Figure 58.62 • Efficacité des mesures prises contre les erreurs indépendamment du risque

CAUSES DES DÉFAILLANCES	EFFICACITÉ REQUISE DES MESURES DE CONTRÔLE OU DE PRÉVENTION DES DÉFAILLANCES POUR CHAQUE NIVEAU D'INTÉGRITÉ DE SÉCURITÉ			
Intégrité du matériel: défauts isolés	Contrôle des défaillances assuré par des mesures concernant la configuration ou les composants			
	1	2	3	4
Intégrité du matériel: défauts multiples par accumulation	Contrôle des défaillances assuré par des mesures concernant la configuration, les composants ou des mesures techniques			
	1	2	3	4
Intégrité des systèmes: matériels et logiciels	Mesures de prévention des défaillances			
	1	2	3	4
	Mesures de contrôle des défaillances			
	1	2	3	4
Intégrité des systèmes: environnement	Mesures de prévention des défaillances			
	1	2	3	4
	Mesures de contrôle des défaillances			
	1	2	3	4
Intégrité des systèmes: exploitation	Mesures de prévention des défaillances			
	1	2	3	4
	Mesures de contrôle des défaillances			
	1	2	3	4
Efficacité des mesures:	minimale	faible	moyenne	élevée

Figure 58.63 • Exemples de dispositions prises pour contrôler ou éviter les erreurs dans les systèmes informatiques

DÉFAILLANCES DU SEP	MESURES DE PRÉVENTION DES DÉFAILLANCES
Avant mise en service, par exemple: • Erreur dans les spécifications • Erreur dans le dimensionnement • Erreur de programmation • Erreur pendant la mise en œuvre	• Utilisation d'outils de développement • Conception structurée • Vérification de la CEM • Simulation • Analyse du programme • Tests de type • Equipes de conception différentes
Après mise en service, par exemple: • Défaillance de RAM/ROM • Défaillance du processeur • Défaillance des entrées-sorties • Erreur dans le déroulement du programme provoquée par IEM • Erreur introduite lors de modifications	MESURES DE CONTRÔLE DES DÉFAILLANCES • Redondance des matériels • Redondance des logiciels • Tests de RAM/ROM • Tests en ligne (voie unique) • Tests des entrées-sorties • Tests du processeur • Surveillance des sorties

CEM = Compatibilité électromagnétique
IEM = Interférences électromagnétiques

ces défauts doivent donc être prises lorsque les systèmes de sécurité sont encore au stade du développement. Ce type de mesures doit être pris non seulement au niveau de la conception, mais aussi aux stades suivants du développement, de l'installation et des modifications. Certaines défaillances peuvent être évitées si elles sont découvertes et corrigées à ces stades (DIN, 1990).

Comme le montre le dernier incident décrit, la panne d'un seul transistor peut entraîner la défaillance technique d'équipements automatisés extrêmement complexes. Etant donné que chaque circuit comprend plusieurs milliers de transistors et d'autres composants, de nombreuses mesures de prévention doivent être prises pour identifier ces défaillances qui se manifestent dans des conditions de fonctionnement et déclencher les réactions appropriées dans le système informatique. La figure 58.63 décrit les types de défaillances des systèmes électroniques programmables et donne des exemples des précautions qui peuvent être prises pour éviter ou contrôler les défaillances des systèmes informatiques (DIN, 1990; CEI, 1992).

Les possibilités et les perspectives des systèmes électroniques programmables (Automates programmables industriels (API)) en technologie de la sécurité

Les machines et les installations modernes deviennent de plus en plus complexes et doivent accomplir des tâches de plus en plus étendues dans des délais toujours plus courts. C'est la raison pour laquelle les systèmes informatiques se sont répandus dans presque tous les secteurs de l'industrie depuis le milieu des années soixante-dix. Cette complexité accrue a largement contribué à l'augmentation du coût de l'amélioration de la technologie de la sécurité appliquée à ces systèmes. Le recours aux logiciels et aux ordinateurs pose un défi majeur pour la sécurité sur le lieu de travail, mais permet en revanche de mettre en œuvre de nouveaux systèmes à tolérance d'erreur dans le domaine de la technologie de la sécurité.

Un vers amusant, mais aussi instructif d'Ernst Jandl, «Lichtung: Manche meinen lechts und rinks kann man nicht velwechsern, werch ein Illtum» aide à expliquer ce qu'on entend par le concept de tolérance d'erreur. Pour les besoins du français, on peut le transcrire ainsi: «Beaucoup pensent qu'on ne peut pas intelchangel omble et rumièle, querre elleul.» Malgré l'inversion des lettres *r* et *l*, un adulte normal comprend facilement cette phrase. Une personne n'ayant qu'une connaissance sommaire du français en serait capable elle aussi. Cette tâche est en revanche quasiment impossible pour un système de traduction automatique.

Cet exemple montre qu'un être humain peut réagir d'une façon beaucoup plus tolérante à l'erreur qu'une machine à traduire. En effet, l'être humain, comme tous les êtres vivants, est capable de tolérer certaines défaillances en les rapportant à son expérience. Si l'on considère les machines utilisées actuellement, on constate que la plupart pénalisent les défaillances de leurs utilisateurs non pas par un accident, mais par une diminution de la production. Cette particularité conduit les opérateurs à neutraliser ou à contourner les protections. La technologie informatique moderne met à la disposition de la sécurité au travail des systèmes en mesure de réagir intelligemment, c'est-à-dire de manière adaptée. De tels systèmes rendent ainsi possible un mode de comportement tolérant à l'erreur sur les machines les plus récentes. Ils commencent par avertir l'utilisateur en cas de fausse manœuvre et n'arrêtent la machine que s'il n'y a pas d'autre moyen d'éviter un accident. L'analyse des accidents montre qu'il existe dans ce domaine un potentiel considérable d'amélioration de la sécurité (Reinert et Reuss, 1991).

LES LOGICIELS ET LES ORDINATEURS: SYSTÈMES AUTOMATISÉS HYBRIDES

Waldemar Karwowski
et Jozef Zurada

Un système automatisé hybride (SAH) vise à intégrer les possibilités des machines à intelligence artificielle (basées sur la technologie informatique) et les capacités des personnes qui interagissent avec elles dans le cadre de leur travail. L'utilisation des systèmes SAH pose essentiellement le problème de la manière dont le sous-système humain et le sous-système machine devraient être conçus pour que l'on tire le meilleur parti des connaissances et des capacités de ces deux constituants du système hybride, et celui de la manière dont les opérateurs humains et les éléments de la machine devraient interagir afin que leurs fonctions se complètent. De nombreux systèmes automatisés hybrides ont évolué en tant que produits de l'application des méthodes modernes de gestion de l'information et du contrôle pour automatiser et intégrer différentes fonctions de systèmes technologiques souvent complexes. L'utilisation initiale des systèmes SAH s'est identifiée à l'introduction de systèmes informatiques dans la conception et l'exploitation de systèmes de contrôle en temps réel pour les réacteurs nucléaires, les usines chimiques et la fabrication des composants électroniques. A l'heure actuelle, ces systèmes sont présents également dans de nombreuses activités de services, comme le contrôle du trafic aérien ou les procédures de navigation de l'aviation civile, ainsi que dans la conception et l'utilisation de véhicules intelligents et de systèmes de navigation pour le transport routier.

Dans les systèmes technologiques modernes, les progrès constants de l'automatisation informatisée ont transformé la nature des tâches humaines, qui ne nécessitent plus des capacités sensorimotrices, mais des capacités cognitives, nécessaires à la résolution des problèmes, à la prise de décisions dans la surveillance des systèmes et aux tâches de contrôle hiérarchique. Par exemple, dans les systèmes de fabrication intégrée par ordinateur, les opérateurs humains ont essentiellement des tâches de surveillance de systèmes, de résolution de problèmes et de prise de décisions. Les activités cognitives du contrôleur humain dans un environnement SAH consistent à: 1) planifier les tâches sur une période donnée; 2) mettre au point des procédures (ou étapes) pour atteindre l'ensemble des objectifs prévus; 3) surveiller le déroulement des processus technologiques; 4) assurer «l'éducation» du système par le biais d'un ordinateur interactif; 5) intervenir en cas de comportement anormal du système ou de changement des priorités du contrôle; 6) obtenir des informations sur les effets des actions de contrôle grâce au retour d'information provenant du système (Sheridan, 1987).

La conception des systèmes hybrides

Les interactions opérateur-machine dans un système SAH impliquent l'utilisation de boucles de communication dynamiques entre les opérateurs humains et les machines intelligentes — processus qui comprend la collecte et le traitement des informations, le déclenchement et l'exécution de tâches de contrôle et la prise de décisions — au sein d'une structure de répartition des fonctions entre l'opérateur et la machine. Ces interactions devraient refléter au moins le haut niveau de complexité des systèmes automatisés hybrides, ainsi que les caractéristiques des opérateurs humains et les exigences des tâches. Le système automatisé hybride peut par conséquent se définir comme une fonction de cinq variables, à savoir:

$$\text{SAH} = (T, U, C, E, I)$$

où T = exigences de la tâche (physiques et cognitives); U = caractéristiques de l'utilisateur (physiques et cognitives); C = caractéristiques de l'automatisation (matériel et logiciel, y compris les interfaces informatiques); E = environnement du système; I = un ensemble d'interactions entre les éléments ci-dessus.

L'ensemble d'interactions I représente toutes les interactions possibles entre T, U et C dans E, quelles que soient leur nature ou la force de leur liaison. Ainsi, l'une des interactions possibles peut concerner la relation entre les données mises en mémoire dans l'ordinateur et les connaissances correspondantes que peut posséder l'opérateur. Les interactions I peuvent être élémentaires (c'est-à-dire limitées à l'association d'un seul élément à un autre), ou complexes, associant par exemple l'opérateur, le logiciel employé pour l'exécution de la tâche et l'interface physique avec l'ordinateur.

Les concepteurs de nombreux systèmes automatisés hybrides concentrent leurs efforts sur l'intégration assistée par ordinateur de machines et d'autres équipements complexes en tant qu'éléments d'une technologie informatisée et prêtent rarement beaucoup d'attention à la nécessité, pourtant de première importance, d'une intégration efficace de l'élément humain dans ces systèmes. De ce fait, un grand nombre des systèmes technologiques informatisés actuels ne sont pas totalement compatibles avec les capacités des opérateurs humains en ce qui concerne les aptitudes et les connaissances nécessaires à un contrôle et une surveillance efficaces de ces systèmes. Cette incompatibilité se manifeste à tous les niveaux des tâches de l'opérateur, de la machine et du couple opérateur-machine et peut être définie dans le cadre de l'individu ou dans celui de l'installation ou de l'entreprise dans leur ensemble. Les problèmes posés par l'intégration des personnes et de la technologie dans les entreprises manufacturières de pointe apparaissent aux premiers stades de la conception du système SAH. Ils peuvent être conceptualisés à l'aide du modèle suivant d'intégration de la complexité des interactions I entre les concepteurs du système D, les opérateurs humains H ou les utilisateurs potentiels du système et la technologie T:

$$I(H, T) = F[I(H, D), I(D, T)]$$

où I représente les interactions ayant lieu dans une structure SAH donnée et F les relations fonctionnelles entre les concepteurs, les opérateurs et la technologie.

Le modèle d'intégration ci-dessus montre que les interactions entre les utilisateurs et la technologie sont déterminées par le résultat de l'intégration des deux interactions précédentes, c'est-à-dire: 1) entre les concepteurs du système SAH et les utilisateurs potentiels; et 2) entre les concepteurs et la technologie SAH (au niveau des machines et de leur intégration). On notera que s'il existe en général de fortes interactions entre les concepteurs et la technologie, on ne trouve que de très rares exemples de relations aussi fortes entre les concepteurs et les opérateurs.

On peut avancer que, même dans les systèmes les plus automatisés, le rôle de l'humain reste déterminant pour obtenir de bonnes performances en cours de fonctionnement. Bainbridge (1983) a identifié une série de problèmes qui concernent l'exploitation des systèmes SAH et qui découlent de la nature même de l'automatisation:

1. *Opérateurs qui ne se tiennent plus au courant*. Les opérateurs humains sont présents dans le système pour exercer un contrôle si nécessaire, mais comme ils ne se tiennent plus au courant des évolutions, ils ne peuvent plus conserver les aptitudes manuelles et la longue connaissance du système qui sont souvent nécessaires en cas d'urgence.
2. *Images mentales obsolètes*. Les opérateurs humains risquent de ne pas pouvoir réagir rapidement aux modifications dans le comportement du système s'ils n'ont pas été suffisamment

attentifs au fonctionnement de celui-ci dans les périodes précédentes. Il se peut également que leur connaissance de ce fonctionnement ou l'image qu'ils en ont ne permette pas de déclencher ou de mettre en œuvre les réactions nécessaires.

3. *Disparition des compétences des prédécesseurs*. Les nouveaux opérateurs ne sont pas toujours en mesure d'acquérir la connaissance du système informatisé que seule l'expérience donne et, de ce fait, ils ne pourront pas exercer efficacement le contrôle requis.
4. *Autorité de l'automatisation*. Si le système informatisé a été mis en place parce qu'il exécute mieux les tâches que l'opérateur humain, on peut se demander sur quelles bases l'opérateur pourra déterminer si les décisions prises par le système sont correctes ou non.
5. *Apparition de nouveaux types d'erreurs humaines dues à l'automatisation*. Les systèmes informatisés conduisent à de nouveaux types d'erreurs et donc à des accidents qui ne peuvent pas être soumis aux techniques d'analyses classiques.

L'attribution des tâches

L'une des questions importantes pour la conception d'un système SAH est de déterminer le nombre et la nature des fonctions ou des responsabilités à attribuer respectivement aux opérateurs humains et aux ordinateurs. On distingue généralement trois catégories fondamentales de problèmes d'attribution des tâches: 1) la répartition des tâches entre le contrôleur humain et l'ordinateur; 2) la répartition des tâches entre les opérateurs; 3) la répartition des tâches entre l'ordinateur de contrôle et l'ordinateur de base. Dans une situation idéale, les décisions d'attribution devraient être prises dans le cadre d'une procédure structurée préalablement à la conception de base du système. Malheureusement, ce processus systématique est rarement possible, du fait que les fonctions à attribuer nécessitent parfois un examen plus poussé ou doivent être exécutées de manière interactive entre la composante humaine et la composante machine du système, c'est-à-dire par application du paradigme de contrôle hiérarchique. L'attribution des tâches dans les systèmes automatisés hybrides devrait s'attacher à délimiter les responsabilités de contrôle de l'opérateur et de l'ordinateur et prendre en compte la nature des interactions entre l'opérateur et les systèmes informatiques d'aide à la décision. Il conviendrait de considérer également les moyens du transfert de l'information entre la machine et les interfaces d'entrée-sortie de l'opérateur, ainsi que la compatibilité des logiciels avec les aptitudes humaines à la résolution des problèmes.

Dans les approches traditionnelles de la conception et de la gestion des systèmes automatisés hybrides, les travailleurs étaient considérés comme des systèmes d'entrée-sortie déterministes, et on avait tendance à négliger la nature téléologique du comportement humain, c'est-à-dire un comportement orienté vers les objectifs et reposant sur l'acquisition des informations pertinentes et le choix des objectifs (Goodstein, Anderson et Olsen, 1988). Pour donner de bons résultats, la conception et la gestion des systèmes automatisés hybrides avancés doit reposer sur une description des fonctions mentales humaines nécessaires à une tâche déterminée. L'approche de «l'ingénierie cognitive» (décrite plus en détail ci-après) propose que les systèmes hybrides opérateur-machine soient conçus, élaborés, analysés et évalués en termes de processus mentaux humains, c'est-à-dire que l'on tienne compte de la représentation mentale des systèmes adaptatifs par l'opérateur. Corbett (1988) a défini comme suit les critères d'une approche centrée sur l'humain de la conception et de l'exploitation des systèmes SAH.

1. *Compatibilité*. L'exploitation du système ne devrait pas nécessiter des compétences sans rapport avec celles qui existent, mais devrait permettre à ces dernières d'évoluer. L'opérateur devrait apporter et recevoir des informations compatibles avec les pratiques courantes, de manière que l'interface corresponde à ses connaissances et compétences déjà acquises.
2. *Transparence*. On ne peut pas contrôler un système sans le comprendre. Pour que son apprentissage soit facilité, l'opérateur doit donc être en mesure de «voir» les processus internes du logiciel de contrôle du système. Un système transparent facilite l'établissement par les utilisateurs d'un modèle interne des fonctions de prise de décisions et de contrôle que le système est capable d'assurer.
3. *Minimum de surprises*. Le système ne devrait rien faire qui puisse dérouter les opérateurs par rapport aux informations dont ils disposent sur l'état détaillé du système à un moment donné.
4. *Contrôle des perturbations*. Les tâches incertaines au sens de l'analyse de la structure des choix devraient être sous le contrôle de l'opérateur humain, avec une aide informatisée à la prise de décisions.
5. *Faillibilité*. Les connaissances et compétences implicites des opérateurs humains ne devraient pas être écartées de la conception du système. Les opérateurs ne devraient jamais être placés dans une situation où ils assisteraient, impuissants, à une opération incorrecte dictée par le logiciel.
6. *Réversibilité des erreurs*. Le logiciel devrait fournir par anticipation, à l'opérateur, des informations sur les conséquences probables d'une opération ou d'une stratégie particulières.
7. *Souplesse de fonctionnement*. Le système devrait laisser aux opérateurs humains la liberté de choisir le meilleur compromis entre les besoins et les limites des ressources en changeant de stratégie d'exploitation sans perdre l'assistance du logiciel de contrôle.

L'ingénierie cognitive des facteurs humains

L'ingénierie cognitive des facteurs humains s'intéresse à la manière dont les opérateurs humains prennent des décisions sur le lieu de travail, résolvent des problèmes, formulent des plans et acquièrent de nouvelles compétences (Hollnagel et Woods, 1983). Les comportements des opérateurs à l'intérieur d'un système SAH peuvent être classés en trois grandes catégories, selon Rasmussen (1983):

Le comportement machinal correspond à une activité sensori-motrice mise en œuvre dans le cadre d'actions ou d'activités exécutées sans contrôle conscient, et qui représente des schémas de comportements naturels, automatiques et fortement intégrés. Les activités humaines appartenant à cette catégorie sont considérées comme une séquence d'actes professionnels organisée en fonction d'une situation donnée. Le comportement machinal est donc l'expression de schémas de comportement plus ou moins mémorisés ou d'instructions préprogrammées dans un domaine spatio-temporel.

