CESICS

Commission des Experts
pour la Sécurité dans l'Industrie Chimique
de la Suisse

Bulletin

Systèmes de conduite de procédé et événements

De la sécurité des installations conduites par ordinateur

Bulletin de la CESICS No. 5 Août 1998

BULLETIN DE LA CESICS No. 5 Août 1998

Systèmes de conduite de procédé et événements

De la sécurité des installations conduites par ordinateur

Dans l'industrie chimique, la conduite automatique de procédés s'est largement répandue ces dernières années. Presque toutes les nouvelles installations sont pilotées par un ordinateur ou un système de conduite de procédé (dans ce bulletin, des expressions telles que "ordinateur", "calculateur de procédé", "CPU" [central processing unit], "système d'automation", "système de conduite de procédé", "système de commande" sont considérées comme synonymes). Les avantages de l'automation sont évidents: économie de personnel d'exploitation, optimisation du déroulement des procédés et de la qualité des produits, etc.

La plupart du temps, l'automation devrait aussi tendre vers une plus grande sécurité: la fiabilité de la conduite des appareils est améliorée, des paramètres importants du procédé peuvent être surveillés en permanence, un dépassement des valeurs limites prédéfinies déclenche des signaux d'alarme et induit des contre-mesures. La probabilité d'apparition d'une situation ou d'un événement dangereux indésirable peut ainsi être fortement réduite. Ce but n'est toutefois atteint que si certaines règles et mesures de précaution sont respectées lors de l'automatisation, c.à.d. lors de la conception des capteurs, des actionneurs, du hardware et du software, mais aussi lors de l'exploitation, de l'entretien et d'éventuelles modifications. Leur inobservation peut créer de nouvelles sources de danger, souvent difficilement détectables et risque de provoquer dans certains cas des incidents aux conséquences graves. - Ce bulletin veut illustrer de tels dangers par la description d'événements et indiquer les moyens de les maîtriser. En les lisant, il faut cependant se garder de généraliser les mesures prises dans chaque cas; selon les circonstances, d'autres mesures peuvent aussi se révéler adéquates, même dans des cas très semblables.

Les 9 événements décrits ci-après sont survenus au cours de ces dernières années. Ils ont été choisis arbitrairement parmi la documentation concernant des incidents utilisée pour la préparation de ce bulletin. Les causes et lacunes ressortant des avis d'événements et qui sont en relation avec un système d'automation peuvent se classer dans les catégories suivantes:

① *Hardware et capteurs*
- Capteur de température défectueux
- Sonde de niveau défectueuse
- Carte d'interface inadaptée
- Pas de deuxième niveau de sécurité

② *Alimentation en énergie*
- Programmation inadéquate du comportement du calculateur lors de la remise sous tension après une coupure de courant
- Coupure du courant 24 V - système non protégé

③ *Software*
- Erreur de programmation: priorités inadéquates
- Pas de sécurité par software contre des erreurs de manipulation prévisibles
- Pas de hiérarchisation des alarmes

④ *Interventions manuelles*
- Des interventions manuelles sur l'installation ne sont reconnues et prises en considération par le calculateur que si les éléments actionnés sont équipés des émetteurs de signaux nécessaires.

Exemples d'incidents, catégories de causes

Surchauffe d'un réacteur batch ①

Pour la fabrication d'un colorant, la masse réactionnelle devait être maintenue à une température de 135 °C durant 10 heures. Après 8 heures, des fluctuations inexplicables de température sont apparues sur le calculateur de procédé. La température intérieure du réacteur affichée est descendue en dessous de la valeur de consigne, ce qui a automatiquement enclenché le chauffage. Finalement, une alarme LERR (**L**oop **Err**or) est survenue, suivie d'une mise en sécurité automatique. Des contrôles sur place ont cependant indiqué une température intérieure de 153 °C et une pression intérieure de 5.6 bar.

La sonde intérieure de température était défectueuse et indiquait une température intérieure trop basse (= défaillance passive). De ce fait, le calculateur activait le chauffage conformément à la programmation. La mise en route du refroidissement d'urgence par le

La correspondance concernant ce Bulletin peut être adressée à:
Dr. H. Künzi, Président de la CESICS, F. Hoffmann-La Roche AG, Postfach, 4070 Basel
Dr. K. Eigenmann, membre du comité directeur, Novartis International AG, Postfach, 4002 Basel
Dr. R. Ott, membre du comité directeur, Suva, Postfach, 6002 Luzern
Hr. H. Burg, Dahlienstrasse 17, 4106 Therwil

personnel d'exploitation a présenté des difficultés, parce que la sonde défectueuse et l'alarme LERR ramenaient toujours à l'état de sécurité prévu par le software.

La pression induite dans le réacteur par une élévation supplémentaire incontrôlée de la température intérieure aurait automatiquement déclenché le refroidissement d'urgence en atteignant 7 bar (correspondant à env. 167 °C). Un danger aigu de réaction exponentielle (Runaway) n'existait pas, car la TMR_{ad}[1] est supérieure à 24h à 165 °C. Le réacteur aurait en outre pu être vidé d'urgence dans un deuxième réacteur, maintenu constamment libre à cet effet.

Afin de diminuer encore plus le danger d'une défaillance passive d'une sonde de température, la température intérieure est dorénavant surveillée par deux sondes de température couplées de façon redondante et soumises à un contrôle de plausibilité (contrôle du synchronisme). Une différence prédéfinie entre les deux sondes déclenche la mise en position de sécurité du software.

Panne d'ordinateur au cours d'une condensation de chlorure cyanurique en milieu aqueux ①

Au cours d'une réaction avec du chlorure cyanurique en milieu aqueux à 16 °C dans un réacteur de 25 m^3, la commande du procédé est tombée en panne à cause d'un défaut d'une carte d'interface. Il ne fut soudain plus possible ni d'agiter, ni de surveiller la température dans le réacteur. A ce moment, 20% de la soude caustique nécessaire pour neutraliser l'acide chlorhydrique formé avaient déjà été ajoutés. Le calculateur a été remis en fonction après env. 2½ heures, afin de poursuivre la réaction. L'hydrolyse exothermique du chlorure cyanurique, qui s'est poursuivie sans agitation pendant ce temps, a entraîné une élévation de température involontaire: 103 °C étaient affichés sur la console de commande. La température n'a pu être ramenée à 25 °C qu'en ajoutant d'urgence 2 tonnes de glace et en enclenchant le refroidissement à la saumure.

