) et surviennent lorsqu'un opérateur ne réussit pas à comprendre la situation en cours sur le procédé supervisé. Plusieurs facteurs concourent à ces erreurs :

• une « perte de contact » de l'opérateur avec le procédé : l'automatisation ayant confiné les opérateurs en salle de contrôle, ces derniers perdent peu à peu les connaissances sur la réalité physique des installations et se construisent une représentation du procédé sur la base des informations reportées par l'automate (voir l'accident « Perte de contact avec le procédé » page 17). Quand une situation anormale se produit, ils sont de moins en moins capables de les interpréter efficacement ;

Fig. 1 : Les types de défaillances matérielles de la fonction traitement d'un automate

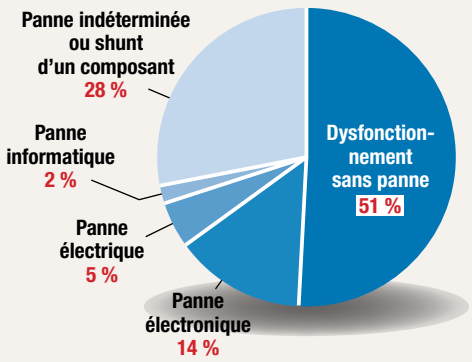


Fig. 2 : Les symptômes des erreurs de conduite

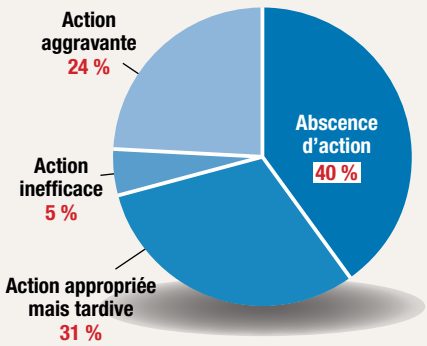
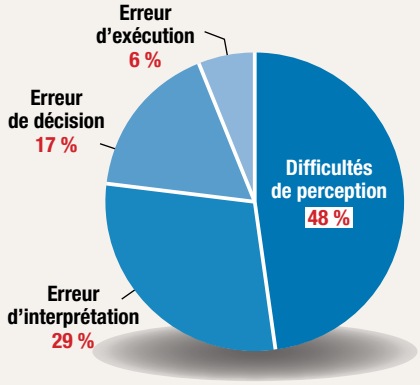


Fig. 3 : La nature des erreurs de conduites



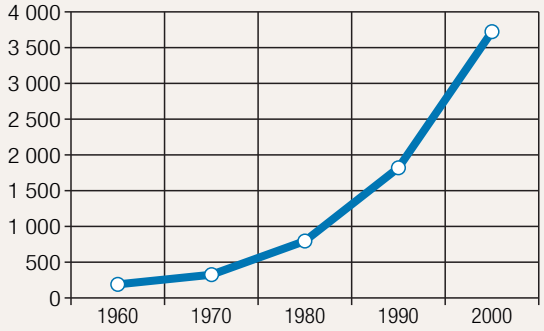
• l'augmentation exponentielle des alarmes non hiérarchisées lors des situations anormales contribue à noyer l'opérateur de conduite sous un flux d'informations qu'il n'est plus capable d'exploiter (voir fig. 4).
Les erreurs de décision sont plus rares (17 %). Elles trouvent leur origine dans un biais lié à l'opinion que porte l'opérateur de conduite sur l'automate :
• la méfiance peut l'amener à ignorer certaines informations reportées par l'automate quand elles contredisent l'idée qu'il se fait de la situation, voire à court-circuiter les automatismes qui pourraient bloquer ou compliquer son action (voir l'accident « Méfiance envers l'automate » page 17) ;
• à l'inverse, l'opérateur peut avoir une confiance aveugle dans l'automate et ne plus prêter attention à certains signaux alarmants : il laisse l'automate décider à sa place même si la situation voudrait qu'il reprenne la main.
La pression peut aussi perturber les capacités décisionnelles de l'opérateur, quand sa décision doit être rapide ou qu'elle est porteuse d'enjeux techniques ou financiers. Enfin, quelques cas d'accidents mettent en relief les limites de procédures incomplètes ou mal rédigées, qui ne permettent pas de gérer la situation inhabituelle en cours.
Pour finir, les erreurs d'exécution sont les moins nombreuses (6 %) et traduisent les inévitables erreurs que peut faire un opérateur humain à son poste de travail, comme une saisie erronée ou l'activation du mauvais bouton (voir l'accident « Erreur de saisie » page 17).