1. *Le comportement procédural* est orienté vers les objectifs, structuré grâce à un contrôle par anticipation par le biais d'une règle ou d'une procédure mémorisées, c'est-à-dire une activité ordonnée permettant de composer une séquence de sous-programmes dans une situation de travail familière. La règle est généralement suggérée par l'expérience passée et reflète les propriétés fonctionnelles qui régissent le comportement de l'environnement. Les activités basées sur un comportement procédural reposent sur un savoir-faire explicite en ce qui concerne l'application des règles adéquates. L'ensemble de données pour la décision se compose de références en vue de la reconnaissance et de l'identification d'états, d'événements ou de situations.
2. *Le comportement cognitif* est contrôlé par les objectifs, ceux-ci étant formulés de façon explicite à partir d'une connaissance de l'environnement et des objectifs de la personne. La structure interne du système est représentée par un «modèle men-

tal». Ce type de comportement permet de développer et de tester différents plans dans des conditions de contrôle inhabituelles et donc incertaines, et il est nécessaire lorsque l'expérience pratique ou les règles sont indisponibles ou inadéquates et que l'on doit les remplacer par la résolution de problèmes et la planification.

Dans la conception et la gestion d'un système SAH, il convient de prendre en compte les caractéristiques cognitives des travailleurs pour assurer que le fonctionnement du système soit compatible avec le modèle intérieur selon lequel la personne décrit les fonctions de ce système. Le niveau de description du système devrait donc être transféré des aspects du comportement machinal à ceux des comportements procédural et cognitif, et l'on devrait appliquer des méthodes appropriées d'analyse cognitive des tâches pour identifier le modèle de système de l'opérateur. La mise au point d'un système SAH pose un problème connexe, celui de la conception de moyens de transmission de l'information entre l'opérateur et les éléments du système automatisé, tant au niveau physique qu'au niveau cognitif. Ce transfert d'informations devrait être compatible avec les modes d'information utilisés aux différents niveaux de l'exploitation du système, à savoir visuel, verbal, tactile ou hybride. Cette compatibilité informationnelle est le gage que les différentes formes de transfert d'information ne comporteront qu'un minimum d'incompatibilité entre le support et la nature de l'information. Ainsi, un affichage visuel est préférable pour la transmission des informations spatiales, tandis que les vecteurs auditifs peuvent servir à acheminer des informations textuelles.

L'opérateur humain construit assez souvent un modèle interne qui décrit l'exploitation et le fonctionnement du système d'après son expérience, sa formation ou les instructions qu'il a reçues relativement au type d'interface opérateur-machine en cause. Compte tenu de cette réalité, les concepteurs d'un système SAH devraient s'efforcer d'intégrer aux machines (ou à d'autres systèmes artificiels) un modèle des caractéristiques physiques et cognitives de l'opérateur humain, c'est-à-dire de donner au système une image de l'opérateur (Hollnagel et Woods, 1983). Ils devraient également tenir compte du niveau d'abstraction de la description du système et des différentes catégories de comportement de l'opérateur à considérer. Ces niveaux d'abstraction pour la modélisation du comportement humain dans l'environnement de travail sont: 1) forme physique (structure anatomique); 2) fonctions physiques (fonctions physiologiques); 3) fonctions généralisées (mécanismes psychologiques et processus cognitifs et affectifs); 4) fonctions abstraites (traitement de l'information); 5) motivations fonctionnelles (structures de valeurs, mythes, religions, interactions humaines) (Rasmussen, 1983). Ces cinq niveaux doivent être pris en compte simultanément par les concepteurs pour assurer l'efficacité des systèmes SAH.

La conception du logiciel du système

Etant donné que le logiciel est un élément essentiel d'un environnement SAH, son développement, y compris la conception, les tests, le fonctionnement et les modifications, ainsi que sa fiabilité, devraient être considérés aux premiers stades du développement du système SAH. Cela devrait permettre de réduire les coûts de la détection et de la suppression des erreurs. Il est toutefois difficile d'évaluer la fiabilité des éléments humains d'un système SAH, car les possibilités de modéliser les performances humaines dans l'exécution des tâches, la charge de travail ou les erreurs potentielles restent limitées. Un travail mental excessif ou insuffisant peut respectivement conduire au surmenage ou à l'ennui, avec pour conséquence une dégradation des performances humaines, suivie d'erreurs et d'une aggravation du risque d'accidents. Les concepteurs d'un système SAH devraient employer des interfaces adaptatives, faisant appel aux techniques de l'intelligence artificielle, pour résoudre ces problèmes. Outre la compatibilité opérateur-machine, la question de l'adaptabilité réciproque entre l'opérateur et la machine devrait être considérée afin de réduire les niveaux de stress dans les cas de possibles dépassements des capacités humaines.

En raison du niveau de complexité élevé de nombreux systèmes automatisés hybrides, l'identification des risques potentiels liés au matériel, au logiciel, aux procédures d'exploitation et aux interactions opérateur-machine de ces systèmes joue un rôle déterminant dans le succès des efforts en vue de réduire les dommages matériels et corporels. Les risques pour la sécurité et la santé que présentent les systèmes automatisés hybrides complexes, comme ceux qui font appel à la technologie de la fabrication assistée par ordinateur (FAO), sont manifestement l'un des aspects les plus critiques de la conception et de l'exploitation de ces systèmes.

Les problèmes de sécurité des systèmes

Les environnements automatisés hybrides, avec leur important potentiel de comportement erratique du logiciel de contrôle en cas de perturbation, ont fait naître une nouvelle génération de risques d'accidents. A mesure que les systèmes automatisés hybrides deviennent plus polyvalents et plus complexes, les perturbations du système, y compris les problèmes de démarrage et d'arrêt ainsi que les écarts dans le contrôle du système, peuvent accroître sensiblement la possibilité de graves dangers pour les opérateurs. Paradoxalement, dans de nombreuses situations anormales, les opérateurs comptent habituellement sur le bon fonctionnement des sous-systèmes de sécurité automatiques, ce qui peut accroître le risque d'accidents graves. Une étude d'accidents liés à des dysfonctionnements de systèmes techniques de contrôle a révélé, par exemple, que le tiers environ des séquences d'accident impliquaient une intervention humaine sur la boucle de contrôle du système perturbé.

Etant donné que les mesures de sécurité classiques ne peuvent pas être facilement adaptées aux environnements SAH, les stratégies de contrôle et de prévention des accidents devraient être reconsidérées en fonction des caractéristiques propres à ces systèmes. Par exemple, dans le domaine des technologies de fabrication avancées, de nombreux processus se caractérisent par l'existence d'importants flux d'énergie difficiles à prévoir par les opérateurs. De plus, les problèmes de sécurité se présentent généralement aux interfaces entre les sous-systèmes, ou lorsque les perturbations du système progressent d'un sous-système à un autre. Selon l'Organisation internationale de normalisation (ISO, 1994b), les risques associés à l'automatisation industrielle varient selon les types de machines intégrés au système de fabrication en cause et selon la manière dont le système est installé, programmé, utilisé, entretenu et réparé. Par exemple, une comparaison entre les accidents liés à des robots en Suède et d'autres types d'accidents a montré que les robots pouvaient être les plus dangereuses de toutes les machines utilisées dans les industries manufacturières avancées. Le taux d'accidents en rapport avec des robots industriels était estimé à un accident grave pour 45 années-robot, supérieur au taux d'un accident pour 50 années-machine dans le cas des presses industrielles. Il convient de noter à ce propos qu'aux Etats-Unis les presses industrielles étaient responsables d'environ 23% de la totalité des accidents mortels liés aux machines dans l'industrie métallurgique sur la période 1980-1985, les presses mécaniques venant en tête pour le produit gravité × fréquence dans le cas des accidents non mortels.

Les dispositifs mis en œuvre dans les technologies de fabrication avancées comportent de nombreuses parties mobiles qui présentent des dangers pour les travailleurs en raison de changements de position complexes hors du champ visuel des opérateurs. Du fait

de la rapidité des progrès technologiques dans la fabrication intégrée par ordinateur, il est devenu impératif d'étudier les effets des technologies de fabrication avancées sur les travailleurs. Afin d'identifier les dangers occasionnés par les différents composants d'un environnement SAH de ce type, il est nécessaire de procéder à une analyse approfondie des accidents antérieurs. Dans les rapports sur les accidents en relation avec des machines conduites par des opérateurs, il est cependant difficile de déterminer la part qui revient aux accidents dus à des robots, et il se peut donc qu'un pourcentage élevé d'accidents de ce type ne soient pas signalés comme tels. Selon la réglementation japonaise sur la sécurité et la santé «les robots industriels actuels ne sont pas équipés de systèmes de sécurité fiables et il n'est pas possible de protéger les travailleurs contre les dangers qu'ils présentent, à moins d'en réglementer l'utilisation». Les résultats de l'étude conduite par le ministère japonais du Travail sur les accidents liés aux robots industriels (Sugimoto, 1987), portant sur 190 usines et 4 341 robots en service, ont révélé l'existence de 300 perturbations liées aux robots, dont 37 cas d'actions dangereuses ayant failli conduire à un accident, 9 cas d'accidents avec lésions et 2 cas d'accidents mortels. D'autres études montrent que l'automatisation informatisée n'élève pas nécessairement le niveau global de la sécurité, étant donné qu'il n'est pas possible de se protéger des pannes matérielles par les seules fonctions du logiciel et que les contrôleurs du système ne sont pas toujours d'une extrême fiabilité. En outre, dans un système SAH complexe, on ne peut pas se fier exclusivement aux détecteurs de sécurité pour déceler une situation dangereuse et prendre les mesures de protection voulues.

Les effets de l'automatisation sur la santé humaine

Comme on l'a vu précédemment, les personnes qui travaillent dans des environnements SAH ont essentiellement des activités de contrôle hiérarchique, de surveillance, d'assistance au système et de maintenance. On peut également classer ces activités en quatre grands groupes: 1) programmation des tâches, c'est-à-dire codage des instructions de guidage et de contrôle des machines; 2) surveillance de la production du système et de ses composants de contrôle; 3) maintenance des composants du système en vue de prévenir ou d'atténuer les dysfonctionnements des machines; 4) exécution de différentes tâches connexes. Un grand nombre d'études récentes sur l'impact des systèmes sur le bien-être des travailleurs ont conclu que, bien que l'emploi d'un tel système dans la production ait pu éliminer des tâches pénibles et dangereuses, le travail dans cet environnement peut se révéler déplaisant et stressant pour le personnel. Parmi les sources de stress figurent l'obligation d'un contrôle permanent dans de nombreuses applications SAH, la portée limitée des activités confiées, le faible niveau d'intervention des travailleurs autorisé par la conception du système et les risques pour la sécurité associés à la nature imprévisible et incontrôlable des équipements. Même si certains travailleurs participant aux activités de programmation et de maintenance estiment qu'il s'agit là d'un défi à relever qui peut avoir un effet positif sur leurs conditions de travail, cet effet est souvent compensé par la nature complexe et exigeante de ces activités ainsi que par la pression exercée par la hiérarchie pour que ces activités soient menées à bien rapidement.

Bien que dans certains environnements SAH les opérateurs soient tenus à l'écart des sources d'énergie traditionnelles (flux de travail et mouvements de la machine) en fonctionnement normal, de nombreuses tâches doivent encore être effectuées au contact direct d'autres sources d'énergie. En raison de l'augmentation constante du nombre des éléments des système SAH, il est nécessaire d'accorder une attention particulière au confort et à la sécurité des travailleurs et à l'élaboration de mesures efficaces de prévention des accidents, compte tenu en particulier du fait que les travailleurs ne sont plus en mesure de s'adapter à la complexité croissante de ces systèmes.

Pour répondre aux besoins actuels de prévention des accidents et de sécurité des travailleurs dans le domaine de la fabrication intégrée par ordinateur, le Comité ISO sur les systèmes d'automatisation industrielle a proposé une nouvelle norme de sécurité intitulée *Systèmes d'automatisation industrielle. Sécurité des systèmes de fabrication intégrée. Prescriptions fondamentales* (ISO, 1994b). Cette norme internationale, élaborée pour tenir compte des risques particuliers des systèmes de fabrication intégrés comprenant des machines industrielles et des équipements annexes, a pour objet de réduire au minimum les risques de lésions pour le personnel travaillant sur un système de fabrication intégré ou à proximité. Les principales sources de risques pour les opérateurs de systèmes de FAO, telles qu'elles ont été déterminées dans cette norme, sont indiquées dans la figure 58.64.

Les erreurs humaines et les erreurs du système

Dans un système SAH, les dangers peuvent provenir du système lui-même, de son association avec d'autres équipements présents dans l'environnement physique ou d'interactions entre les personnes et le système. L'accident corporel n'est que l'une des conséquences possibles des interactions humain-machine dans des situations dangereuses; les quasi-accidents et les dommages matériels sont beaucoup plus fréquents (Zimolong et Duda, 1992). L'apparition d'une erreur peut avoir l'une des conséquences suivantes: 1) l'erreur passe inaperçue; 2) le système est capable de compenser l'erreur; 3) l'erreur conduit à une panne de la machine ou à un arrêt du système; 4) l'erreur conduit à un accident.

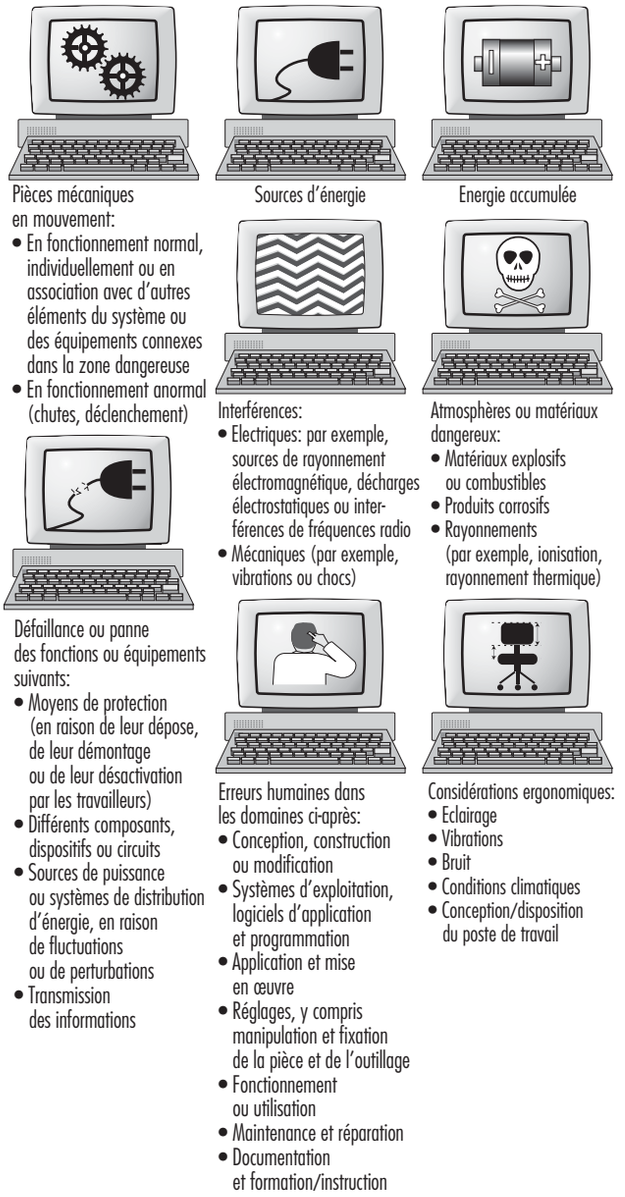
Etant donné que toutes les erreurs humaines entraînant un incident critique ne provoquent pas nécessairement un accident, il convient en outre de classer les conséquences selon les catégories ci-après: 1) incident mettant en cause la sécurité (c'est-à-dire tout événement non intentionnel, quelles que soient ses conséquences, lésions, dommages ou pertes); 2) accident (c'est-à-dire événement mettant en cause la sécurité et entraînant des lésions, des dommages ou des pertes); 3) incident avec dommages (c'est-à-dire événement mettant en cause la sécurité et entraînant des dommages matériels); 4) quasi-accident (c'est-à-dire événement mettant en cause la sécurité et lors duquel des lésions, des dommages ou des pertes ont été évités de peu et fortuitement); 5) accident potentiel (c'est-à-dire événement mettant en cause la sécurité et qui aurait pu occasionner des lésions, des dommages ou des pertes mais qui, en raison des circonstances, n'a même pas eu pour résultat un quasi-accident).

On peut distinguer trois types fondamentaux d'erreurs humaines dans un système SAH:

1. Inattentions et omissions relativement aux compétences.
2. Erreurs relativement aux règles.
3. Erreurs relativement aux connaissances.

Cette taxinomie, inventée par Reason (1990), repose sur une modification de la classification compétences-règles-connaissances de Rasmussen précédemment décrite pour les performances humaines. Au niveau des compétences, les performances humaines sont régies par un schéma mémorisé d'instructions préprogrammées, représentées sous la forme de structures analogiques dans un domaine spatio-temporel. Le niveau des règles s'applique à la gestion de problèmes familiers dont les solutions sont régies par des règles mémorisées (dites «productions» dans la mesure où elles sont appelées, ou produites, à la demande). Ces règles imposent de faire des diagnostics (ou jugements) ou de prendre certaines mesures correctives compte tenu de l'application de conditions qui exigent une réaction appropriée. A ce niveau, les erreurs humaines sont en général associées à des erreurs de classification

Figure 58.64 • Principales sources de dangers dans la fabrication assistée par ordinateur (FAO)



Source: ISO, 1994.

des situations conduisant soit à l'application de la mauvaise règle, soit à une erreur dans les jugements et procédures rappelés pour le cas en question. Les erreurs relatives aux connaissances se produisent dans des situations nouvelles, pour lesquelles les actions doivent être planifiées «en ligne», c'est-à-dire au moment même, selon des processus analytiques conscients et à l'aide de connaissances mémorisées. Les erreurs à ce niveau découlent de l'insuffisance des ressources et du caractère incomplet ou erroné des connaissances.