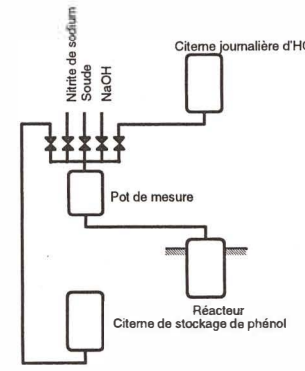
L'hydrolyse autocatalytique et exothermique du chlorure cyanurique est bien connue. L'état critique, résultant de la panne des fonctions de surveillance et de l'agitateur durant la première phase de la réaction, aurait dû être reconnu et enregistré lors de l'analyse des risques. L'adjonction d'une surveillance de la température et d'un contrôle de l'agitation, tous deux indépendants du système de conduite de procédé, auraient p. ex. constitué des mesures adéquates dans ce cas.

Débordement d'un pot de mesure d'acide chlorhydrique ① ③

Pendant la fabrication d'un colorant, un pot de mesure sur peson, relié à un réacteur, a été rempli d'acide chlorhydrique à partir d'une citerne de réserve (citerne journalière d'HCl, voir le schéma). Le calculateur a donné l'ordre de fermer la vanne d'HCl lorsque le poids désiré a été atteint. La vanne est cependant restée ouverte et le remplissage du pot a continué. Le non-fonctionnement de la vanne a été signalé sur le tableau de commande. Des essais de fermeture de la vanne d'HCl par une commande d'urgence ou par un ordre donné manuellement ont échoué, si bien que le pot a été trop rempli. - Le pot de mesure pouvait également être rempli de substances provenant d'autres citernes, par l'intermédiaire d'une conduite collectrice. L'acide a bientôt débordé à travers ce collecteur, pour aboutir dans une citerne de phénol située à un étage inférieur et, de celle-ci, dans le bâtiment.

L'ordre de fermeture de la vanne d'HCl n'a pas été transmis à cause d'une carte d'interface défectueuse (avec sorties digitales). La même carte d'interface a encore actionné d'autres vannes. La défectuosité de la carte a ainsi provoqué l'ouverture de la vanne du phénol dans la conduite collectrice, ce qui a permis à l'acide de couler dans la citerne de phénol. La défectuosité de la carte n'a pas permis la mise automatique des vannes en position de sécurité.

Lors de la conception de l'installation et spécialement du système de distribution, on avait admis (sans vérification) que l'installation se mettrait en état de sécurité en cas de panne de la carte d'interface, c.à.d. que les vannes seraient en état de sécurité "fermées".



[1] TMR_{ad}, Time to maximum rate, c.à.d. le délai jusqu'à l'explosion thermique (maximum de la vitesse de décomposition dans des conditions adiabatiques)

Cependant, une défaillance de la carte crée **n'importe quel** signal de sortie, ce qui a été confirmé par le fabricant des cartes. Des positions définies de sécurité deviennent par conséquent illusoires.

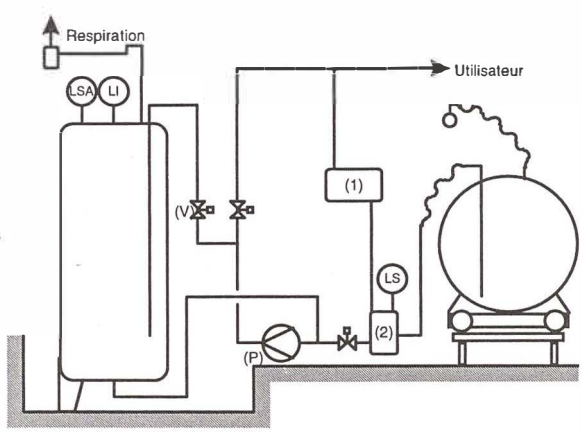
Lorsque des substances chimiques, susceptibles de réagir violemment entre elles, sont amenées dans un pot de mesure commun par une conduite collectrice, leur mélange doit être évité de façon sûre, c.à.d. par des mesures techniques. Dans ce cas particulier, cela signifie la nécessité d'aménager une sécurité par le hardware, en plus du verrouillage des vannes d'amenée par le software (une vanne ouverte = toutes les autres fermées). Un remplissage excessif du pot de mesure peut être évité par une alarme de niveau haut. Selon la portée d'un éventuel écoulement de substances, il faut également installer un niveau de sécurité indépendant (appréciation par l'analyse des risques).

Ecoulement d'acide chlorosulfonique ① ③

Lors du dépotage d'un wagon-citerne, la citerne de stockage a été trop remplie. En l'espace de 3 - 4 minutes, 1 - 2 tonnes d'acide chlorosulfonique se sont écoulées dans le bassin de rétention de la citerne. Le brouillard formé par réaction avec l'eau contenue dans le bassin a notablement incommodé l'environnement immédiat de l'usine et a conduit à déclencher l'alarme du voisinage (sirènes).

Les causes identifiées sont une fausse indication de la mesure de niveau dans la citerne (LI; level indicator) et une erreur dans le programme de l'ordinateur. Celui-ci aurait dû interrompre le remplissage de la citerne lorsque l'alarme de niveau haut (LSA, level switch alarm) a réagi.

Le parc à citernes, encore récemment commandé manuellement au moyen d'une électronique conventionnelle, a été automatisé en même temps qu'un rack de conduites a été construit jusque vers l'un des principaux utilisateurs.