UN RÔLE CORRECTIF MALGRÉ TOUT

Les opérateurs en salle de contrôle ont un rôle tout aussi important, si ce n'est plus, que les composants matériels pour assurer la sécurité des procédés automatisés. Leurs erreurs peuvent provoquer ou aggraver une situation dégradée et mener à l'accident. Mais il ne faut pas oublier que ces mêmes opérateurs arrivent le plus souvent à rattraper des situations dégradées et à éviter un accident. Cet article a montré l'importance de leur assurer des conditions de travail appropriées, aussi bien matérielles qu'organisationnelles, pour minimiser les risques d'erreurs principalement liés à des difficultés de perception et d'interprétation des informations dont ils ont besoin pour effectuer efficacement leurs tâches de supervision. ■

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

Fig. 4 : Évolution du nombre d'alarmes différentes que doit gérer un opérateur de conduite de plate-forme pétrolière entre 1960 et 2005

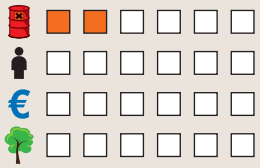


(source : World Oil, septembre 2006)

L'étude « Accidentologie des automatismes industriels, partie 2/3 : La fonction traitement, de l'écran… à l'accident » est disponible sur le site Internet du Barpi.

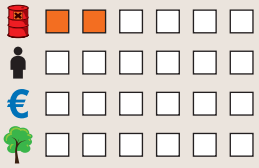
QUELQUES ACCIDENTS ILLUSTRATIFS

PANNE DE CARTE ÉLECTRONIQUE



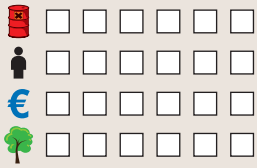
2 mai 2012. Lors d'une livraison de méthoxyméthane (DME) dans une usine de produits cosmétiques, un flexible de transfert gonfle au niveau du raccord vers l'installation fixe et fuit en raison d'une incompatibilité entre le matériau du flexible et le produit livré. L'opératrice constate la fuite et alerte 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 minutes. La mise en sécurité aurait dû être déclenchée par une détection gaz qui s'est révélée inopérante à cause d'un défaut matériel des cartes électroniques de la centrale de traitement (cartes anciennes 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.

PARAMÈTRES DE CONDUITE NON PRÉVUS



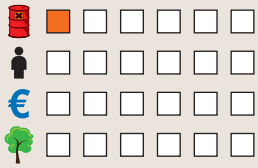
3 mars 2005. Dans une usine chimique, 0,6 t de chlorure d'hydrogène (HCl) s'échappent pendant 10 minutes de l'ensemble des fours et évents de l'atelier de sulfate de potassium lors du nettoyage des circuits d'HCl. Un employé résidant à proximité du site alerte le poste de garde. La mise en service de l'arrosage d'urgence permet de stopper les émissions. Le dysfonctionnement d'un des deux dispositifs de mesure de pression de la sortie de gaz des fours (sans lien direct avec l'intervention) a entraîné la fermeture de la vanne de régulation du circuit de tirage des gaz. N'étant plus tirés, les gaz se sont échappés des fours, causant l'accident. L'absence d'alarme sur la régulation du tirage a retardé l'intervention du personnel et l'absence d'inter-comparaison entre les deux mesures de pression a rendu impossible la détection de la dérive du capteur défaillant. Pour diminuer la probabilité d'un nouvel incident, une alarme de détection d'écart entre les deux mesures de pression est installée et une procédure identifiant les interventions délicates imposant notamment la présence de l'encadrement est rédigée.

PERTE DE CONTACT AVEC LE PROCÉDÉ



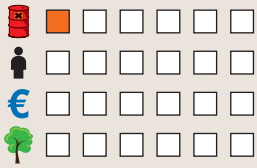
16 octobre 2002. Dans le cadre du redémarrage d'une centrale thermique, le turbo-alternateur est remis en service le 15 octobre à 14 h et couplé sur le réseau national sans dysfonctionnement. Entre le 15 octobre au soir et le 16 au matin, une montée en température anormale entraîne l'auto-inflammation de l'huile dans la caisse à huile et un incendie autour du turbo-alternateur. Plusieurs mesures correctives sont prises : mise en place 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.

ERREUR DE SAISIE



15 juillet 2007. À 21 h 03, le tableauteur, chargé de la section catalyse de l'unité de craquage catalytique (FCC) d'une raffinerie, entre une valeur erronée d'ouverture 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 minutes provoquant des émissions à la torche, puis son arrêt progressif.
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.

MÉFIANCE ENVERS L'AUTOMATE



28 juillet 2009. Dans une centrale électrique, un transfert de fioul domestique du bac primaire 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. 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 a par ailleurs constaté 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…

> Indices accidents