Les systèmes génériques de modélisation des erreurs (Generic Error-Modelling Systems (GEMS)) proposés par Reason (1990), qui tentent de déterminer les origines des types fondamentaux d'erreurs humaines, peuvent servir à établir la taxinomie du comportement humain dans un système SAH. Les GEMS s'efforcent d'intégrer deux domaines distincts de recherche des erreurs: 1) les inattentions et omissions, dans lesquelles l'action s'écarte de l'intention par suite d'erreurs d'exécution ou de mémorisation; et 2) les erreurs proprement dites, dans lesquelles l'action se déroule conformément au plan, mais où ce plan n'est pas adapté à l'objectif recherché.

L'évaluation et la prévention des risques dans la fabrication assistée par ordinateur (FAO)

Selon la norme ISO (ISO, 1994b), l'évaluation des risques en FAO doit être effectuée de manière à réduire au minimum tous les risques et à servir de base pour déterminer des objectifs et des mesures de sécurité dans l'élaboration des programmes ou des plans visant à créer un environnement de travail sûr et à garantir la sécurité et la santé du personnel. Les dangers du travail dans des environnements SAH peuvent être caractérisés de la façon suivante: 1) l'opérateur humain peut avoir à pénétrer dans la zone dangereuse pour remédier à des incidents ou effectuer des tâches de révision ou de maintenance; 2) la zone dangereuse est difficile à déterminer, à observer ou à contrôler; 3) le travail peut être monotone; 4) les accidents qui se produisent dans les systèmes de fabrication intégrée par ordinateur sont souvent graves. Chaque danger identifié devrait être évalué du point de vue des risques qu'il présente, et il convient de déterminer et de mettre en place des mesures de sécurité appropriées en vue de réduire ces risques au minimum. Les dangers devraient également être estimés du point de vue de tous les aspects d'un processus donné: l'unité elle-même, l'interaction entre unités, les parties en service du système et le fonctionnement du système complet dans l'ensemble des modes et conditions d'exploitation prévus, y compris les conditions dans lesquelles les moyens de protection normaux sont désactivés pour la programmation, les vérifications, les recherches de pannes, la maintenance ou les réparations.

La phase de conception de la stratégie de sécurité de la norme ISO (ISO, 1994b) pour la FAO comprend les éléments ci-après:

- spécification des limites des paramètres du système;
- application d'une stratégie de sécurité;
- identification des dangers;
- évaluation des risques associés;
- suppression des dangers ou diminution des risques dans toute la mesure du possible.

Les spécifications de la sécurité du système devraient comprendre:

- une description des fonctions du système;
- un plan ou un modèle du système;
- les résultats d'une étude de l'interaction des divers processus de travail et des activités manuelles;
- une analyse des séquences du processus, y compris les interactions manuelles;
- une description des interfaces avec les convoyeurs ou les lignes de transport;
- les organigrammes des processus;
- les plans d'implantation;
- les plans des dispositifs d'alimentation et d'évacuation;
- la détermination de l'espace nécessaire pour l'alimentation et l'évacuation des matériaux;
- les rapports d'accidents disponibles.

Conformément à la norme ISO (ISO, 1994b), toutes les prescriptions nécessaires pour garantir la sécurité de fonctionnement d'un système de FAO devraient être prises en compte dans la conception des procédures de planification systématique de la sécurité. Cela comprend toutes les mesures de protection pour réduire efficacement les risques, et cela exige:

- l'intégration de l'interface opérateur-machine;
- la définition précoce de la position des personnes intervenant dans le système (dans le temps et dans l'espace);
- une étude précoce des moyens de réduire le travail isolé;
- la prise en compte des éléments de l'environnement.

La procédure de planification de la sécurité devrait notamment tenir compte des problèmes de sécurité ci-après en matière de FAO:

- *Sélection des modes de fonctionnement du système*. Les équipements de commande devraient permettre au moins les modes de fonctionnement suivants: 1) mode normal ou de production (c'est-à-dire avec tous les dispositifs de protection normaux reliés et en service); 2) fonctionnement avec neutralisation de certains dispositifs de protection normaux; 3) fonctionnement empêchant l'apparition de situations dangereuses par l'action du système ou par une opération manuelle à distance (par exemple, fonctionnement local, isolation de la source d'énergie ou blocage mécanique de conditions dangereuses).
- *Formation, installation, mise en service et essais de fonctionnement*. Lorsqu'il est nécessaire que du personnel pénètre dans la zone dangereuse, les mesures de sécurité suivantes devraient être prévues dans le système de contrôle: 1) action maintenue (type commande de l'homme mort); 2) dispositif de validation; 3) vitesse réduite; 4) puissance réduite; 5) arrêt d'urgence mobile.
- *Sécurité lors de la programmation, de la maintenance et des réparations*. Pendant la programmation, seul le programmeur devrait être autorisé à pénétrer dans l'espace protégé. Des procédures d'inspection et de maintenance devraient être prévues pour garantir que le système fonctionne en permanence comme prévu. Le programme d'inspection et de maintenance devrait tenir compte des recommandations du fournisseur du système et des fournisseurs des différents éléments de celui-ci. Il va sans dire que le personnel assurant la maintenance ou les réparations devrait être formé aux procédures nécessaires à l'accomplissement des tâches requises.
- *Dépannage*. Lorsqu'un dépannage impose de pénétrer dans l'espace protégé, l'opération doit avoir lieu après une déconnexion sûre (ou, si possible, après une condamnation). Des mesures complémentaires devraient être prises pour éviter l'apparition d'une situation dangereuse à la suite d'une fausse manœuvre. Lorsque des risques peuvent apparaître pendant un dépannage sur certaines parties du système ou sur les machines des systèmes voisins, ces systèmes doivent eux aussi être mis hors service et protégés contre un démarrage intempestif. Il conviendrait d'attirer l'attention, au moyen d'instructions et de signaux d'avertissement, sur le fait que l'on procède à un dépannage sur des éléments qui ne peuvent pas être complètement surveillés.

Le contrôle des perturbations des systèmes

Dans de nombreuses installations SAH utilisées en fabrication assistée par ordinateur, les opérateurs remplissent le plus souvent des tâches de contrôle, de programmation, de maintenance, de préréglage, d'entretien ou de recherche de pannes. Les perturbations du système conduisent à des situations qui obligent les travailleurs à pénétrer dans les zones dangereuses. On peut donc admettre que ces perturbations restent la principale raison des interventions humaines en FAO, étant donné que la programmation des systèmes s'effectue le plus souvent hors des zones à accès restreint. L'un des principaux problèmes de sécurité dans la FAO consiste donc à prévenir les perturbations, car la plupart des risques surviennent au stade de la recherche de pannes. Eviter les perturbations est un objectif commun à la recherche de la sécurité et à celle du rendement.

Une perturbation dans un système de FAO est un état ou une fonction du système qui s'écarte de l'état prévu ou souhaité. Outre leurs effets sur la productivité, les perturbations de la FAO ont une incidence directe sur la sécurité des personnes impliquées dans l'exploitation du système. Une étude finlandaise (Kuivanen, 1990) a montré que la moitié environ des perturbations en fabrication automatisée compromettent la sécurité des travailleurs. Les principales causes des perturbations étaient des erreurs de conception du système (34%), des défaillances des composants (31%), des erreurs humaines (20%) et des facteurs extérieurs (15%). La plupart des défaillances de machines étaient provoquées par le système de contrôle et, dans celui-ci, la plupart des défaillances se produisaient dans les détecteurs. Un moyen efficace d'accroître le niveau de sécurité des installations de FAO consiste à réduire le nombre des perturbations. Bien que les actions humaines sur les systèmes perturbés permettent d'éviter des accidents dans un environnement SAH, elles peuvent également y contribuer. Par exemple, une étude des accidents liés à des dysfonctionnements de systèmes de contrôle techniques a montré qu'environ un tiers des séquences d'accident comportaient une intervention humaine sur la boucle de contrôle du système perturbé.

Les grands sujets de recherche en matière de prévention des perturbations dans la FAO concernent: 1) les principales causes des perturbations; 2) les composants et fonctions peu fiables; 3) l'impact des perturbations sur la sécurité; 4) l'impact des perturbations sur le fonctionnement du système; 5) les dommages matériels; 6) les réparations. La sécurité des systèmes SAH devrait être planifiée au stade de la conception du système, en accordant toute l'attention voulue à la technologie, aux personnes et à l'organisation, et elle devrait faire partie intégrante du processus global de planification technique des systèmes SAH.

La conception des systèmes SAH: les défis futurs

Pour tirer le meilleur parti des systèmes automatisés hybrides qui viennent d'être décrits, il est nécessaire d'adopter une vision nettement plus large du développement de ces systèmes, reposant sur l'intégration des personnes, de l'organisation et de la technologie. Trois grands types d'intégration devraient être mis en œuvre:

1. *Intégration des personnes*, en assurant une communication efficace entre elles.
2. *Intégration humain-ordinateur*, par la mise au point d'interfaces et d'interactions adaptées entre les personnes et les ordinateurs.
3. *Intégration technologique*, en assurant des interfaces et des interactions efficaces entre les machines.

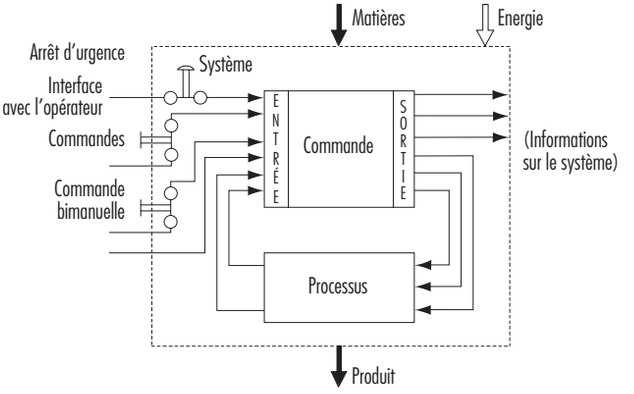
La conception des systèmes automatisés devrait répondre aux critères minimaux ci-après: 1) flexibilité; 2) adaptation dynamique; 3) meilleures capacités de réaction; 4) nécessité de motiver le personnel et de mieux exploiter ses compétences, son jugement et son expérience. Cela nécessite également que l'organisation, les méthodes de travail et les technologies des systèmes SAH soient mises au point de manière à permettre aux personnes, à tous les niveaux du système, d'adapter leurs stratégies de travail à la diversité des situations de contrôle des systèmes. Il faudra pour cela concevoir et mettre au point les organisations, les méthodes de travail et les technologies des systèmes SAH sous la forme de systèmes ouverts (Kidd, 1994).

Un système automatisé hybride ouvert (SAHO) est un système qui reçoit des informations de son environnement et lui en renvoie. Le principe d'un système ouvert peut s'appliquer non seulement aux architectures des systèmes et aux organisations, mais aussi aux méthodes de travail, aux interfaces humain-ordinateur et aux relations entre les personnes et les technologies: on peut mentionner, par exemple, les systèmes d'organisation, les systèmes de contrôle et les systèmes d'aide à la décision. Un système ouvert est également adaptatif dans la mesure où il laisse aux personnes une grande liberté pour la définition du mode de fonctionnement du système. Ainsi, dans le domaine des techniques de fabrication

avancées, les critères des systèmes automatisés hybrides ouverts correspondent à la notion de fabrication intégrée humain-ordinateur. Pour la conception de la technologie, il y a lieu de considérer alors l'architecture globale de ces systèmes, y compris les points suivants: 1) prise en compte du réseau de groupes; 2) structure de chaque groupe; 3) interactions entre les groupes; 4) nature du logiciel d'appui; 5) besoins en communication technique et en intégration entre les modules du logiciel d'appui.

Le système automatisé hybride adaptatif, contrairement au système fermé, ne limite pas le champ d'action des opérateurs. Le rôle du concepteur d'un système SAH est de créer un système qui réponde aux préférences personnelles des utilisateurs et qui leur permette de travailler de la façon qu'ils estiment la mieux adaptée. Une condition préalable à la contribution de l'utilisateur est le développement d'une méthodologie de conception adaptative, c'est-à-dire d'un système SAHO permettant l'emploi des technologies assistées par ordinateur dans le processus de conception. La nécessité d'élaborer une méthodologie de conception adaptative est l'une des exigences immédiates pour la mise en pratique du concept SAHO. On devra mettre au point un niveau différent de technologie de contrôle hiérarchique humain adaptatif. Ces technologies devraient permettre à l'opérateur humain de «voir» le système de contrôle, normalement invisible, du fonctionnement du système SAH, par exemple par l'emploi d'un système vidéo rapide et interactif à chaque point de contrôle et de commande du système. Un autre besoin important, enfin, est celui d'une méthodologie pour la mise au point d'une assistance par ordinateur, intelligente et hautement adaptative, appliquée aux rôles et aux fonctionnements humains dans les systèmes automatisés hybrides.

Figure 58.65 • Conception générale des systèmes de commande



LES PRINCIPES DE CONCEPTION DE SYSTÈMES DE COMMANDE SÛRS

Georg Vondracek

Il est généralement admis que les systèmes de commande doivent être d'une utilisation sûre. C'est dans cet esprit que la plupart des systèmes de commande modernes sont conçus selon le modèle illustré à la figure 58.65.

La méthode la plus simple pour rendre un système de commande sûr consiste à l'enfermer dans une enceinte inviolable interdisant tout accès et toute intervention humaine dans la zone dangereuse. Un tel système présenterait une très grande sécurité, mais il est irréalisable, étant donné que l'interdiction d'accès rendrait impossibles les essais, les réparations et les réglages. Compte tenu qu'un accès aux zones dangereuses doit être autorisé dans certaines situations, il est nécessaire de prévoir d'autres mesures de protection que de simples cloisons, barrières ou écrans pour faciliter la production, l'installation et la maintenance.

Certaines de ces mesures peuvent être intégrées totalement ou en partie au système de commande:

- Les mouvements peuvent être arrêtés immédiatement par des boutons d'arrêt d'urgence lorsqu'une personne pénètre dans la zone dangereuse.
- Les commandes à boutons-poussoirs devraient être maintenues enfoncées pour que les mouvements correspondants soient exécutés.
- Les commandes bimanuelles ne devraient autoriser les mouvements que lorsque les deux mains sont occupées à maintenir enfoncés les deux organes de commande et se trouvent donc à l'écart des zones dangereuses.

Les mesures de protection de ce type sont activées par les opérateurs. Mais comme l'élément l'humain constitue souvent un point faible dans les applications, de nombreuses fonctions, telles que celles décrites ci-après:

- Les mouvements des bras des robots sont très lents pendant l'«apprentissage» ou la maintenance. Leur vitesse est cependant surveillée en permanence et si, par suite d'une défaillance du système de contrôle, elle venait à augmenter de façon imprévue au cours d'une période de maintenance ou d'apprentissage, le système de surveillance entrerait en action et interromprait immédiatement le mouvement.
- Une cellule de détection contrôle l'accès à une zone dangereuse. Si le faisceau lumineux est interrompu, la machine s'arrête automatiquement.

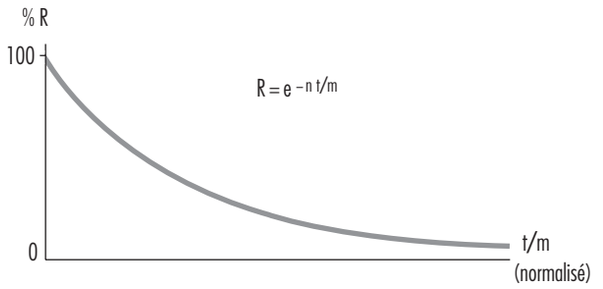
Le bon fonctionnement des systèmes de commande est la plus importante des conditions préalables à la production. Si une fonction de production est interrompue à la suite d'une défaillance du système de commande, c'est tout au plus gênant, mais pas dangereux. Si une fonction liée à la sécurité n'est pas assurée, cela peut entraîner des pertes de production, des dégâts matériels, des lésions corporelles, voire des accidents mortels. Les fonctions du système de commande qui ont un rapport avec la sécurité doivent donc être plus fiables et plus sûres que les fonctions courantes. Aux termes de la directive 98/37/CE du Conseil de l'Union européenne concernant le rapprochement des législations des Etats membres relatives aux machines (CEE, 1989), les systèmes de commande doivent être conçus de façon à être sûrs et fiables.

Les systèmes de commande sont constitués d'un certain nombre de composants reliés entre eux pour exécuter une ou plusieurs fonctions. Les systèmes de contrôle sont subdivisés en voies. Une voie est une partie de la commande chargée d'une fonction particulière (par exemple, démarrage, arrêt normal, arrêt d'urgence). La voie est matérialisée par une chaîne de composants (transistors, diodes, relais, portes, etc.) par lesquels l'information représentant cette fonction (le plus souvent sous forme de signaux électriques) est transférée de l'entrée à la sortie.

La conception des voies de commande pour les fonctions en rapport avec la sécurité (celles qui impliquent des êtres humains) doit répondre aux critères ci-après:

- Les composants employés dans les voies de commande ayant des fonctions en rapport avec la sécurité doivent être capables

Figure 58.66 • Formule de fiabilité



de supporter les conditions rigoureuses d'une utilisation normale. D'une manière générale, ils doivent être suffisamment fiables.

- Les défauts affectant la logique ne doivent pas créer de situations dangereuses. D'une manière générale, les voies en rapport avec la sécurité doivent être suffisamment à l'épreuve des défaillances.
- Les influences extérieures (facteurs extérieurs) ne doivent pas provoquer de défaillances temporaires ou permanentes des voies en rapport avec la sécurité.

La fiabilité R

La fiabilité est l'aptitude d'une voie de commande ou d'un composant à assurer sans défaillance la fonction requise dans des conditions spécifiées et pendant un laps de temps donné. Des méthodes appropriées permettent de calculer la probabilité de fiabilité pour des composants ou des voies de commande spécifiques. La fiabilité doit toujours être définie en fonction du temps et elle est généralement exprimée par la formule indiquée à la figure 58.66.