L'acide chlorosulfonique était l'un des produits devant être fournis automatiquement à l'utilisateur par une conduite du rack. Compte tenu des risques inhérents à l'acide chlorosulfonique, on avait décidé de vidanger la conduite dans la citerne après chaque livraison. Outre les séquences "Dépotage du wagon-citerne" et "Fourniture à l'utilisateur", il a fallu programmer l'opération supplémentaire "Vidange de la conduite". Lors de la séquence "Vidange", l'acide chlorosulfonique coulait à travers un réservoir intermédiaire (1) dans le récipient d'amorçage (2). Dès que l'indicateur de niveau LS de celui-ci affichait "haut", la vanne d'arrêt (V) recevait l'ordre de s'ouvrir et la pompe (P) celui de se mettre en marche.

Le jour de l'incident, lorsque le wagon-citerne a été raccordé et que le dépotage a commencé, la commande de l'installation était toujours en mode "Vidange de la conduite". Après remplissage du récipient d'amorçage (2), la vanne V s'est normalement ouverte et la pompe s'est mise en marche. Le niveau dans le récipient d'amorçage est resté "haut" durant tout le dépotage. L'indicateur de niveau LI de la citerne a eu une défaillance. Bien que l'alarme de niveau haut LSA ait réagi, les ordres de fermeture de la vanne V et d'arrêt de la pompe en résultant sont restés sans effet. La structure particulière du software donnait la priorité à l'enchaînement "niveau du récipient d'amorçage (LS2) haut → pompe en marche/vanne V ouverte".

Le software de la commande du parc à citernes a été entièrement restructuré. Les diverses séquences fonctionnelles ont été totalement séparées (livraison/transfert du wagon-citerne à la citerne de stockage, fourniture à l'utilisateur, vidange).

Afin d'éviter autant que possible d'incommoder le voisinage par des brouillards d'acide, même en cas d'avarie, le stockage d'acide chlorosulfonique a été déplacé dans un parc entièrement fermé. A son nouvel emplacement, la citerne a de nouveau été équipée d'un indicateur de niveau, ainsi que d'une alarme de niveau haut entièrement indépendante du système d'automation.

Ecoulement d'acide sulfurique par suite de remplissage excessif d'un pot de mesure ③

Un pot de mesure pour de l'acide sulfurique à 60 % a été trop rempli. La cause en est une faute de frappe lors de l'introduction de la valeur de consigne sur le tableau de commande.

Lorsque le remplissage excessif provoque une situation dangereuse comme dans ce cas, le pot de mesure doit être équipé d'une alarme de niveau haut.

Celle-ci doit fiablement interrompre le remplissage lorsque celui-ci dépasse un degré déterminé. Si une telle mesure n'est pas jugée indispensable, il faudrait au moins utiliser les possibilités de l'ordinateur pour limiter les saisies des valeurs de consigne par le software, de telle façon qu'une entrée dépassant une limite déterminée (capacité maximale du pot de mesure) soit refusée, et pour verrouiller le remplissage et l'indicateur de niveau.

Explosion dans un compresseur à anneau liquide ③

Une explosion s'est produite dans un compresseur à anneau liquide lors de la mise en route d'un réacteur en boucles destiné à l'oxydation du mélange d'un aromatique nitré et d'un butylate alcalin dans du cyclohexane. L'oxydation se fait au moyen d'oxygène gazeux (phase gazeuse: 8% O_2 dans N_2) sous pression. La phase gazeuse épuisée est amenée à un compresseur à anneau liquide (cyclohexane/tert. butanol), comprimée de 5 à 9 bar, refroidie, enrichie en O_2 et à nouveau introduite dans le réacteur en boucles. La concentration en O_2 ne doit pas dépasser 8%, afin d'éviter la formation d'un mélange de gaz explosible. Cette condition est garantie par une surveillance du taux d'O_2: un faible flux de gaz de mesure est prélevé dans le flux de gaz principal et conduit vers 2 sondes d'O_2 branchées en redondance. Lorsque le taux d'O_2 est inférieur à 8%, de l'oxygène frais est introduit par une vanne de régulation. Lorsque le taux d'O_2 dépasse 8%, l'installation se met en position de sécurité du hardware.

Peu avant l'incident, d'importantes fluctuations de pression ont été enregistrées dans le circuit gazeux, en aval du compresseur. Le point de fusion du liquide de l'anneau du compresseur est de 8 °C. La température du réfrigérant dans l'échangeur de chaleur situé après le compresseur n'est cependant que de 5 °C. Il est probable que l'échangeur de chaleur a été bouché par un mélange de solvants entraîné et cristallisé. Cela explique les variations de pression, qui ont fortement perturbé le flux de gaz de mesure. Il est possible qu'un petit condenseur de la conduite du gaz de mesure ait aussi été bouché pour la même raison. Toutes les conduites de gaz de mesure étaient surveillées par des rotamètres, qui ont transmis des signaux d'alarme dans les minutes précédant l'incident (débit inférieur à la valeur de consigne). A ce moment, on ne mesurait plus la concentration momentanée d'O_2 dans la boucle, mais une valeur quelconque < 8%. De ce fait, la vanne de régulation d'O_2 a reçu l'ordre de rester ouverte pour augmenter le taux d'O_2 jusqu'aux 8% voulus. La concentration d'O_2 est probablement montée en peu de temps à plus de 50% et la pression excessive a suffi à enflammer le mélange.

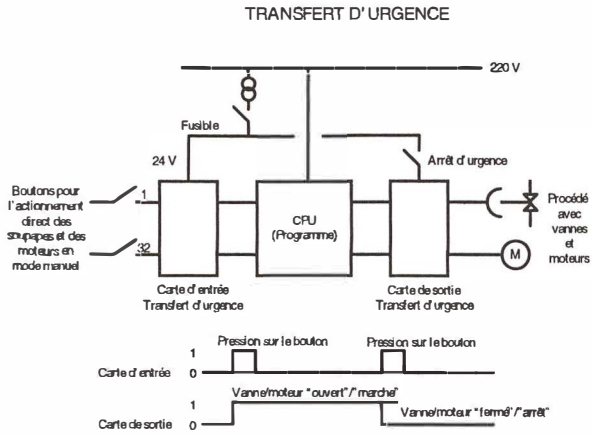
Bien que la surveillance du débit du gaz de mesure ait transmis toute une série d'alarmes, elle n'a pas déclenché automatiquement l'état de sécurité du hardware. Le personnel de la salle de commande n'a pas interprété les signaux conformément à leur signification réelle (pas de débit de gaz de mesure = mesure d'O_2 perturbée et risque d'explosion dû à un taux d'O_2 éventuellement trop élevé). Les signaux auraient dû amener le déclenchement manuel de l'état de sécurité du hardware (arrêt d'urgence).

S'il est indispensable de laisser le personnel de la salle de commande actionner l'arrêt d'urgence ou modifier les paramètres d'exploitation manuellement, il faut donner, en plus d'autorisations d'intervention définies, des directives précises indiquant comment réagir lors des diverses alarmes. Les alarmes demandant une intervention immédiate et ciblée pour éviter un état critique du point de vue sécurité ne doivent pas figurer sur l'écran ou sur la bande imprimée comme une information parmi d'autres. Il est judicieux d'établir une hiérarchie des alarmes selon l'urgence des interventions et de signaler visiblement celles qui exigent une action immédiate (p. ex. couleur différente sur l'écran, format spécial pour l'impression, évent. signal acoustique).

Activation simultanée de tous les transferts d'urgence dans un parc à citernes ② ① ③

L'interrupteur d'arrêt d'urgence du système de commande d'un parc à citernes a été déplacé du circuit de 220 V sur celui de 24 V. Pour cela, l'alimentation en 24 V de la commande du parc à citernes a été coupée en enlevant le fusible. Lors du rétablissement de l'alimentation en 24 V, tous les produits stockés, entre autres de l'oléum à 25% et à 66%, du mélange sulfonitrique, de l'acide chlorosulfonique et de l'aniline, ont été simultanément transvasés vers la citerne de secours. Seule l'intervention immédiate du chef d'équipe présent, qui a actionné l'arrêt d'urgence, a permis de ramener l'installation en état de sécurité et ainsi d'éviter un événement grave. Comme seules de faibles quantités des diverses substances sont parvenues dans la citerne de secours, la réaction chimique incontrôlée y est restée sans conséquences.

La cause de cette situation dangereuse est que l'on n'a pas tenu compte, lors de la conception de la sécurité technique du système de commande, d'une propriété des cartes d'entrée (cartes d'interface); voir le schéma ci-après:



En mode manuel, une pression sur un bouton-poussoir de la console de commande ouvre une vanne ou met un moteur en marche. Une deuxième pression sur le même bouton ferme la vanne ou arrête le moteur. L'électricien d'entreprise a ôté le fusible de 24 V pour déplacer l'interrupteur d'arrêt d'urgence du circuit de 220 V sur celui de 24 V. L'alimentation des cartes d'entrée et de sortie a ainsi été coupée. Lors du rétablissement du circuit de 24 V, les cartes d'interface ont transmis à la CPU (central processing unit) l'information que tous les boutons-poussoirs avaient été actionnés (voir le schéma: état 1). De ce fait, les transferts d'urgence ont été activés. - Une coupure de courant, provoquée p. ex. par un fusible qui saute, aurait également déclenché le transfert d'urgence lors de la remise sous tension.

Lors de la conception d'une installation, il faut préciser la procédure de remise en service automatique à partir de l'état de sécurité du hardware et la tester lors de la mise en exploitation.

Une analyse des risques systématique montre le danger présenté par un transfert simultané de substances chimiques. Selon l'appréciation de la portée des conséquences, il aurait au moins fallu prévoir un verrouillage des divers transferts par le software, voire même un niveau de sécurité indépendant.

Activation involontaire de toutes les sorties digitales[2] ② ③

Une coupure de courant a mis hors service le système de conduite de procédé d'une installation de production automatisée. L'installation s'est alors correctement mise en position de sécurité du hardware. Après réparation d'un fusible défectueux de l'onduleur (élément de l'alimentation de secours), l'alimentation en courant a été rétablie. Contre toute attente, l'installation ne s'est pas mise en état de sécurité du software. Toutes les sorties digitales du système de conduite de procédé ont été inopinément activées: des moteurs furent mis en route, des vannes furent ouvertes ou fermées. Cette situation ne s'est corrigée qu'au bout d'env. 5 secondes, lorsque l'état de sécurité du software voulu s'est déclenché. - A l'exception d'une interruption de la production, on ne dut heureusement pas déplorer de dommages. Cependant, une telle activation incontrôlée d'actionneurs, même de courte durée, pourrait provoquer un événement aux conséquences graves, selon la nature de l'appareillage et des produits impliqués.

Une "répétition" de l'incident en marche à vide de l'installation a montré ce qui suit: une panne de courant entraîne correctement la mise en position de sécurité du hardware. Mais lors du rétablissement du courant, le "watchdog" est d'abord déconnecté et l'ordinateur procéde en première priorité à un autocontrôle durant 3 - 5 secondes. Pendant cette opération, toutes les sorties digitales passent de la position "0" à la position "1". Le système de conduite de procédé ne met automatiquement l'installation en position de sécurité du software qu'à la fin de ce contrôle. Une mesure immédiate a consisté à modifier l'installation de façon que toutes les sorties digitales se mettent sur "0" lors du rétablissement du courant. - Apparemment, la remise en marche de l'installation à partir de la position de sécurité du hardware après une coupure de courant n'a pas été vérifiée suffisamment à fond lors de la mise en exploitation.

Un produit pulvérulent pollue un sous-sol ④

Le détecteur de fumée du sous-sol d'un bâtiment de fabrication a déclenché l'alarme-incendie. Les pompiers ont constaté un nuage dense de poussière, qu'ils ont rabattu au moyen de brouillard d'eau. Le sous-sol du bâtiment a été fortement pollué par un produit pulvérulent.