La fiabilité des systèmes complexes

Les systèmes sont constitués de composants. Si l'on connaît les indices de fiabilité des composants, on peut calculer celui de l'ensemble du système par la méthode suivante:

Les systèmes en série

La fiabilité totale R_{tot} d'un système en série comprenant N composants de même fiabilité R_C se calcule comme mentionné à la figure 58.67.

La fiabilité totale est inférieure à celle du composant le moins fiable. Cette fiabilité totale diminue sensiblement lorsque le nombre de composants augmente.

Les systèmes en parallèle

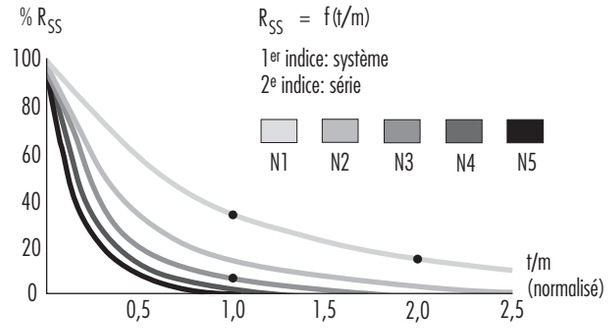
La fiabilité totale R_{tot} d'un système en parallèle comprenant N composants de même fiabilité R_C se calcule comme indiqué à la figure 58.68.

La connexion en parallèle de deux composants ou plus améliore sensiblement la fiabilité totale.

La figure 58.69 montre un exemple pratique. On remarquera que ce circuit arrête le moteur de façon plus fiable. Le moteur sera arrêté même en cas de défaillance du relais A ou B.

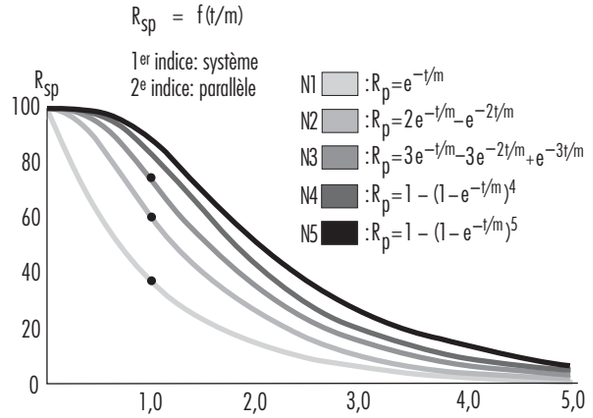
Le calcul de la fiabilité totale d'une voie est simple si l'on dispose de tous les indices de fiabilité des composants correspondants. Dans le cas de composants complexes (circuits intégrés, microprocesseurs, etc.), ce calcul est difficile, voire impossible, si le fabricant n'a pas communiqué les informations nécessaires.

Figure 58.67 • Diagramme de fiabilité de composants reliés en série



$R_{tot} = R_c^N$
(formule pour N composants de même fiabilité R_C reliés en série)

Figure 58.68 • Diagramme de fiabilité de composants reliés en parallèle



$R_{tot} = 1-(1-R_c)^N$
(formule pour N composants de même fiabilité R_C reliés en parallèle)

Figure 58.69 • Exemple d'application pratique de la figure 58.68

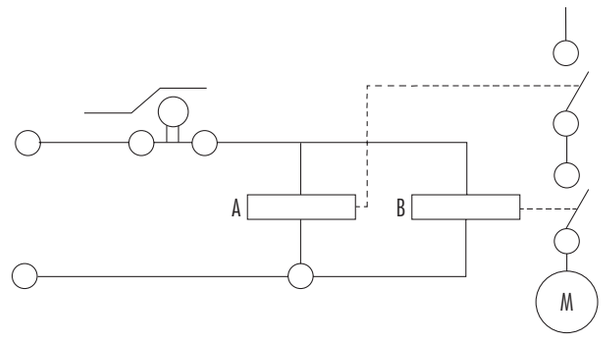


Figure 58.70 • Voie de commande en rapport avec la sécurité et assurant la fonction de sécurité requise

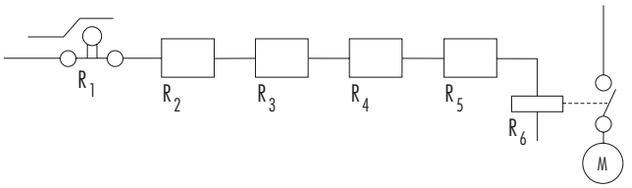


Figure 58.71 • Voie de commande en rapport avec la sécurité à deux sous-voies entièrement séparées

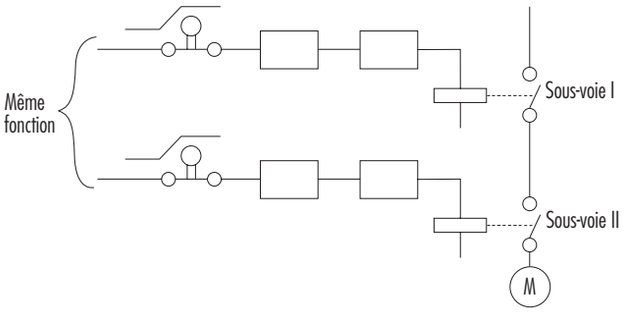


Figure 58.72 • Voie de commande en rapport avec la sécurité à deux sous-voies entièrement séparées se surveillant mutuellement

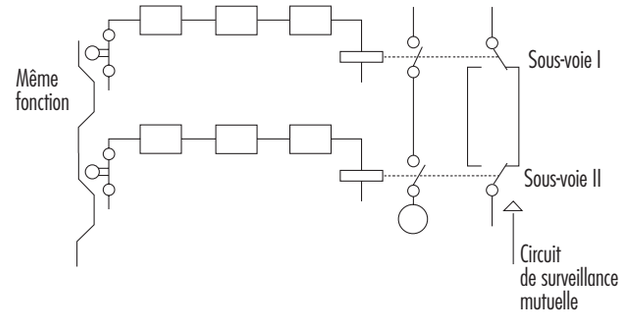
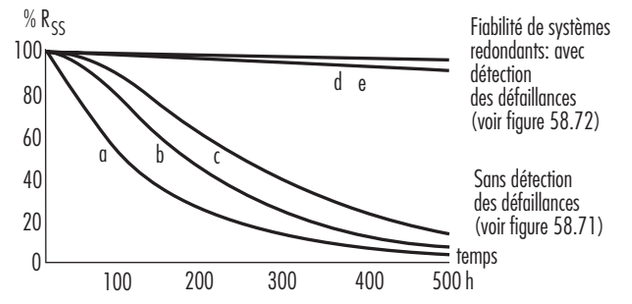


Figure 58.73 • Fiabilité de systèmes redondants avec ou sans détection des défaillances



La sécurité

Lorsque les professionnels évoquent la question de la sécurité et demandent des machines sûres, ils se réfèrent à la sécurité de la machine ou du système dans son ensemble. Cette notion est cependant trop générale et trop imprécise pour s'appliquer à la conception des systèmes de commande. Une définition de la sécurité qui soit pratique et utilisable pour les concepteurs des circuits de commande pourrait être la suivante: la sécurité est l'aptitude d'un système de commande à assurer la fonction requise dans les limites prescrites et pendant un laps de temps donné, même en cas d'apparition de défauts prévisibles. Il est donc nécessaire de préciser, au stade de la conception, quel doit être le niveau de sécurité de la voie ayant un rapport avec la sécurité (le concepteur peut mettre au point une voie protégée contre la première défaillance, contre une défaillance quelconque, contre deux défaillances, etc.). En outre, une voie affectée à une fonction de prévention des accidents peut être essentiellement fiable, sans qu'elle soit pour autant totalement protégée contre les défaillances. Les exemples suivants permettent de mieux expliquer ce principe:

Exemple 1

L'exemple illustré à la figure 58.70 est celui d'une voie en rapport avec la sécurité et assurant la fonction de sécurité requise. Le premier composant peut être un contacteur surveillant, par exemple, la position d'une porte d'accès à une zone dangereuse. Le dernier composant est un moteur d'entraînement de parties mécaniques situées dans la zone dangereuse.

La fonction de sécurité nécessaire dans ce cas est double: si la porte est fermée, le moteur peut fonctionner. Si la porte est ouverte, il doit être arrêté. Connaissant les fiabilités R_1 à R_6, on peut calculer la fiabilité $R_{tot.}$ Les concepteurs doivent choisir des composants fiables pour conserver au système complet un niveau de fiabilité suffisamment élevé (c'est-à-dire que la conception intègre la probabilité que la fonction soit toujours assurée après vingt ans par exemple). Les concepteurs doivent donc répondre à deux obligations: 1) le circuit doit assurer la fonction voulue; 2) la fiabilité de la voie de contrôle complète doit être suffisante.

La question qui se pose alors est la suivante: cette voie assurera-t-elle les fonctions de sécurité voulues même si une défaillance se produit dans le système (par exemple, si les contacts d'un relais restent collés ou si un composant ne fonctionne pas correctement)? La réponse est «non». En effet, une seule voie de contrôle, constituée uniquement de composants reliés en série et travaillant avec des signaux statiques, ne présente pas de protection contre une défaillance. Cette voie ne peut avoir qu'une certaine fiabilité, garantissant la probabilité que la fonction sera assurée. Dans une telle situation, la sécurité est toujours définie par rapport aux défaillances.

Exemple 2

Si une voie de contrôle doit être à la fois fiable et sûre, elle doit être modifiée de la façon indiquée à la figure 58.71. L'exemple illustré est celui d'une voie de contrôle en rapport avec la sécurité, composée de deux sous-voies entièrement séparées.

Cette conception assure une sécurité contre la première défaillance (et les éventuelles défaillances ultérieures de la même sous-voie), mais elle n'offre pas de garantie contre deux défaillances pouvant se produire simultanément ou non dans deux sous-voies différentes, étant donné qu'elle est dépourvue de circuit de détection des défaillances. Par conséquent, les deux sous-voies fonctionnent au départ avec une grande fiabilité (voir le cas des systèmes en parallèle), mais après la première défaillance, une seule voie continue de fonctionner, et la fiabilité diminue. Si une deuxième défaillance se produit sur la sous-voie encore en service, les deux voies seront hors service et la fonction de sécurité ne sera plus assurée.

Exemple 3
L'exemple illustré à la figure 58.72 concerne une voie de contrôle en rapport avec la sécurité constituée de deux sous-voies entièrement séparées et se surveillant mutuellement.

Cette configuration est protégée contre les défaillances, car après une défaillance quelconque, une seule sous-voie cesse d'être fonctionnelle, tandis que l'autre reste disponible et assure la fonction de sécurité. Ce système comporte en outre un circuit de détection des défaillances. Lorsque, par suite d'une défaillance, les deux sous-voies ne fonctionnent plus de manière identique, cette situation est détectée par un circuit «exclusif ou» et la machine est automatiquement mise à l'arrêt. Cette solution consistant à prévoir des sous-voies ayant un rôle pour la sécurité est l'une des meilleures pour la conception des systèmes de contrôle des machines. Ces sous-voies sont protégées contre une défaillance et elles sont en outre suffisamment fiables pour que les risques d'apparition de deux défaillances simultanées soient infimes.

La redondance

Il est évident que les concepteurs peuvent employer différentes méthodes pour améliorer la fiabilité ou la sécurité contre les défaillances. Les exemples précédents montrent comment une fonction (par exemple, si la porte est fermée, le moteur peut fonctionner, si la porte est ouverte, il doit être mis à l'arrêt) peut être assurée par application de différentes solutions. Certaines sont très simples (une seule sous-voie) et d'autres plus complexes (deux sous-voies avec surveillance mutuelle) (voir figure 58.73).

Les circuits ou composants complexes présentent, par rapport aux dispositifs plus simples, une certaine redondance. La redondance peut se définir ainsi: 1) la redondance est la présence de moyens (composants, voies, coefficients de sécurité plus élevés, tests supplémentaires, etc.) en plus grand nombre que ce qui est nécessaire à la seule exécution de la fonction souhaitée; 2) la redondance n'améliore évidemment pas la fonction, qui est exécutée de toute manière. Elle n'améliore que la fiabilité ou la sécurité.

Certains professionnels de la sécurité pensent que la redondance se résume à l'installation de systèmes doubles ou triples. Cette interprétation est très restrictive et la redondance peut être prise dans un sens bien plus large et plus souple. On peut envisager qu'elle ne soit pas intégrée uniquement au matériel, mais aussi au logiciel. L'amélioration du coefficient de sécurité (par exemple, le choix d'une corde plus solide) peut également être considérée comme une forme de redondance.

L'entropie

L'entropie, terme principalement employé en thermodynamique et en astronomie, peut se définir ainsi: toute chose tend à se dégrader. Il est donc absolument certain que tous les composants, sous-systèmes ou systèmes sont voués, indépendamment de la technologie mise en œuvre, à tomber en panne à un moment quelconque. Cela signifie qu'il n'existe pas de systèmes, sous-systèmes ou composants absolument fiables ou sûrs. Tous sont simplement plus ou moins fiables et sûrs, selon la complexité de leur structure. Les défaillances qui se produisent inévitablement tôt ou tard démontrent l'action de l'entropie.

Le seul moyen dont disposent les concepteurs pour faire obstacle à l'entropie est la redondance, qui est obtenue: a) en introduisant une fiabilité supplémentaire dans les composants; b) en assurant un supplément de sécurité dans l'architecture du circuit. C'est uniquement en accroissant dans une proportion suffisante la probabilité que la fonction désirée soit assurée pendant toute la période voulue que les concepteurs peuvent dans une certaine mesure se prémunir contre l'entropie.

L'évaluation des risques

Plus le risque est grand, plus grande doit être la fiabilité ou la sécurité nécessaires, et inversement. Ce principe est illustré par les deux cas suivants:

Cas 1
L'accès à un moule monté sur une machine de moulage par injection est protégé par une porte. Si la porte est fermée, la machine peut fonctionner. Si elle est ouverte, tous les mouvements dangereux doivent être arrêtés. En aucun cas (même celui d'une défaillance de la voie en rapport avec la sécurité), un mouvement quelconque, en particulier ceux qui actionnent l'outil de moulage, ne peut se produire.

Cas 2
L'accès à une ligne d'assemblage à commande automatique, sur laquelle de petits composants en plastique sont assemblés sous une pression pneumatique, est protégé par une porte. Si cette porte est ouverte, la ligne doit être arrêtée.

Dans le cas 1, une défaillance du système de commande de la porte peut conduire à un accident grave par suite d'une fermeture imprévue de l'outil. Dans le cas 2, la défaillance du système de commande de la porte ne peut provoquer que des blessures légères ou des dégâts insignifiants.

Il est évident que, dans le premier cas, il est nécessaire d'introduire une redondance nettement supérieure pour obtenir la fiabilité ou la sécurité requise contre les défaillances en vue d'une protection contre un risque extrêmement élevé. En fait, selon la norme européenne EN 201, le système de contrôle de la porte de la machine de moulage par injection doit être équipé de trois voies: deux voies électriques et à surveillance mutuelle et une voie équipée principalement de circuits hydrauliques et de test. Ces trois fonctions de surveillance concernent toutes la même porte.

En revanche, dans des applications comme celle du cas 2, une voie unique actionnée par un contacteur à action directe suffit par rapport au risque.

Les catégories de commande

Etant donné que toutes les considérations ci-dessus reposent, d'une manière générale, sur la théorie de l'information, et qu'elles sont donc valables pour toutes les technologies, il est indifférent que le système de commande soit basé sur des composants électroniques, électromécaniques, mécaniques, hydrauliques ou pneumatiques, sur une combinaison de ces dispositifs, ou sur une quelconque autre technologie. L'inventivité du concepteur, d'une part, et les considérations économiques, de l'autre, sont les facteurs déterminants du choix dans un éventail pratiquement illimité de solutions permettant de réaliser des voies en rapport avec la sécurité.

Pour éviter les confusions, il est commode de définir certains critères de tri. Les structures de voies les plus couramment employées pour assurer les fonctions liées à la sécurité sur les systèmes de contrôle des machines peuvent être classées selon:

- la fiabilité;
- le comportement en cas de défaillance;
- le délai de signalisation de la défaillance.

Le tableau 58.5 montre certaines de leurs combinaisons (il n'est pas possible de les mentionner toutes).

La catégorie applicable à une machine particulière et à son système de contrôle pour la sécurité est généralement spécifiée dans les nouvelles normes européennes, à moins que l'autorité nationale, l'utilisateur et le constructeur ne conviennent d'une autre catégorie. Le concepteur développe alors un système de commande répondant aux caractéristiques exigées. Pour la conception des voies de commande, on peut notamment prendre en considération les éléments ci-après:

Tableau 58.5 • Combinaisons possibles d'architectures de circuits assurant des fonctions de sécurité dans les systèmes de commande de machines

Critères (Questions)	Stratégie de base					
	Augmentation de la fiabilité (l'apparition d'une défaillance est-elle repoussée à un avenir lointain?)			Structure de circuit (architecture) adaptée: une défaillance sera au moins détectée (catégorie 2) ou son effet sur la voie sera éliminé (catégorie 3) ou elle sera révélée immédiatement (catégorie 4)		
	Catégories					
	Cette solution est mauvaise par principe	B	1	2	3	4
Les composants du circuit peuvent-ils résister aux influences prévisibles; sont-ils conformes aux technologies modernes?	Non	Oui	Oui	Oui	Oui	Oui
A-t-on employé des principes et des composants éprouvés?	Non	Non	Oui	Oui	Oui	Oui
Les défaillances peuvent-elles être détectées automatiquement?	Non	Non	Non	Oui	Oui	Oui
Une défaillance empêche-t-elle l'exécution de la fonction liée à la sécurité?	Oui	Oui	Oui	Oui	Non	Non
Quand la panne est-elle détectée?	Jamais	Jamais	Jamais	A un stade précoce (au plus tard à la fin d'une période n'excédant pas un cycle de la machine)	Immédiatement (lorsque le signal perd son caractère dynamique)	
		Dans les produits grand public	**A employer dans les machines**			

- Les composants doivent résister aux influences prévisibles *(oui/non)*.
- Leur construction doit être conforme aux normes techniques les plus récentes *(oui/non)*.
- On utilise des composants et des méthodes éprouvés *(oui/non)*.
- Les défaillances doivent impérativement être détectées *(oui/non)*.
- La fonction sécuritaire sera-t-elle assurée même en cas de défaillance *(oui/non)*?
- Quand la défaillance sera-t-elle détectée *(jamais, rapidement, immédiatement)*?