Le sécheur à pulvérisation et à lit fluidisé installé dans ce bâtiment est équipé d'un système de nettoyage, qui peut être mis en marche par l'ordinateur de procédé. Un liquide de nettoyage est pompé vers divers emplacements du sécheur (qui s'étend du rez-de-chaussée au 6e étage) depuis une citerne ouverte installée au sous-sol. Le liquide retourne dans la citerne du sous-sol par des vannes d'écoulement. Les nombreuses vannes de ce système de nettoyage sont normalement toutes pilotées par le sys-

---

[2] Sortie digitale (DOT): Signal de sortie activant des actionneurs "binaires", p. ex. vannes ouvertes/fermées, mise en marche ou arrêt de moteurs à vitesse fixe

tème de contrôle de procédé. Elles peuvent cependant aussi être commandées depuis la console, et même directement sur place, en actionnant le commutateur magnétique de chaque vanne au moyen d'un tournevis. Compte tenu de leur grand nombre, toutes ces vannes n'ont pas été munies d'interrupteurs de fin de course, ni d'affichage de leur position sur le calculateur. Les collaborateurs ont été instruits de n'actionner les vannes du système de nettoyage qu'au moyen de l'ordinateur.

Contrairement aux prescriptions, une vanne d'écoulement de nettoyage a été ouverte manuellement le jour de l'incident. Sa position n'était pas visible sur l'ordinateur. La vanne est restée ouverte et lorsqu'une légère surpression (max. 0.2 mbar) s'est produite durant la phase d'exploitation suivante, du produit pulvérulent a été soufflé par cette vanne jusque dans la citerne ouverte de nettoyage et de là dans le sous-sol.

Les collaborateurs ont à nouveau été instruits de n'actionner le système de nettoyage qu'au moyen de l'ordinateur. Plusieurs ouvertures dans les murs du sous-sol ont été bouchées. - Cet incident démontre la problématique des interventions manuelles dans des procédés automatisés. Elles doivent être sécurisées par les meilleures mesures organisationnelles possibles (instructions, check-lists, doubles contrôles).

Dangers, conclusions, mesures

Les incidents décrits ci-dessus forment un petit choix arbitraire parmi le grand nombre d'événements dans lesquels des systèmes de conduite de procédé ou des commandes automatiques sont impliqués d'une façon ou d'une autre. Ces exemples montrent que les systèmes d'automation doivent être intégrés plus fréquemment et plus à fond dans l'analyse systématique des risques des procédés et des installations. Cela implique une étroite collaboration entre l'exploitant responsable de l'installation et le spécialiste de la conception du système de conduite de procédé. L'exploitant de l'installation devrait aussi comprendre la logique du programme.

Dangers

Fiabilité des éléments du hardware

Les systèmes d'automation ont, en plus de leurs fonctions de commande et de régulation du procédé, aussi des tâches de surveillance et de sécurité. Ils se composent d'éléments techniques qui, comme tous les produits techniques, n'ont qu'une fiabilité limitée. La défaillance ou le dysfonctionnement de composants isolés (p. ex. capteurs, transmetteurs de signaux ou de données, cartes d'interface, unité centrale, actionneurs et leur alimentation en énergie) surviennent en général d'une manière aléatoire avec une certaine probabilité statistique. Ils peuvent entraîner des dérangements non détectés du système d'automation, voire même à sa mise hors service. Les fonctions de sécurité dévolues au système ne peuvent alors, à leur tour, plus être garanties. - La défaillance ou le dysfonctionnement de chaque composant isolé (erreur active ou passive), le comportement en cas de coupure de courant et le risque d'erreurs systématiques (common mode failure) doivent par principe être pris en considération. La plupart des défaillances d'éléments du hardware surviennent dans les parties périphériques de l'installation et non dans le système de conduite de procédé lui-même.

Erreurs et lacunes cachées du software

Les réactions d'un système d'automation au déroulement du procédé, suivi au moyen de capteurs, sont prédéfinies par le software (le programme). Celui-ci peut cependant contenir des erreurs difficilement décelables, surtout lorsqu'il n'a pas été établi en étroite collaboration entre l'auteur du procédé et le programmeur (de façon à ce que l'exploitant comprenne la logique du programme). Il en est de même lorsque l'exploitant a dû adapter le software, p. ex. à cause de modifications du procédé ou de l'appareillage. Des tests approfondis permettent de détecter et d'éliminer un grand nombre d'erreurs du software, y compris pour des situations extrêmes. Il est cependant impossible de tester toutes les combinaisons possibles d'erreurs de programmation et d'états techniques de fonctionnement, surtout pour des programmes importants. - Les erreurs et les lacunes du software sont des erreurs systématiques, c.à.d. que l'événement indésirable déclenché par une combinaison définie de conditions **surviendra toujours** lorsque cette combinaison sera réalisée. Dans des cas extrêmes, une installation pourra être exploitée durant des années avant que le cas survienne une fois. L'erreur du software prend alors le caractère d'un piège tendu. - Ce risque peut être abordé au moyen de mesures prises en dehors du programme, p. ex. par une conception du procédé sûre par elle-même ou par un deuxième niveau de sécurité indépendant (voir sous ce titre).

Interventions manuelles

Les procédés partiellement automatisés requièrent souvent des interventions du personnel, p. ex. pour le choix d'un programme déterminé ou d'une recette, pour l'introduction de valeurs de consigne

(température, quantités à ajouter, etc.), mais aussi pour le nettoyage de l'installation en vue d'un changement de produit. Des erreurs sont également possibles lors de telles interventions, comme lors de toute activité humaine. Une situation particulièrement critique existe lorsque le système de conduite de procédé n'identifie et n'affiche pas l'intervention manuelle (p. ex. l'ouverture d'une vanne de vidange) et que l'on oublie de rétablir l'état normal.

Contrôles sur place par le personnel d'exploitation

Dans les installations entièrement automatisées, les avaries et les dérangements (p. ex. défaut d'étanchéité, remplissage excessif d'un récipient, surchauffe d'un moteur), dont le programme ne tient pas compte et qui ne sont donc pas surveillés par des capteurs, ne peuvent plus être reconnus précocement lors de contrôles sur place par le personnel d'exploitation dans la même mesure que dans des installations conventionnelles commandées manuellement.