Ce processus est réversible. A partir des mêmes questions, on peut déterminer à quelle catégorie appartient une voie de commande mise au point précédemment.

Exemples de catégories

Catégorie B
Les composants utilisés principalement dans les voies de contrôle des appareils grand public doivent résister aux influences prévisibles et être conçus selon les normes pertinentes. On peut citer comme exemple un interrupteur bien conçu.

Catégorie 1
L'emploi de principes et de composants éprouvés est typique de la catégorie 1. On peut citer dans cette catégorie les interrupteurs à action directe (c'est-à-dire nécessitant une ouverture forcée des contacts). Le fonctionnement de ces interrupteurs, constitués d'éléments robustes, demande un effort relativement élevé, ce qui leur confère une très haute fiabilité du point de vue de la seule ouverture des contacts. Ce type d'interrupteur est capable d'assurer l'ouverture de contacts collés, voire soudés. (Note: des composants comme les transistors et les diodes ne sont pas considérés comme étant éprouvés.) La figure 58.74 illustre un contrôle de catégorie 1.

Cette voie emploie l'interrupteur à action directe S. Le contacteur K est contrôlé par le voyant L. L'opérateur est averti d'un collage des contacts normalement ouverts (NO) grâce au voyant L. Le contacteur K comporte des contacts à guidage forcé. (Note: les relais et contacteurs à contacts à guidage forcé possèdent, par comparaison avec les relais et contacteurs ordinaires, une cage spéciale en matériau isolant, de sorte que si des contacts normalement fermés (NF) sont effectivement fermés, tous les contacts NO doivent être ouverts, et inversement. Il est donc possible d'utiliser les contacts NF pour vérifier que les contacts de travail ne sont ni collés ni soudés.)

Catégorie 2
La catégorie 2 assure une détection automatique des défaillances. Cette détection doit être activée avant chaque mouvement dangereux. Le mouvement ne sera exécuté que si le résultat du test est positif; dans le cas contraire, la machine sera mise à l'arrêt. Les systèmes de détection automatique des défaillances sont employés sur les cellules de détection pour confirmer qu'elles fonctionnent toujours. Ce principe est illustré à la figure 58.75.

Ce système de commande est testé régulièrement ou occasionnellement par injection d'une impulsion à l'entrée. Dans un système fonctionnant correctement, cette impulsion est transférée à la sortie et comparée à une impulsion provenant d'un générateur de test. Si les deux impulsions sont présentes, il est évident que le système fonctionne. En revanche, s'il n'y a pas d'impulsion en sortie, c'est la preuve d'une défaillance.

Catégorie 3
Ce circuit a déjà été décrit dans l'exemple 3 de la partie «La sécurité» du présent article, voir figure 58.72.

L'objectif d'une détection automatique des défaillances et d'une capacité d'assurer la fonction de sécurité même en cas de défaillance en un point quelconque peut être atteint grâce à des structures de commande à deux voies et à une surveillance réciproque des deux voies.

Pour les systèmes de contrôle des machines seulement, les défaillances nécessitent un examen. Il existe deux types de défaillances:

- Les défaillances *non dangereuses* sont celles dont l'apparition provoque un passage de la machine à un «état de sécurité» en assurant l'arrêt du moteur.
- Les défaillances *dangereuses* sont celles dont l'apparition provoque un passage de la machine à un «état d'insécurité», dans lequel le moteur ne peut pas être arrêté ou démarre de façon imprévisible.

Catégorie 4
La catégorie 4 assure l'envoi à l'entrée d'un signal dynamique à évolution permanente. La présence d'un signal dynamique en sortie signifie *en marche* («1») et son absence *à l'arrêt* («0»).

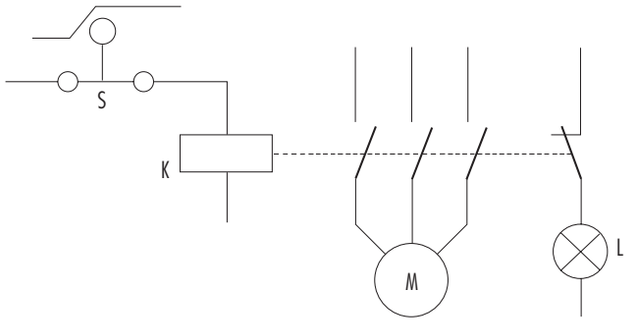
Dans ce type de circuit, le cas le plus fréquent est l'absence du signal dynamique en sortie après la défaillance d'un composant. (Note: le potentiel statique à la sortie est sans importance.) On peut dire de ces circuits qu'ils sont à «sécurité intégrée». Toutes les défaillances sont signalées immédiatement et non, comme dans les circuits de catégorie 3, après la première défaillance.

Remarques complémentaires sur les catégories de systèmes de commande
Le tableau 58.5 a été établi pour les systèmes courants de commande de machines et montre uniquement les structures de circuits de base. Selon la directive européenne sur les machines, les calculs doivent être effectués en supposant une seule défaillance par cycle de la machine. C'est la raison pour laquelle la fonction de sécurité n'est pas exigée en cas de double défaillance simultanée. On suppose qu'une défaillance sera détectée sur un seul cycle de la machine. La machine sera mise à l'arrêt et réparée. Le système de commande redémarre sans défaillances et il est totalement opérationnel.

Le concepteur doit avoir pour objectif premier d'éviter les défaillances «permanentes», c'est-à-dire non détectées au cours d'un même cycle et qui risquent donc d'être associées ensuite à de nouvelles défaillances (cumul de défaillances). Des combinaisons de ce genre (une défaillance permanente et une nouvelle défaillance) peuvent mettre en défaut même les circuits de catégorie 3.

Malgré ces dispositions, il demeure possible que deux défaillances indépendantes se produisent simultanément dans le même cycle de machine. Ce cas est cependant très improbable, surtout si l'on utilise des composants très fiables. Pour les applications à très haut risque, il convient d'employer trois sous-voies ou plus. Cette conception repose sur le fait que le temps moyen entre défaillances est nettement supérieur à la durée du cycle de la machine.

Figure 58.74 • Interrupteur à action directe



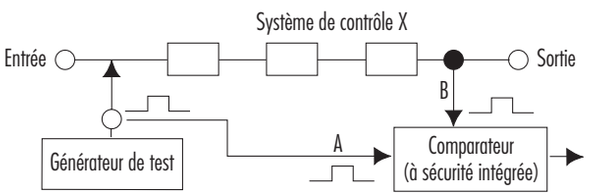
Cela ne signifie pas cependant que le tableau ne puisse pas être développé. Le tableau 58.5 est fondamentalement et structurellement très semblable au tableau 58.2 de la norme européenne EN 954-1. En revanche, on n'a pas cherché à inclure un nombre excessif de critères de tri. Les critères sont définis selon les lois rigoureuses de la logique, de sorte que seules sont à attendre des réponses claires (OUI ou NON). On peut ainsi obtenir une évaluation, un tri et une classification plus précis des circuits étudiés (voies en rapport avec la sécurité) et, surtout, une amélioration sensible de la reproductibilité de l'évaluation.

La situation idéale serait celle où l'on pourrait classer les risques selon différents niveaux, puis établir un lien direct entre les niveaux de risque et les catégories, quelle que soit la technologie employée. Ce n'est toutefois pas entièrement réalisable. Peu de temps après la création de ces catégories, il est apparu qu'un certain nombre de questions ne recevaient pas une réponse suffisante, y compris lorsqu'il s'agissait de la même technologie. Que faut-il préférer, un composant de catégorie 1 très fiable et bien conçu ou un système répondant aux critères de la catégorie 3, mais d'une fiabilité médiocre?

Pour exposer ce dilemme, il convient de différencier deux qualités: la fiabilité et la sécurité (contre les défaillances). Elles ne sont pas comparables, car toutes deux présentent des caractéristiques différentes:

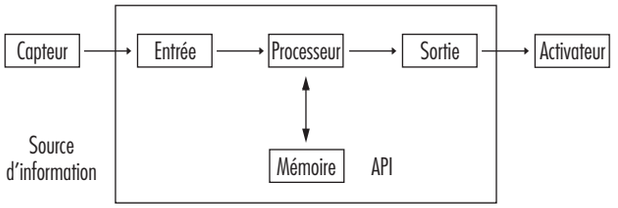
- Le composant doté de la plus grande fiabilité présente la caractéristique gênante qu'en cas de défaillance (même si celle-ci est très improbable) la fonction ne sera plus exécutée.
- Les systèmes de catégorie 3, qui continuent d'assurer la fonction en cas de défaillance unique, n'offrent pas de garanties dans le cas de deux défaillances simultanées (l'important étant de savoir si les composants employés sont suffisamment fiables).

Figure 58.75 • Circuit comportant un détecteur de défaillances



Si:
A = B pas de défaillance dans le système de commande X
A ≠ B défaillance dans le système de commande X

Figure 58.76 • Circuit de système à API



Compte tenu de ce qui précède, la meilleure solution pourrait être (dans le cas d'un risque élevé) d'utiliser des composants de haute fiabilité et de les assembler de manière que le circuit offre une sécurité contre au moins une défaillance, et plus si possible. Il est clair que cette solution n'est pas la plus économique. En pratique, le processus d'optimisation résulte généralement de l'ensemble de ces influences et considérations.

L'expérience de l'utilisation pratique des catégories montre qu'il est rarement possible de concevoir un système de commande permettant de ne mettre en œuvre qu'une seule catégorie dans toute l'installation. On rencontre plus généralement une combinaison de deux, voire trois éléments, chacun d'une catégorie différente, comme le montre l'exemple suivant:

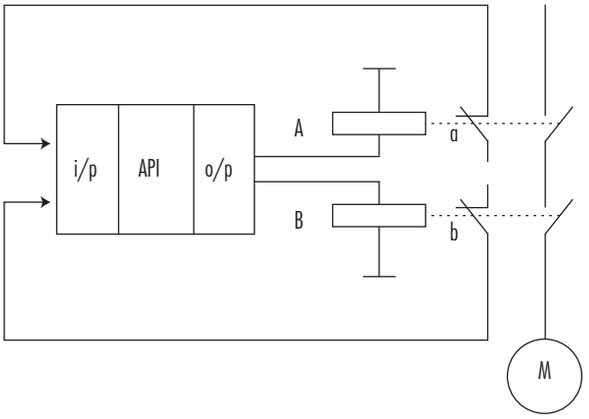
Un grand nombre de cellules de détection sont conçues en catégorie 4, dans laquelle une voie fonctionne avec un signal dynamique. A l'extrémité de ce système, on trouve habituellement deux sous-voies à surveillance réciproque, fonctionnant avec des signaux statiques (cette disposition répond aux critères de la catégorie 3).

Selon la norme européenne EN 61496, ces cellules de détection sont classées comme dispositifs de protection électrosensibles de type 4, bien qu'elles ne comportent que deux parties. Il n'existe malheureusement pas de consensus sur la dénomination à adopter pour les systèmes de commande à deux ou plusieurs parties appartenant chacune à une catégorie différente.

Systèmes électroniques programmables (Automates programmables industriels (API))

Les principes appliqués pour créer le tableau 58.5 peuvent, avec certaines restrictions bien entendu, s'appliquer généralement aux API.

Figure 58.77 • Circuit API avec système de détection des défaillances



Le système à API uniquement

Lorsque la commande est assurée par des API, l'information est transmise du capteur à l'activateur par un grand nombre de composants. On peut même dire qu'elle «traverse» le logiciel (voir figure 58.76).

Bien que les API modernes soient très fiables, ils ne le sont pas toujours autant qu'il le faudrait pour traiter les fonctions de sécurité. De plus, les systèmes à API courants ne sont pas assez sûrs, car ils n'exécutent pas la fonction sécuritaire en cas de défaillance. Par conséquent, il est interdit d'y recourir pour gérer les fonctions de sécurité sans mesures complémentaires.

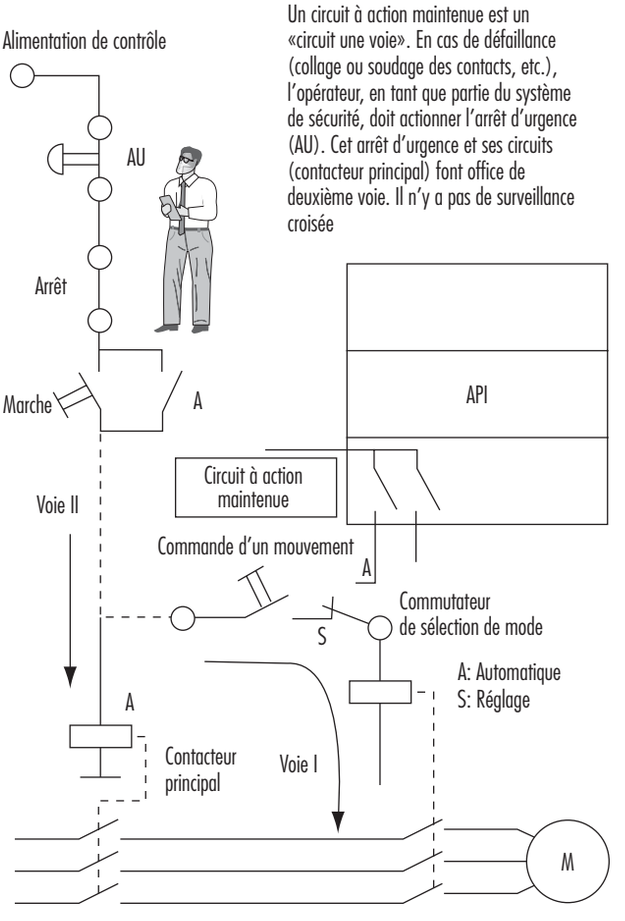
Applications à très faibles risques: systèmes à un API et dispositions complémentaires

Lorsqu'un seul API est utilisé pour la commande, le système se compose des parties principales suivantes:

La partie entrée

Un moyen d'améliorer la fiabilité d'un capteur et de l'entrée d'un API consiste à doubler le nombre de ses composants. Ce type de configuration d'entrée à système double peut également être surveillé par un logiciel, afin de vérifier que les deux systèmes fournissent la même information. On peut ainsi détecter une défaillance dans la partie entrée. Cette conception est à peu près

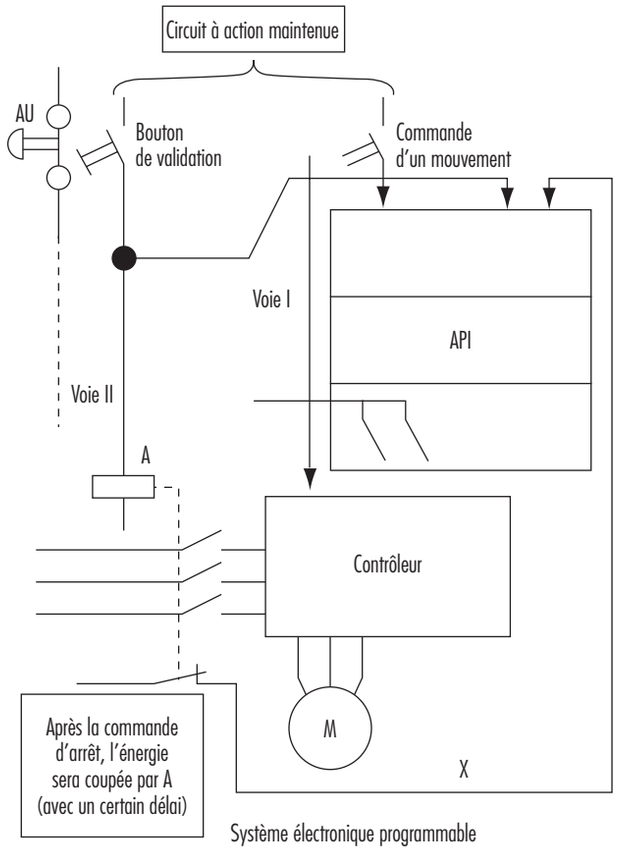
Figure 58.78 • Configuration type pour la catégorie d'arrêt 0



Source: EN 60204-1, 1992, paragr. 9.2.2.

Figure 58.79 • Configuration type pour la catégorie d'arrêt 1

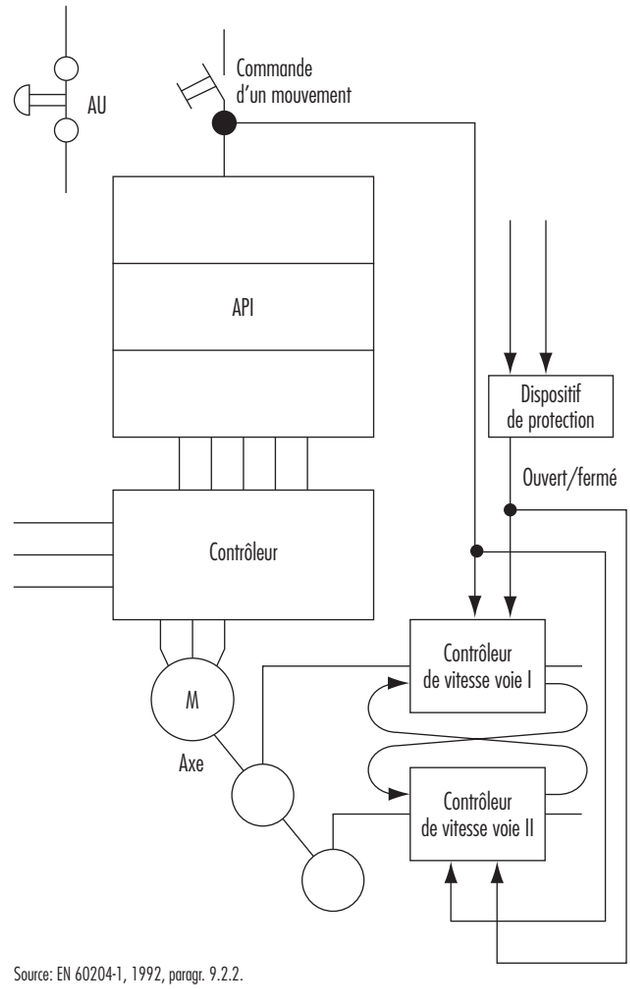
Pour faire fonctionner l'entraînement, il faut appuyer simultanément sur le bouton de validation et sur le bouton de commande (par exemple, mouvement d'axe). Une défaillance de la voie I n'est pas détectée automatiquement. Cependant, pour la plupart des défaillances de la voie I, la machine ne fonctionnera pas correctement et l'opérateur remarquera donc la défaillance. Une défaillance de la voie II sera détectée par l'API (voir la boucle de surveillance X). L'arrêt du mouvement (S) est sûr, l'énergie étant interrompue deux fois. La surveillance croisée peut être considérée comme presque complète.