Malveillance

On doit tenir compte de la vulnérabilité des installations automatisées au sabotage. Une intervention malveillante pourrait p. ex. se faire par une manipulation du software, par des interventions on-line sur le système (localement ou par un réseau) ou par des virus informatiques (particulièrement dans des systèmes ouverts ou basés sur des PC).

Conclusions, mesures:

Principe, probabilité et portée

Le principe fondamental, selon lequel une simple faute ou la panne d'un seul composant d'une installation ou d'un système ne doit pas provoquer un état critique grave du point de vue sécurité, est aussi valable lors de l'utilisation de systèmes d'automation (on surestime quelque peu tant la fiabilité d'un composant isolé d'une installation ou d'un système que celle des collaborateurs exploitant l'installation). - Un système d'automation offre en premier lieu des possibilités pour réduire fortement la *probabilité* de survenance d'un événement indésirable, mais pas sa *portée*. Les mesures complémentaires découlant de l'analyse des risques gardent en général leur valeur lors de l'introduction d'un système d'automation.

Recherche des dangers

Le cahier CESICS 4 "Introduction à l'analyse des risques" présente les méthodes usuelles de recherche des dangers dans l'industrie chimique. Une méthode importante de cette recherche pour les installations chimiques est la "Hazard and operability study" (HAZOP, procédure PAAG). Dans "Computer control and human error" (voir la bibliographie), T. Kletz donne des références au sujet d'une méthodologie analogue, en cours de développement depuis quelque temps, pour la recherche des dangers dans les systèmes de conduite de procédé, "CHAZOP" (Computer hazard and operability study).

Catégories des dangers

Le tableau ci-dessous montre une classification possible des potentiels de danger en fonction de l'importance prévisible des dommages.

Potentiel	Importance prévisible des dommages			Exemples
	Homme	Environnement	Technique	
faible	pas de mise en danger, faibles nuisances par des odeurs, du bruit, etc.	pas de mise en danger notable, pas de conséquences hors de l'enceinte de l'usine	dégâts insignifiants à faibles aux bâtiments, aux appareils et aux produits	- filtration sur bande en milieu aqueux - sécheur à bande, produit humide (eau), pas ou difficilement combustible
moyen	blessures légères, éventuellement courte interruption du travail, pas de conséquences notables	atteinte réversible dans l'enceinte de l'usine, régénération complète	dégâts notables aux bâtiments, aux appareils et/ou aux produits	- la plupart des procédés en chimie des spécialités, en partie aussi les opérations de retraitement
élevé	blessures graves avec hospitalisation, conséquences graves, évacuation nécessaire	atteintes régionales irréversibles ou non, régénération seulement à long terme	destruction de bâtiments, d'appareils et/ou de produits coûteux	- réactions très exothermiques, substances à forte énergie de décomposition - produits particulièrement toxiques - opérations avec risque particulier d'explosion (manipulation d'éther éthylique, hydrogénations, etc.)

La conception des mesures de sécurité du système d'automation doit toujours être adaptée au potentiel de danger existant pour une phase donnée du procédé. A partir d'un potentiel moyen de danger, le système d'automation devrait être équipé, dans le software de l'utilisateur, p. ex. d'une auto-surveillance (watchdog), d'éléments redondants, ainsi que de tests de plausibilité et d'une corrélation des valeurs mesurées.

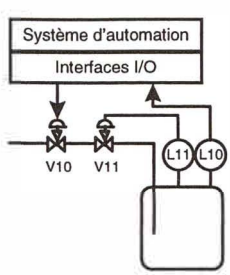
Niveau de sécurité indépendant

La sécurité ne doit pas dépendre du seul système d'automation installé lorsque le potentiel de danger est élevé. Dans de tels cas, il faut prévoir un niveau de sécurité indépendant pour sécuriser les paramètres critiques du procédé et pour déclencher un état de sécurité. Outre une redondance des capteurs et des actionneurs, cela implique en outre la redondance de la transmission et du traitement des signaux (y compris l'alimentation en énergie). Pour des tâches simples de surveillance et de sécurité, cela peut p. ex. se faire par une connexion par hardware des capteurs et des éléments actifs redondants. Il peut être avantageux, pour des installations comprenant des verrouillages complexes, de mettre en service un deuxième système d'automation (de préférence différent), comportant des comparaisons automatiques de signaux, des tests de plausibilité à intervalles réguliers, des contrôles de fonctionnement, ainsi que pour le déclenchement de positions de sécurité. - Deux exemples simples d'un niveau de sécurité indépendant sont présentés ci-après.

Positions de sécurité

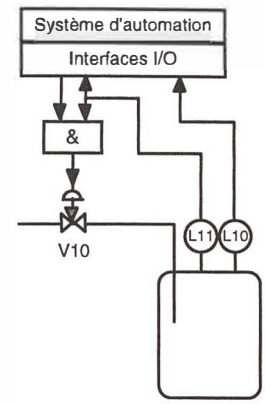
Lors de dérangements critiques sur le plan sécurité, des mesures doivent être déclenchées automatiquement, même sans intervention d'un opérateur, mettant l'installation dans un état de sécurité défini pour la phase du procédé en cours et l'y maintenant. Le retour au fonctionnement normal ne doit pas se faire automatiquement. La procédure de remise en route peut varier selon l'étape du procédé et doit être exactement décrite pour chaque cas prévisible.

Redondance du cheminement et du traitement du signal (par hardware)



Niveau de sécurité indépendant: Alarme de niveau haut redondante de V11/L11

Alarme de niveau haut avec verrouillage supplémentaire du hardware



Niveau de sécurité indépendant: Connexion par hardware de L11/V10 par un élément de verrouillage (&)

Ce montage remplit les critères d'un branchement sélectif "1 de 2" sur les plans de la détection et du traitement des signaux. Une erreur passive de l'ordinateur ne peut pas mettre la sécurité en cause.