Source: EN 60204-1, 1992, paragr. 9.2.2.

Figure 58.80 • Configuration type pour la catégorie d'arrêt 2

L'ordre de marche ou d'arrêt est exécuté uniquement par le système d'exploitation, qui ne présente pas par lui-même une sûreté suffisante. Il est donc nécessaire de prévoir en complément un «système de surveillance de la vitesse» pour les actions «pas de mouvement» et «mouvement lent». En cas de défaillance du système d'exploitation (API, unité de contrôle ou de commande), le système complémentaire de surveillance de la vitesse détectera la situation d'insécurité et provoquera l'arrêt de la machine dans des conditions de sécurité.



Source: EN 60204-1, 1992, paragr. 9.2.2.

identique à ce qui est exigé pour la catégorie 3. En revanche, comme la surveillance est assurée par un logiciel et une fois seulement, on peut classer le système dans la catégorie 3- (soit moins fiable que la 3).

La partie centrale

Cette partie peut assez difficilement être doublée, mais il est possible de la tester. A la mise sous tension (ou en cours d'opération), on peut effectuer une vérification du jeu d'instructions complet. On peut également vérifier la mémoire, aux mêmes intervalles, à l'aide de configurations binaires appropriées. Si ces vérifications s'achèvent sans défaillance, cela prouve que les deux parties concernées, le processeur et la mémoire, fonctionnent correctement. Certaines caractéristiques de la partie centrale sont typiques de la catégorie 4 (signal dynamique) et d'autres de la catégorie 2 (tests périodiques à des intervalles appropriés). Le problème est que ces tests, bien qu'étendus, ne peuvent pas être véritablement complets, en raison de la nature même des systèmes à API unique.

La partie sortie

Comme l'entrée, la sortie (y compris les activateurs) peut être doublée. On surveille les deux sous-systèmes pour s'assurer qu'ils donnent le même résultat. Les défaillances seront détectées, et la fonction de sécurité assurée. Mais cette partie présente les mêmes points faibles que l'entrée, et il y a donc lieu de retenir la catégorie 3.

Sur la figure 58.77, la même fonction est acheminée jusqu'aux relais *A* et *B*. Les contacts de contrôle *a* et *b* indiquent alors à deux systèmes d'entrée si les deux relais se comportent de la même façon (ce qui n'est pas le cas si une défaillance s'est produite sur l'une des deux voies). La surveillance est assurée dans ce cas également par le logiciel.

Le système dans son ensemble peut être décrit comme de catégorie 3-/4/2/3- si la surveillance est étendue et bien faite. Il est toutefois impossible d'éliminer totalement de ces systèmes les

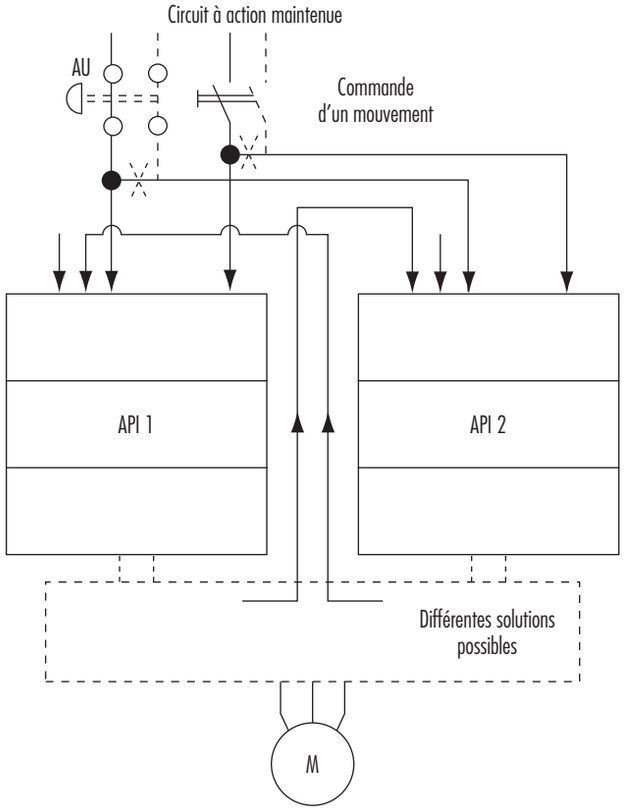
points faibles décrits ci-dessus. En pratique, les systèmes à API unique amélioré ne sont utilisés pour des fonctions liées à la sécurité que lorsque les risques sont assez faibles (Hölscher et Rader, 1984).

Les applications à risques faibles et moyens, à un seul API
Presque toutes les machines actuelles sont équipées d'une unité de commande à API. Pour résoudre le problème d'une fiabilité insuffisante et d'une sécurité contre les défaillances habituellement insuffisante, on applique généralement les méthodes suivantes pour la conception des systèmes:

- Dans les machines relativement simples comme les ascenseurs, les fonctions sont divisées en deux groupes: 1) celles qui ne sont pas liées à la sécurité sont gérées par l'API; 2) celles qui sont liées à la sécurité sont rassemblées en une seule chaîne (le circuit de sécurité) et traitées à l'extérieur de l'API (voir figure 58.78).
- La méthode exposée ci-dessus ne convient pas aux machines plus complexes. Une des raisons tient au fait que ces solutions ne présentent généralement pas une sécurité suffisante. Pour les applications à risques moyens, les solutions choisies devraient satisfaire aux exigences de la catégorie 3. Les figures 58.79 et 58.80 montrent certains principes généraux de l'agencement de ces systèmes.

Figure 58.81 • Système perfectionné à deux API

Toutes les fonctions de sécurité sont traitées électroniquement, mais par deux API indépendants, avec surveillance réciproque complète et permanente. On notera que cette figure ne décrit que l'architecture d'un système de base. Il est possible d'y apporter des améliorations très diverses



Les applications à risques élevés: systèmes à deux API ou plus
Mis à part des considérations de complexité et de coût, rien n'interdit aux concepteurs d'employer des systèmes API entièrement doublés, comme les systèmes Siemens Simatic S5-115F, 3B6 Typ CAR-MIL ou autres. Ceux-ci comportent en général deux API identiques, avec un logiciel homogène, et supposent un recours à des API et des compilateurs «éprouvés» (on peut considérer qu'un API ou un compilateur éprouvés sont des équipements dont l'utilisation dans de nombreuses applications pratiques et sur trois années au moins a permis de démontrer que les défaillances systématiques étaient manifestement éliminées). Quoique ces systèmes à API double ne présentent pas les points faibles des systèmes à API unique, ils ne résolvent pas pour autant tous les problèmes (voir figure 58.81).

Les défaillances systématiques

Les défaillances systématiques, qui peuvent avoir pour origine des erreurs de spécification, de conception ou autres, se rencontrent aussi bien dans le matériel que dans le logiciel. Les systèmes à double API conviennent aux applications liées à la sécurité. Ces configurations permettent de détecter les défaillances aléatoires du matériel. Grâce à une diversification du matériel, comme l'utilisation de deux types d'équipements différents ou de produits de deux fabricants différents, on peut déceler les défaillances systématiques du matériel (il est très improbable qu'une défaillance systématique identique du matériel survienne sur les deux API).

Les logiciels

Les logiciels sont un élément nouveau dans les questions de sécurité. Un logiciel peut être correct ou incorrect (relativement aux défaillances). A la différence du matériel, un logiciel correct ne peut pas devenir soudainement incorrect. Dans ces conditions, les objectifs consisteront à éradiquer toutes les erreurs du logiciel ou du moins à les identifier.

Il existe plusieurs moyens d'atteindre ce but. L'un est la vérification du programme (une deuxième personne tente de découvrir les erreurs au cours d'un essai ultérieur). Une autre possibilité est la diversification des logiciels, qui consiste à faire traiter le même problème par deux programmes, écrits par deux programmeurs différents. Si les résultats sont identiques (dans certaines limites), on peut supposer que les deux parties des programmes sont correctes. Sinon, on peut supposer la présence d'erreurs. (Note: l'architecture matérielle doit naturellement être également prise en compte.)

Résumé

Pour l'utilisation des API, il convient en général de prendre en compte les considérations de base suivantes, qui ont été exposées dans les sections précédentes:

- Un système de commande sans aucune redondance peut être classé en catégorie B. Un système de commande avec des dispositions complémentaires peut correspondre à la catégorie 1 ou supérieure, mais sans dépasser 2.
- Un système de commande en deux parties, avec une comparaison réciproque des résultats, peut être classée en catégorie 3. Un système de commande en deux parties, avec une comparaison réciproque des résultats et une plus ou moins grande diversification, peut être classé en catégorie 3 et convient pour des applications à risques plus élevés.

Dans les systèmes comportant des API, la nécessité d'évaluer également la qualité du logiciel est un nouvel élément à considérer. S'il est correct, un logiciel est fiable à 100%. Au stade actuel du développement technologique, les meilleures solutions techniques connues ne seront probablement pas utilisées, en raison des limitations économiques qui subsistent. Par ailleurs, différents

groupes d'experts (par exemple EC, EWICS) continuent d'élaborer des normes pour les applications des API à la sécurité. Plusieurs normes sont déjà disponibles (VDE 0801, CEI 65A, etc.), mais le domaine est si vaste et si complexe qu'aucune ne peut être considérée comme définitive.

LES PRINCIPES DE SÉCURITÉ POUR LES MACHINES-OUTILS À COMMANDE NUMÉRIQUE

Toni Retsch, Guido Schmitter et Albert Marty

Lorsqu'on automatise un équipement de production simple et classique, comme une machine-outil, on obtient à la fois des systèmes techniques complexes et de nouveaux risques. Cette automatisation consiste à équiper les machines-outils avec des systèmes à commande numérique par calculateur (Computer Numeric Control (CNC)). Ces machines (fraiseuses, centres d'usinage, perceuses ou meuleuses) sont alors appelées machines-outils à commande numérique. Pour déterminer les risques des machines-outils automatiques, il est nécessaire d'analyser les différents modes de fonctionnement de chaque système. Les analyses antérieures indiquent qu'il convient de distinguer deux types de fonctionnement: le fonctionnement normal et le fonctionnement particulier.

Lorsqu'on s'efforce de déterminer les caractéristiques de sécurité requises pour les machines-outils à commande numérique, il est souvent impossible de définir des mesures spécifiques, en raison peut-être d'un manque de réglementation et de normes propres à ces équipements et apportant des solutions concrètes. Pour déterminer les caractéristiques de sécurité, il est nécessaire de procéder à une identification systématique des risques au moyen d'une analyse des risques, notamment lorsque ces ensembles techniques complexes sont équipés de systèmes de commande programmables (ce qui est le cas des machines-outils à commande numérique).

Lorsqu'il s'agit de machines-outils à commande numérique de conception récente, le constructeur est tenu d'effectuer une analyse des risques que pourraient comporter ces équipements et de montrer, au moyen de solutions constructives, que tous les risques pour les personnes sont supprimés quel que soit le mode de fonctionnement. Tous les risques identifiés doivent faire l'objet d'une évaluation dans laquelle chaque risque d'événement est associé à l'étendue des dommages qu'il peut causer et à sa fréquence. Le risque à évaluer est également classé dans une catégorie (risque minime, normal ou accru). Chaque fois que l'évaluation conduit à mettre en évidence un risque qui ne peut pas être accepté, des solutions (mesures de sécurité) doivent être trouvées. Ces solutions ont pour objet de réduire la fréquence d'apparition et l'étendue des dommages d'un incident imprévu et potentiellement dangereux («événement»).

Les solutions adaptées aux risques normaux et accrus doivent être recherchées dans les techniques de sécurité directe et indirecte. Pour les risques minimes, elles relèvent de l'encadrement des pratiques de travail:

- *Technique de sécurité directe.* On entreprend de supprimer les risques au stade de la conception (par exemple, en supprimant les points de cisaillement ou de coincement).
- *Technique de sécurité indirecte.* Le risque subsiste, mais la mise en place de dispositifs techniques a pour effet qu'il ne peut pas se transformer en événement (ces dispositifs peuvent prendre la forme de capots interdisant l'accès aux parties dangereuses en mouvement, de dispositifs de sécurité coupant l'alimentation électrique, d'écrans de protection contre les projections, etc.).
- *Encadrement des pratiques de travail.* Ces solutions ne s'appliquent qu'aux risques résiduels et minimes, c'est-à-dire à ceux où des facteurs d'ordre humain peuvent conduire à un événement indésirable. Un comportement approprié de la personne concernée (observation des consignes des manuels d'utilisation et de maintenance, formation, etc.) permettra d'éviter ce type d'événement.

Les normes de sécurité internationales

La directive du Conseil de l'Union européenne concernant le rapprochement des législations des Etats membres relatives aux machines (89/392/CEE; voir encadré) de 1989 définit les principales exigences de santé et de sécurité en ce qui concerne les machines (selon la définition donnée dans cette directive, une machine est un ensemble de pièces ou d'organes liés entre eux dont au moins un est mobile et possède donc une fonction). (Cette directive a été remplacée par la directive 98/37/CE de 1998.) Les organisations internationales de normalisation élaborent par ailleurs des normes particulières exposant les solutions possibles (par exemple, par l'étude des aspects fondamentaux de la sécurité ou par l'examen des équipements électriques installés sur les machines industrielles). Ces normes ont pour but de définir des objectifs en matière de protection. Ces normes internationales donnent aux constructeurs la base juridique requise pour intégrer ces prescriptions dans les analyses et les évaluations des risques mentionnées plus haut.

Les modes de fonctionnement

En ce qui concerne les machines-outils, on peut distinguer un mode de fonctionnement normal et un mode de fonctionnement particulier. Les statistiques et les enquêtes montrent que la plupart des accidents et incidents ne surviennent pas en fonctionnement normal, c'est-à-dire lors de l'exécution automatique de la tâche concernée, mais lors des modes de fonctionnement particuliers, comme la mise en service, les réglages, la programmation, les essais de production, les vérifications, la recherche de pannes ou la maintenance. En effet, dans ces modes de fonctionnement, des personnes sont généralement présentes dans les zones dangereuses. Le concept de sécurité doit protéger le personnel contre les événements dangereux dans ce type de situation.

Le fonctionnement normal

Le fonctionnement normal d'une machine automatique peut être défini ainsi: 1) la machine accomplit la tâche pour laquelle elle a été conçue et construite sans aucune autre intervention de l'opérateur; 2) dans le cas d'un modèle courant de tour, cela signifie que la pièce est tournée à la forme correcte et que des copeaux sont produits. Si le changement de pièce s'effectue manuellement, ce changement constitue un mode de fonctionnement particulier.

Les modes de fonctionnement particuliers

Les modes de fonctionnement particuliers correspondent aux opérations qui permettent le fonctionnement normal. On peut regrouper dans cette catégorie les changements de pièces ou d'outils, la correction d'un défaut du processus de production ou de la machine, le réglage, la programmation, les essais de production, le nettoyage et la maintenance. En fonctionnement normal, les systèmes automatiques exécutent leurs tâches de manière indépendante. Du point de vue de la sécurité au travail, en revanche, le fonctionnement automatique normal devient critique lorsque l'opérateur doit intervenir dans le processus. Les personnes appelées à le faire ne doivent en aucun cas être exposées à des dangers.

Principales dispositions de la directive du Conseil de la Communauté économique européenne sur les machines

La directive du Conseil en date du 14 juin 1989 sur le rapprochement des législations des Etats membres relatives aux machines (89/392/CEE) s'applique à chacun de ces Etats (CEE, 1989). (Cette directive est maintenant remplacée par la directive 98/37/CE de 1998.)

- Chaque Etat doit intégrer la directive à sa législation.
- Dispositions applicables à compter du 1er janvier 1993.
- Le respect des règles de l'art est exigé de tous les fabricants.
- Le fabricant doit établir un dossier technique de construction comportant des informations complètes sur tous les aspects fondamentaux de santé et de sécurité.
- Le fabricant doit établir une déclaration de conformité et apposer la marque CE sur les machines.
- La non-présentation d'une documentation technique complète à un organisme national de contrôle est considérée comme une absence de conformité aux dispositions de la directive sur les machines et peut entraîner une interdiction de mise sur le marché dans l'ensemble des Etats membres.

Objectifs de sécurité dans la construction et l'utilisation des machines-outils à commande numérique

1. Tours

1.1 Mode de fonctionnement normal

1.1.1 La zone de travail doit être protégée de manière qu'il soit impossible de placer les mains dans les zones dangereuses des mouvements automatiques ou de s'avancer jusqu'à ces zones, volontairement ou non.

1.1.2 Le magasin à outils doit être protégé de manière qu'il soit impossible de placer les mains dans les zones dangereuses des mouvements automatiques ou de s'avancer jusqu'à ces zones, volontairement ou non.

1.1.3 Le magasin à pièces doit être protégé de manière qu'il soit impossible de placer les mains dans les zones dangereuses des mouvements automatiques ou de s'avancer jusqu'à ces zones, volontairement ou non.

1.1.4 L'enlèvement des copeaux ne doit pas occasionner de blessures dues aux copeaux ou aux parties en mouvement de la machine.

1.1.5 Il faut éviter les blessures dues à un accès aux systèmes d'entraînement.

1.1.6 Il ne faut pas qu'il soit possible d'atteindre les zones dangereuses des convoyeurs de copeaux en fonctionnement.

1.1.7 Il faut éviter les projections de pièces ou de parties de pièces qui pourraient blesser les opérateurs ou les tiers.