Exigences pour les boucles de régulation

Les exigences devant être posées pour les circuits de mesure et de régulation peuvent beaucoup varier, selon qu'il s'agit d'éléments pour la conduite normale du procédé, de systèmes de surveillance (pour l'annonce à temps de déviations devant déclencher des mesures de correction) ou d'éléments de protection (pour éviter des états anormaux inacceptables, c.à.d. dangereux). Voir à ce sujet la NAMUR-Empfehlung NE 31 "Anlagensicherung mit Mitteln der Prozessleittechnik" (voir la bibliographie).

Tests de fonctionnement

Toutes les fonctions de surveillance et de sécurité doivent être testées à fond et les résultats de ces tests doivent figurer dans un procès-verbal. L'aptitude au fonctionnement des programmes importants pour la sécurité doit être périodiquement contrôlée.

Alimentation en énergie

Selon les résultats de l'analyse des risques, des dérangements prévisibles de l'alimentation en énergie (y compris l'alimentation de secours et les secteurs à basse tension) doivent être intégrés dans les considérations relatives à la sécurité du système d'automation. Les systèmes de conduite de procédé doivent être munis d'une alimentation secourue. Même le passage à l'alimentation de secours doit être testé dans des conditions réelles, car une coupure ou une baisse de tension, même très brève, peuvent très souvent survenir lors de ce passage.

Utilisation des possibilités de l'ordinateur

Si nécessaire, il faut aussi utiliser les possibilités de l'ordinateur pour reconnaître et éviter à temps des dérangements ou des erreurs n'amenant pas encore directement des états critiques du point de vue sécurité. On peut p. ex. introduire des limites inférieures et/ou supérieures d'acceptation des données chiffrées introduites (quantités, températures, etc.), une surveillance de l'exécution d'ordres selon leurs effets (p. ex. position de vannes, débit, vitesse de rotation d'un agitateur) ou le maintien de certaines fonctions de surveillance, même dans une installation provisoirement inutilisée.

Hiérarchisation des alarmes

Selon les dimensions de l'installation et le genre de dérangements survenant, plusieurs alarmes - dans des cas extrêmes plusieurs centaines - peuvent être déclenchées dans un délai extrêmement bref (pour l'incident de la centrale nucléaire de Three Mile Island: > 500 dans les premières minutes). Les opérateurs peuvent être complètement débordés dans un tel cas. Il est conseillé de classer hiérarchiquement les avis d'alarme possibles selon leur importance et de rendre ceux véritablement urgents mieux visibles, tant sur l'écran que sur la bande imprimée. Si possible, il faut aussi afficher simultanément les mesures à prendre. Le cas échéant, un arrêt total (shut-down) d'urgence peut être adéquat, lorsque trop d'alarmes prioritaires se déclenchent simultanément.

Analyse des risques accompagnant le projet

Le concept d'automation doit déjà être fixé définitivement durant la phase de planification d'une installation. Pour le développement du software, le groupe de projet doit définir aussi précisément que possible les divers opérations et déroulements (y compris les points de recoupement) et en faire une analyse des risques. De celle-ci découleront les mesures nécessaires (p. ex. verrouillages, redondance, refroidissement d'urgence). Des organigrammes de programmation (OP) pourront être établis sur cette base. L'OP est un moyen de communication dans une forme compréhensible tant par l'auteur du procédé que par le programmeur. Il montre les déroulements et les connexions de façon telle que le software établi d'après lui soit proprement structuré et visible dans son ensemble. L'analyse des risques doit être continuellement mise à jour, parallèlement à l'avancement du projet. - En matière de sécurité, le concept d'automation devrait au moins comporter les domaines partiels suivants:

- concept de sécurité du procédé, y compris un concept des points d'interruption sûrs du procédé
- concept d'alarme
- concept de service, de surveillance et d'intervention
- système d'information et concept d'enregistrement
- concept du software d'application
- concept de sécurité

L'automation en tant que mesure de sécurité ne doit pas simplement être "greffée ponctuellement" après coup sur une installation. Elle doit être planifiée et réalisée comme une partie intégrante du procédé, au même titre et en tenant compte de la chimie/physique, de l'homme et de l'installation.

Modifications du hardware et du software

Lors de modifications d'installations automatisées, soit de l'appareillage du procédé, soit du software ou du hardware du système d'automation, il existe souvent le risque de ne pas suffisamment reconnaître et prendre en considération des aspects importants de la sécurité. Il est recommandé d'établir un modus operandi en bonne et due forme pour l'exécution de modifications. Celui-ci réglera p. ex. les compétences et les responsabilités, l'information de toutes les instances intervenantes ou concernées, les tests de fonctionnement et de sécurité à exécuter, de même que la mise à jour soigneuse de la documentation concernant l'installation et le procédé, de l'analyse des risques, et, le cas échéant, des documents de formation et d'exercice.

Formation/instruction

La formation du personnel d'exploitation doit être adaptée aux possibilités techniques et à la complexité des installations. Elle doit être maintenue en permanence à un niveau suffisant. Le personnel d'exploitation doit notamment être en tout temps en mesure d'interpréter correctement l'état du déroulement du procédé et les avis de dérangements et d'agir en conséquence.

Responsible Care

Quelques définitions et explications

Arrêt d'urgence	L'expression peut avoir diverses significations, p. ex. interrupteur coupant le courant de toute une installation ("interrupteur des pompiers"). Dans le cadre de ce bulletin: interrupteur pour le déclenchement manuel de la position de sécurité du hardware.
Carte d'interface	Elément électronique de connexion, qui reçoit les signaux d'organes périphériques (capteurs, actionneurs), les transforme si nécessaire et les transmet à la CPU ou, inversement, transmet des signaux (ordres) de la CPU aux organes périphériques.
Common mode failure	Cause la plus dangereuse, du fait que des équipements de sécurité redondants sont souvent moins fiables en pratique que ce que l'on pourrait en attendre: défaillance de plusieurs éléments d'un système redondant, provoquée par la même cause, du fait de dépendances ignorées. Des causes fréquentes de common mode failure sont p. ex. – des influences extérieures "normales" telles que la poussière, les salissures, la température, l'humidité, la corrosion, les vibrations – des influences extérieures "inattendues" telles qu'une inondation, le feu, des coupures d'énergie, un tremblement de terre – des défauts du projet, de la fabrication ou du matériel – des erreurs de montage, d'entretien ou de remise en état – une spécification insuffisante des exigences. Le fait que des common mode failures aient fréquemment pour origine une erreur de réflexion lors de la conception de l'installation de sécurité aggrave encore le problème.
CPU	Central processing unit, processeur central d'un système d'automation; calculateur/ordinateur de procédé
Erreur active (erreur déclenchant un fonctionnement)	Défaut ayant pour conséquence que, p. ex. le système de sécurité se déclenche sans qu'un état critique existe (p. ex. parce qu'une sonde de température défectueuse simule un dépassement d'une valeur limite critique, ce qui active le refroidissement d'urgence).
Erreur passive (erreur empêchant un fonctionnement) - défaillance passive	Défaut ayant pour conséquence que, malgré un état critique de l'installation, p. ex. le système de sécurité ne se déclenche pas (p. ex. parce qu'une sonde de température défectueuse simule une température inférieure à la valeur de consigne, le chauffage se poursuit, bien que la température ait déjà atteint des valeurs critiques). **Le but principal de tout système de sécurité doit être d'éviter les erreurs passives**.

Etat de sécurité ...	Voir sous "Position (état) de sécurité ..."
Mesures complémentaires	La portée d'un événement peut être limitée par des mesures complémentaires lors d'une défaillance des éléments de sécurité préventifs (exemples: soupapes de sécurité, dilution d'urgence, installation Sprinkler).
Niveau de sécurité indépendant	Niveau prioritaire et totalement indépendant du système d'automation normal de l'installation, pour tous les capteurs et actionneurs importants pour la sécurité. Le déclenchement de ce niveau met l'installation en état de sécurité du hardware, indépendamment de l'état du système d'automation normal. Il peut aussi déclencher des mesures de sécurité supplémentaires (p. ex. dilution de la charge).
Position (état) de sécurité du hardware PSH	Position de sécurité qui n'est déterminée que par les éléments de mesure, de commande et de régulation technique utilisés (et leurs connexions), sur laquelle le système de commande n'a pas d'influence. Elle est principalement déclenchée lorsqu'il existe des indices de défectuosité du système de commande. Elle est conçue de telle façon que – la plupart des organes finaux reviennent en position de base sans énergie – la plupart des moteurs sont déclenchés – les éléments actifs (en général en petit nombre) restent dans leur état momentané (p. ex. agitateurs, pompes de circulation du chauffage et du refroidissement, clapets de ventilation). La PSH peut être déclenchée pour un appareil principal, un groupe d'appareils ou toute une installation.
Position (état) de sécurité du software PSS	Lors de l'apparition d'un état critique de l'installation, les éléments actifs reçoivent l'ordre de se mettre dans un état de sécurité défini par le software (programme) (vannes ouvertes, fermées ou restant en l'état momentané, moteurs en général déclenchés, vannes de régulation ou moteurs à vitesse variable en général sur 0 ou sur la valeur minimale du domaine de réglage). Caractéristiques: – le nombre de PSS est indéterminé (par appareil, par installation ou par étape du procédé). Il est néanmoins conseillé d'en limiter le nombre. – chaque PSS peut être adaptée de façon optimale à la cause qui la déclenche. – une remise en service normal simple est souhaitable. – une PSS ne doit être déclenchée que lorsque le système de commande est encore en état de fonctionner. S'il y a doute à ce sujet, il faut déclencher une PSH.

Redondance	Utilisation d'un nombre plus grand d'éléments, d'appareils ou de systèmes que le nombre minimum nécessaire pour accomplir une tâche. Exemples typiques: mesures multiples d'une même grandeur physique, couplage en série (pour assurer la fermeture) ou en parallèle (pour garantir l'ouverture) de vannes. La condition essentielle pour obtenir une véritable redondance est que les éléments redondants doivent être **indépendants l'un de l'autre**.
Test de plausibilité	Vérification d'une valeur analogique, dont le niveau du signal doit se situer entre 4 et 20 mA ou, pour les commandes pneumatiques, entre 0.2 et 1 bar. La plupart des défauts d'un appareil, tels qu'un court-circuit, une interruption, etc., ont pour conséquence un dépassement de ces limites dans un sens ou dans l'autre. Le test de plausibilité permet de ce fait de détecter jusqu'à 95% des erreurs.
Watchdog ("chien de garde")	Le watchdog est une procédure d'un ordinateur qui a pour tâche de vérifier périodiquement (fréquence type: 1 fois par seconde) toutes les fonctions "vitales" du système (à spécifier en détail).

Bibliographie complémentaire

- VDI/VDE 2180 Bl. 1 - 7 "Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Mess-, Steuerungs- und Regelungstechnik"

- NAMUR-Empfehlung NE 31 "Anlagensicherung mit Mitteln der Prozessleittechnik", 1993

- NAMUR-Empfehlung NE 33 "Anforderungen an Systeme zur Rezeptfahrweise", 1992

- DIN 57113 resp. VDE 0113

- "Programmable Electronic Systems in Safety Related Applications", Health and Safety Executive 1987, HMSO Publications Centre London

- "Out of Control", why control systems go wrong and how to prevent failure; Health and Safety Executive 1995, HMSO Publications Centre London

- "Computer Control and Human Error", T. Kletz, Institution of Chemical Engineers, Rugby England 19951995G

- "Anlagensicherung mit Mitteln der MSR-Technik", Strohmann, Oldenbourg-Verlag, 1983

- "Guidelines for Safe Automation of Chemical Processes" (G 12), Center for Chemical Process Safety (CCPS), AIChem, 1993 (ISBN 0-8169-0554-1)