Causes possibles:

- blocage insuffisant;
- effort de coupe excessif;
- vitesse de rotation excessive;
- choc avec l'outil ou des parties de la machine;
- rupture de la pièce;
- défaut des dispositifs de blocage;
- panne électrique.

1.1.8 Il faut éviter les blessures par projection de dispositifs de blocage de la pièce.

1.1.9 Il faut éviter les blessures par projection de copeaux.

1.1.10 Il faut éviter les blessures par projection d'outils ou de parties d'outils.

Causes possibles:

- défauts du matériau;
- effort de coupe excessif;
- choc avec la pièce ou des parties de la machine;
- insuffisance de blocage ou de serrage.

1.2 Modes de fonctionnement particuliers

1.2.1 Changement de pièces.

1.2.1.1 Le blocage de la pièce doit s'effectuer de manière qu'aucune partie du corps ne puisse être prise entre la pièce et les dispositifs de blocage lors de leur fermeture, ou entre la pièce et la tête du mandrin en mouvement.

1.2.1.2 Il faut éviter la mise en marche d'un mouvement (poupées, axes, mandrins, têtes de tourelle ou convoyeurs de copeaux) à la suite d'une commande défectueuse ou de l'introduction d'un ordre incorrect.

1.2.1.3 La pièce doit pouvoir être manipulée sans danger manuellement ou à l'aide d'outils.

1.2.2 Changement d'outils dans le porte-outils ou la tête de tourelle.

1.2.2.1 Il faut éviter les risques dus à un comportement défectueux du système ou à l'introduction d'un ordre incorrect.

1.2.3 Changement d'outils dans le magasin.

1.2.3.1 Tout mouvement dans le magasin résultant d'un ordre défectueux ou incorrect doit être impossible au cours des changements d'outils.

1.2.3.2 Il ne faut pas qu'il soit possible d'atteindre d'autres parties mobiles de la machine à partir du poste de chargement des outils.

1.2.3.3 Il ne faut pas qu'il soit possible d'atteindre les zones dangereuses pendant la poursuite du mouvement du magasin à outils ou pendant la recherche. S'ils se produisent alors que les protecteurs pour le mode de fonctionnement normal sont retirés, ces mouvements doivent être uniquement du type prescrit, et ils ne doivent être exécutés que pendant la période prescrite et lorsqu'il est possible de garantir qu'aucune partie du corps ne se trouve dans ces zones dangereuses.

Figure 58.32 • Dispositif de retrait des mains sur une presse mécanique

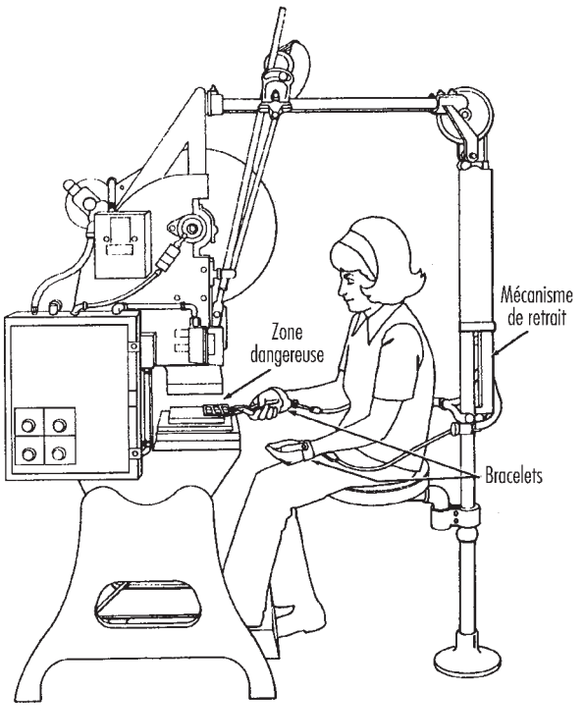


figure 58.31 montre un détecteur de ce type monté sur une machine à poser des œillets. On y voit la sonde de détection en contact avec le doigt de l'opérateur.

Figure 58.33 • Barre sensible à la pression sur un malaxeur de caoutchouc

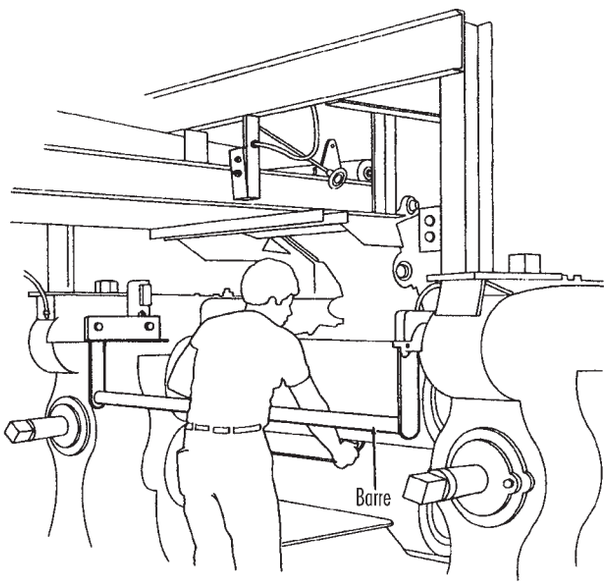
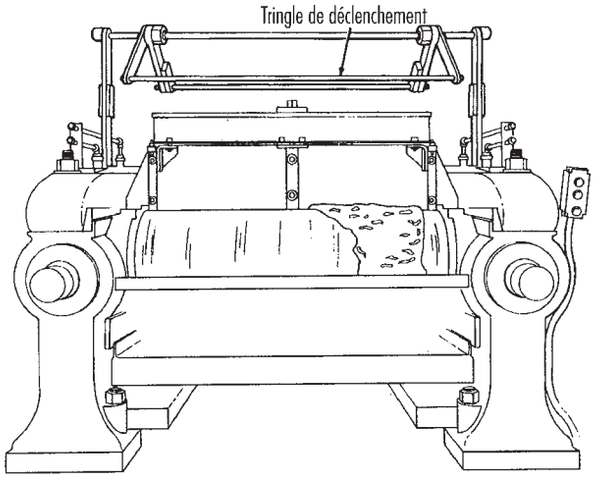


Figure 58.34 • Tringle de déclenchement sur un malaxeur de caoutchouc



Les dispositifs à retrait

Les dispositifs à retrait, qui utilisent un système de câbles attachés aux mains, aux poignets ou aux bras de l'opérateur, sont surtout employés sur les machines effectuant une course. Lorsque le coulisseau est en position haute, l'opérateur peut pénétrer dans la zone de travail. Lorsqu'il commence à descendre, une liaison mécanique assure automatiquement le retrait des mains. La figure 58.32 montre un dispositif à retrait monté sur une presse.

Les dispositifs limitateurs

Les dispositifs limitateurs, qui utilisent des câbles ou des sangles reliant les mains de l'opérateur à un point fixe, étaient en usage dans certains pays. En général, ils ne sont pas considérés comme des protections satisfaisantes, dans la mesure où ils sont faciles à

Figure 58.35 • Câble de déclenchement sur une calandre

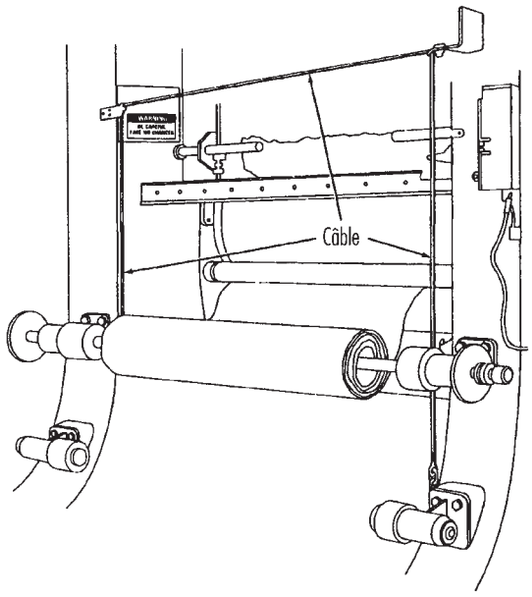
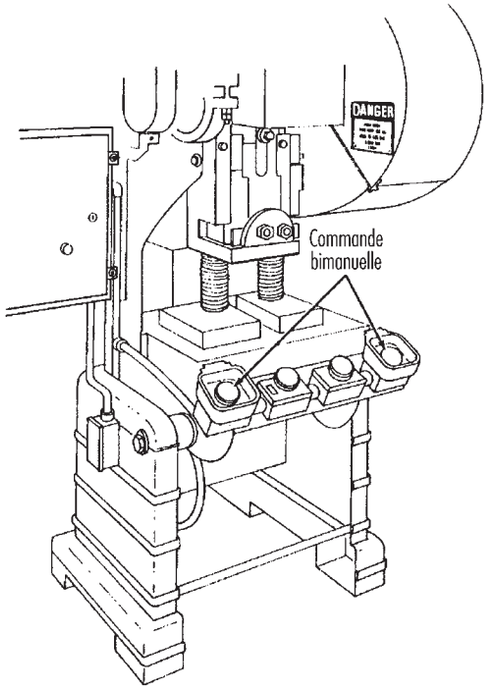


Tableau 58.3 • Dispositifs

Méthode	Action de protection	Avantages	Limites
Photoélectrique (optique)	• La machine n'entame pas son cycle tant que le champ lumineux est coupé • Lorsque le champ lumineux est coupé par une partie du corps de l'opérateur en cours de cycle, le freinage de la machine entre immédiatement en action	• Améliore la liberté de mouvement de l'opérateur	• Ne protège pas contre les pannes mécaniques • Peut nécessiter des alignements et des étalonnages fréquents • Des vibrations excessives peuvent endommager le filament des lampes et le faire griller prématurément • Limité aux machines pouvant être arrêtées avant la fin du cycle
Radiofréquence (champ capacitif)	• La machine n'entame pas son cycle tant que le champ est coupé • Lorsque le champ est coupé par une partie du corps de l'opérateur en cours de cycle, le freinage de la machine entre immédiatement en action	• Améliore la liberté de mouvement de l'opérateur	• Ne protège pas contre les pannes mécaniques • La sensibilité de l'antenne doit être correctement réglée • Limité aux machines pouvant être arrêtées avant la fin du cycle
Electromécanique	• Une barre ou une sonde de contact parcourent une distance prédéterminée entre l'opérateur et la zone de danger • L'interruption de ce mouvement interdit le démarrage du cycle de la machine	• Permet d'accéder au point de fonctionnement	• La barre ou la sonde de contact doivent être correctement réglées pour chaque application; ce réglage doit être maintenu
A retrait	• Au moment où la machine entame son cycle, les mains de l'opérateur sont retirées de la zone de danger	• Supprime la nécessité de barrières auxiliaires ou d'autres dispositifs dans la zone de danger	• Limite les mouvements de l'opérateur • Peut encombrer l'espace de travail entourant l'opérateur • Des réglages sont nécessaires pour chaque application et chaque individu • Nécessite de fréquents contrôles et une maintenance régulière • Nécessite une étroite surveillance de la manière dont l'opérateur utilise le matériel
Déclencheurs de sécurité: • Barre d'appui sensible à la pression • Tringle de déclenchement • Câble ou fil de déclenchement	• Arrêtent la machine lorsqu'ils sont actionnés	• Simplicité d'emploi	• Toutes les commandes doivent être activées à la main • Les commandes peuvent être difficiles à activer en raison de leur emplacement • Ne protège que l'opérateur • Peut nécessiter des dispositifs spéciaux pour tenir les pièces • Peut nécessiter un frein de machine ou un dispositif d'inversion de marche
Commande bimanuelle	• L'opérateur est obligé de se servir simultanément des deux mains, ce qui l'empêche de pénétrer dans la zone de danger	• Les mains de l'opérateur se trouvent à un endroit prédéterminé, à l'écart de la zone de danger • Les mains de l'opérateur sont libres pour prendre une nouvelle pièce lorsque la première moitié du cycle est terminée	• Nécessite une machine à cycle partiel avec frein • On peut contourner certaines commandes bimanuelles en les maintenant avec le bras ou en les bloquant, ce qui permet de ne se servir que d'une main • Ne protège que l'opérateur
Déclencheur à deux mains	• Les deux mains étant simultanément nécessaires, elles se trouvent hors de la zone de danger lorsque le cycle de la machine commence	• Les mains de l'opérateur se trouvent à l'écart de la zone de danger • Peut être adapté à de nombreuses opérations • Ne gêne pas l'introduction manuelle • Ne nécessite pas de réglage à chaque opération	• L'opérateur peut tenter d'accéder à la zone de danger après avoir déclenché l'arrêt de la machine • On peut rendre inopérants certains déclencheurs en les maintenant avec le bras ou en les bloquant, ce qui permet de ne se servir que d'une main • Ne protège que l'opérateur • Peut nécessiter des dispositifs spéciaux
Portillon	• Forme une barrière entre la zone de danger et l'opérateur ou d'autres personnes	• Empêche d'accéder à la zone de danger ou d'y pénétrer	• Peut nécessiter des contrôles fréquents et une maintenance régulière • Peut gêner la visibilité de l'opérateur

Figure 58.36 • Commande bimanuelle sur une presse à embrayage à révolution partielle



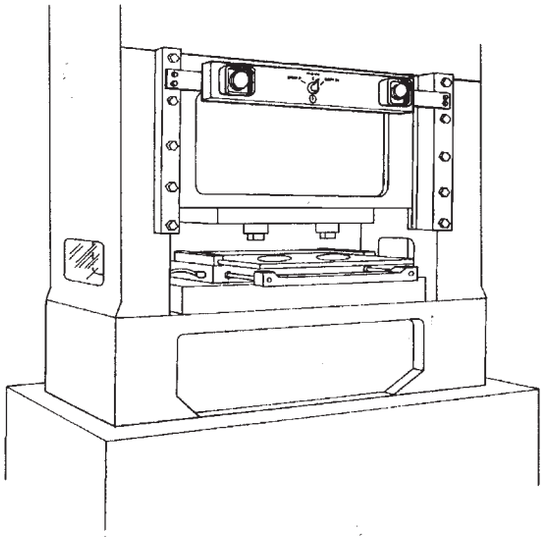
neutraliser par l'opérateur, qui peut alors placer les mains dans la zone dangereuse (voir tableau 58.3).

Les dispositifs de commande de sécurité

Tous ces dispositifs de commande de sécurité sont actionnés manuellement et doivent être réinitialisés manuellement aussi pour remettre en marche la machine:

- Les *commandes de sécurité à déclenchement* tels que les barres d'appui, les tiges de déclenchement et les fils de déclenchement sont des commandes manuelles qui assurent une désactivation rapide de la machine dans les situations d'urgence.
- Les *barres sensibles à la pression* désactivent la machine lorsqu'une personne s'appuie dessus parce qu'elle trébuche, perd l'équilibre ou est entraînée en direction de la machine. Le positionnement de la barre est un facteur critique, car celle-ci doit arrêter la machine avant qu'une partie du corps n'atteigne la zone dangereuse. La figure 58.33 montre une barre sensible à la pression installée sur un malaxeur de caoutchouc.
- Les *dispositifs de sécurité à tringle de déclenchement* désactivent la machine lorsqu'on appuie dessus avec la main. Etant donné que c'est l'opérateur qui doit les actionner en cas d'urgence, leur position est d'une importance capitale. La figure 58.34 montre une tige de déclenchement installée au-dessus d'un malaxeur à caoutchouc.
- Les *câbles de déclenchement* sont placés en périphérie ou à proximité de la zone dangereuse. L'opérateur doit pouvoir les atteindre avec l'une ou l'autre main pour arrêter la machine. La figure 58.35 montre une calandre équipée de ce type de commande.
- Les *commandes bimanuelles* exigent de l'opérateur qu'il appuie constamment et simultanément sur deux boutons pour activer la machine. Lorsqu'elles sont installées sur des presses, ces commandes emploient un embrayage à révolution partielle et un contrôleur de freinage, comme le montre la figure 58.36.

Figure 58.37 • Commande bimanuelle sur une presse à embrayage à révolution complète



Avec ce type de dispositif, les deux mains de l'opérateur doivent se trouver à un emplacement sûr (sur les boutons de la commande) et à une distance de sécurité par rapport à la zone dangereuse pendant que la machine termine son cycle de fermeture.

- *Déclenchement à deux mains*. Le déclencheur à deux mains de la figure 58.37 est généralement employé dans le cas de machines équipées d'embrayages à révolution complète. L'opérateur doit appuyer simultanément sur les deux boutons de commande pour lancer le cycle de la machine, après quoi ses mains sont

Figure 58.38 • Presse mécanique avec portillon

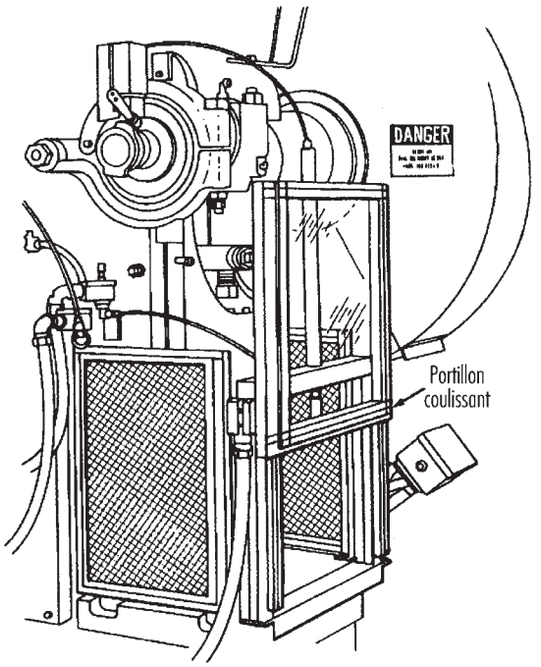
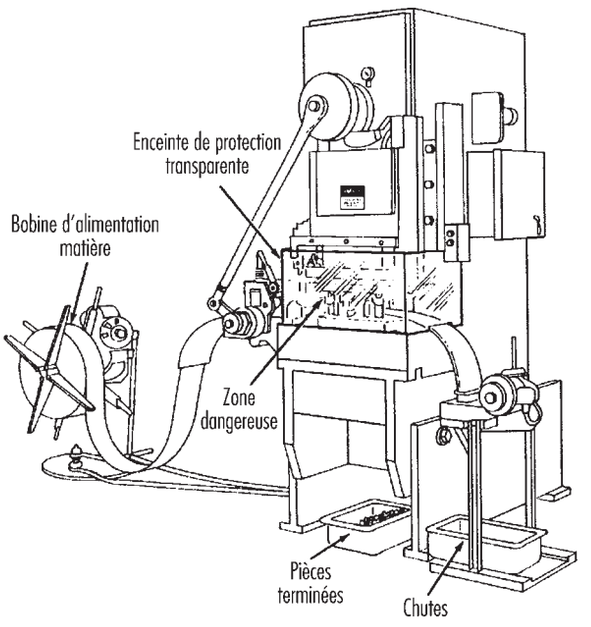


Figure 58.39 • Presse mécanique à alimentation automatique



libérées. Ces déclencheurs doivent être suffisamment éloignés de la zone d'opération pour qu'il soit impossible à l'opérateur de quitter les boutons ou les poignées de commande et d'introduire les mains dans la zone dangereuse avant la fin de la première moitié du cycle. Les mains de l'opérateur sont maintenues suffisamment éloignées pour ne pas pouvoir être placées accidentellement dans la zone dangereuse avant que le coulisseau ou la lame ne soient entièrement abaissés.

- Les *portillons* sont des dispositifs de commande de sécurité comportant une barrière mobile qui protège l'opérateur au point d'opération avant qu'il soit possible de lancer le cycle de la machine. Ils sont souvent conçus pour fonctionner en synchronisation avec le cycle de la machine. La figure 58.38 montre un

Figure 58.40 • Presse mécanique à alimentation par goulotte

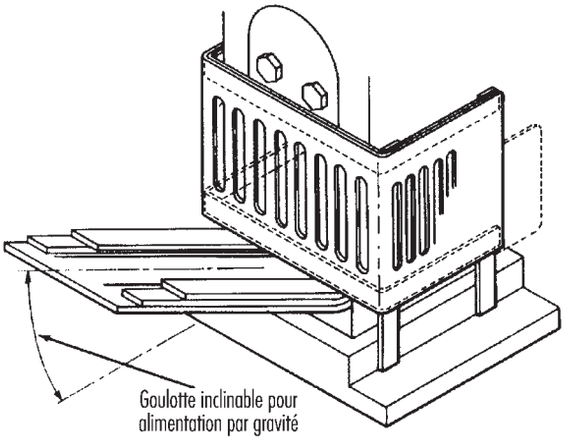
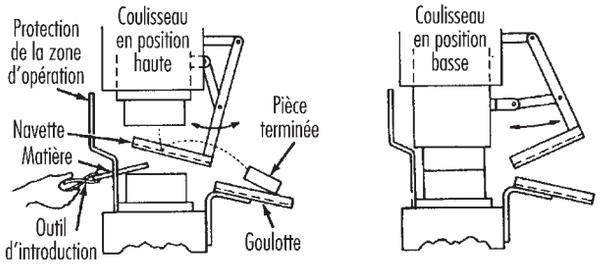


Figure 58.41 • Système d'éjection par navette



portillon installé sur une presse. Si le portillon ne peut pas descendre en position complètement fermée, la presse ne fonctionnera pas. Les portillons trouvent une autre application en tant qu'élément d'un système de sécurité périphérique, où ils interdisent l'accès aux opérateurs et aux passants.

La protection par l'emplacement ou la distance

Avec ce type de solution, la machine ou ses parties en mouvement dangereuses sont placées de telle manière que les zones dangereuses soient inaccessibles ou ne présentent pas de risque pour les travailleurs pendant le fonctionnement normal de la machine. On peut utiliser à cet effet des cloisons ou des clôtures limitant l'accès aux machines ou installer celles-ci à un emplacement où un élément existant des locaux, un mur par exemple, protégera l'opérateur et les autres personnes. Une autre possibilité consiste à placer les parties dangereuses suffisamment haut pour qu'elles soient normalement hors de portée des travailleurs. Il est indispensable d'effectuer une analyse complète des dangers de chaque machine

Figure 58.42 • Mécanisme d'éjection semi-automatique

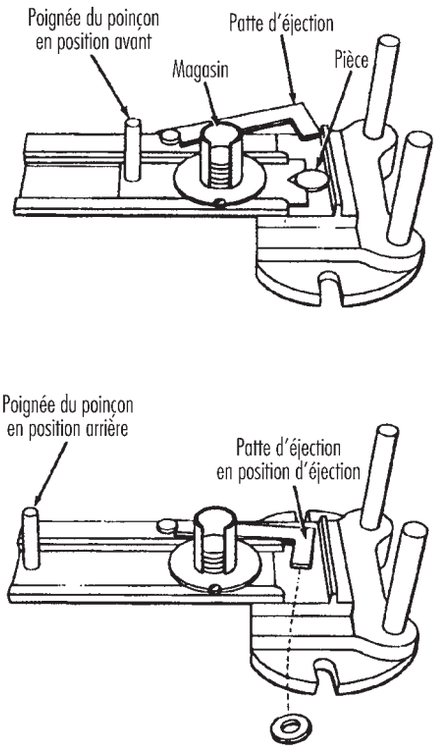


Tableau 58.4 • Méthodes d'alimentation et d'éjection

Méthode	Action de protection	Avantages	Limites
Alimentation automatique	• La matière est introduite à partir de bobines, indexée par le mécanisme de la machine, etc.	• Supprime la nécessité d'une intervention de l'opérateur dans la zone de danger	• D'autres dispositifs sont également nécessaires pour la protection de l'opérateur — généralement des barrières fixes • Impose une maintenance fréquente • Impossibilité d'adaptation aux variations de la matière dans certains cas
Alimentation automatique ou semi-automatique	• La matière est apportée soit de manière entièrement automatique, soit de manière semi-automatique à l'aide de goulottes, de matrices mobiles, d'un plateau tournant, d'élévateurs ou d'un porte-matrice coulissant	• Supprime la nécessité d'une intervention de l'opérateur dans la zone de danger	• D'autres dispositifs sont également nécessaires pour la protection de l'opérateur — généralement des barrières fixes • Impose une maintenance fréquente • Impossibilité d'adaptation aux variations de la matière dans certains cas
Ejection automatique	• Les pièces sont éjectées pneumatiquement ou mécaniquement	• Supprime la nécessité d'une intervention de l'opérateur dans la zone de danger	• Peut créer un risque de projection de copeaux ou de débris • La taille de la matière limite le recours à cette méthode • L'éjection pneumatique peut présenter un danger dû au bruit
Ejection semi-automatique	• Les pièces sont éjectées par un système mécanique actionné par l'opérateur	• L'opérateur n'a pas à pénétrer dans la zone de danger pour retirer les pièces finies	• D'autres dispositifs sont également nécessaires pour la protection de l'opérateur • Impossibilité d'adaptation aux variations de la matière dans certains cas
Robots	• Ils assurent le travail effectué habituellement par un opérateur	• L'opérateur n'a pas à pénétrer dans la zone de danger • Conviennent pour les opérations comportant des facteurs de contrainte importants, comme la chaleur ou le bruit	• Peuvent eux-mêmes créer des dangers • Nécessitent une maintenance maximale • Ne conviennent qu'à des opérations spécifiques

et de chaque situation avant d'envisager cette technique de protection. Les exemples mentionnés ci-dessous ne représentent que quelques-unes des nombreuses applications du principe de la protection par l'emplacement ou la distance.

Opération d'alimentation. L'opération d'alimentation peut faire l'objet d'une mesure de protection par position s'il est possible de maintenir une distance de sécurité pour protéger les mains de l'opérateur. Les dimensions du matériau à travailler peuvent assurer dans certains cas une sécurité suffisante. Dans le cas d'une poinçonneuse simple, par exemple, si le matériau mesure un mètre ou plus et si on ne le travaille que d'un côté, l'opérateur peut le tenir du côté opposé pendant le travail. Toutefois, en fonction de la machine, une protection peut rester nécessaire pour les autres personnes.

Positionnement des commandes. Le positionnement du poste de commande de l'opérateur est l'une des approches possibles de la protection par l'emplacement. S'il n'est pas nécessaire que l'opérateur se tienne à proximité, les commandes de l'opérateur pourront être placées à une distance suffisante de la machine pour assurer la sécurité.

Les systèmes de protection au niveau de l'alimentation et de l'éjection

Il existe un grand nombre de méthodes d'alimentation et d'éjection avec lesquelles il n'est pas nécessaire que les opérateurs placent leurs mains dans la zone dangereuse. Dans certains cas, aucune intervention de l'opérateur n'est nécessaire après le réglage de la machine, alors que dans d'autres, les opérateurs peuvent introduire manuellement le matériau à l'aide d'un mécanisme d'alimentation. De même, on peut concevoir des méthodes d'éjection qui n'exigent aucune intervention de l'opérateur après la mise en marche de la machine. Certaines méthodes d'alimentation et d'éjection peuvent elles-mêmes être source de dangers, comme dans le cas d'un robot qui évite à l'opérateur d'avoir à se tenir à proximité de la machine, mais qui peut créer un nouveau danger par le mouvement de son bras (voir tableau 58.4).

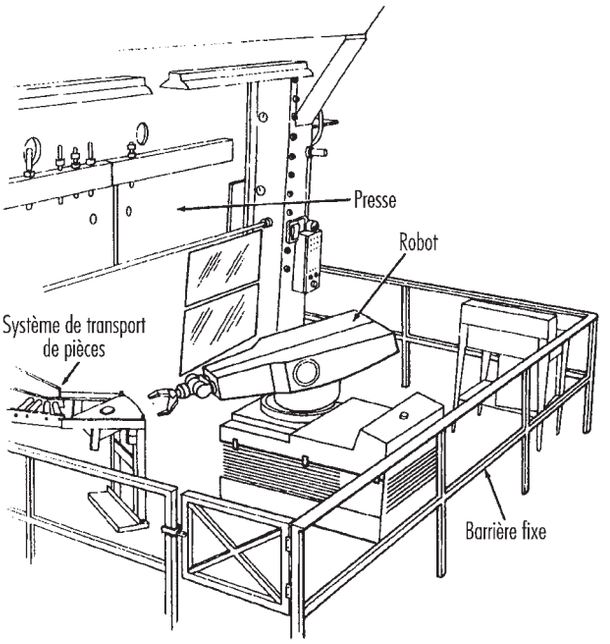
Le recours à l'une des cinq méthodes suivantes d'alimentation et d'éjection pour la mise en sécurité des machines ne supprime pas la nécessité de protecteurs matériels ou d'autres dispositifs, qui devraient être utilisés en fonction des besoins pour assurer une protection contre les dangers.

Alimentation automatique. Les alimentations automatiques réduisent l'exposition de l'opérateur pendant le travail et elles ne demandent souvent aucune intervention de sa part après le réglage et la mise en marche. La presse de la figure 58.39 possède un mécanisme d'alimentation automatique avec une enceinte fixe transparente assurant une protection au niveau de la zone dangereuse.

Alimentation semi-automatique. Avec une alimentation semi-automatique, comme dans le cas d'une presse, l'opérateur utilise un mécanisme pour placer à chaque course la pièce sous le coulisseau. Il n'a pas besoin d'accéder à la zone dangereuse qui est entièrement close. La figure 58.40 montre une alimentation par goulotte dans laquelle chaque pièce est placée à la main. L'emploi d'une alimentation par glissière inclinée permet de centrer la pièce à mesure qu'elle glisse dans la matrice, méthode qui peut en outre simplifier le problème de l'éjection.

Ejection automatique. L'éjection automatique peut employer soit une pression d'air, soit un système mécanique pour retirer la pièce terminée de la presse et elle peut posséder une liaison de sécurité avec les commandes de la machine, afin d'empêcher son fonctionnement tant que l'éjection n'est pas terminée. Le mécanisme de bac-navette montré à la figure 58.41 se déplace sous la pièce finie lorsque le coulisseau remonte. Cette navette saisit ensuite la pièce

Figure 58.43 • Protection par barrières du périmètre d'action d'un robot



débarrassée du poinçon par les axes de dégagement et la repousse vers une glissière. Lorsque le coulisseau descend vers l'ébauche suivante, le bac-navette s'écarte de la matrice.

Ejection semi-automatique. La figure 58.42 montre un mécanisme d'éjection semi-automatique utilisé sur une presse. Lorsque le poinçon se retire de la zone de la matrice, l'éjecteur, qui est mécaniquement couplé au poinçon, chasse la pièce terminée.

Robots. Les robots sont des dispositifs complexes qui chargent et déchargent le matériau, assemblent les pièces, transportent des objets ou effectuent des tâches habituellement assurées par un

Figure 58.44 • Vue arrière d'une cisaille

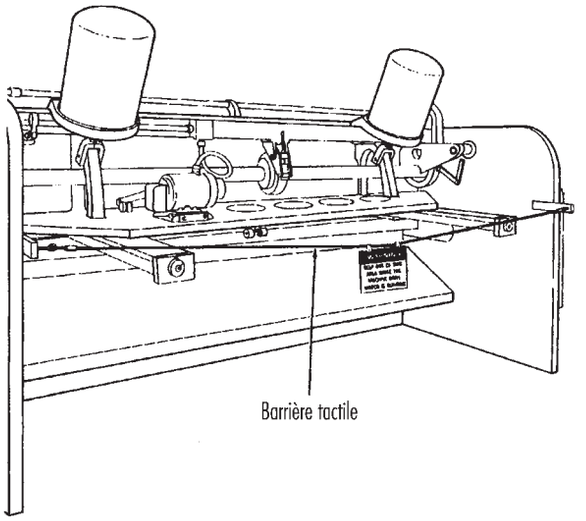
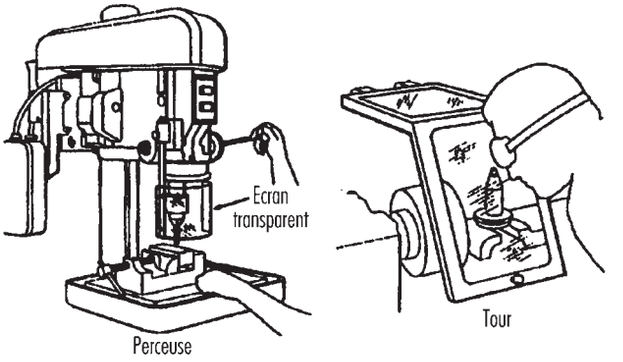


Figure 58.45 • Exemples d'écrans



opérateur, évitant ainsi à celui-ci d'être exposé à des dangers. Leur meilleur champ d'application est celui de la production en gros volumes, qui nécessite des actions répétitives et où ils peuvent assurer une protection contre d'autres dangers pour le personnel. Mais les robots peuvent eux-mêmes créer des dangers justifiant la mise en place de protections appropriées. La figure 58.43 montre l'exemple d'un robot alimentant une presse.

Les autres systèmes et accessoires de protection

Quoique ces accessoires n'assurent pas une protection complète contre les dangers des machines, ils peuvent apporter aux opérateurs une marge de sécurité supplémentaire. Leur application et leur utilisation nécessitent un jugement averti.

Figure 58.46 • Outils de maintien

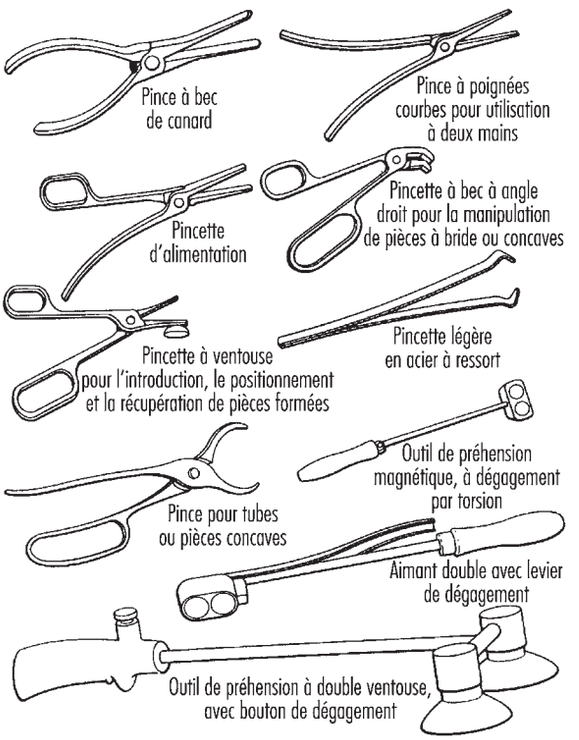
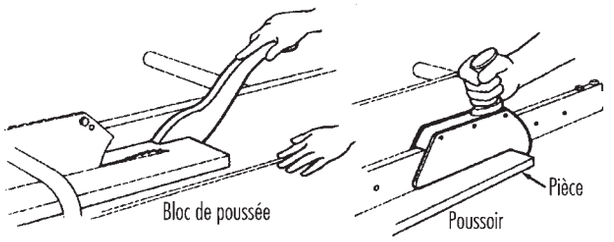


Figure 58.47 • Utilisation d'un poussoir et d'un bloc de poussée



Barrières d'avertissement. Les barrières d'avertissement n'assurent aucune protection physique, mais servent uniquement à rappeler aux opérateurs qu'ils s'approchent de la zone dangereuse. En général, les barrières d'avertissement ne sont pas considérées comme une mesure adéquate dans le cas d'une exposition permanente au danger. La figure 58.44 montre une corde servant de barrière d'avertissement à l'arrière d'une cisaille. Ces barrières n'empêchent pas physiquement les personnes de pénétrer dans les zones dangereuses; elles ne font que les avertir d'un danger.

Ecrans. Les écrans peuvent assurer une protection contre les projections de particules ou de fluides de coupe ou de refroidissement. La figure 58.45 en montre deux applications.

Outils de manipulation. Les outils de manipulation servent à mettre le matériau en place et à le retirer. Ils permettent par exemple d'atteindre la zone dangereuse d'une presse ou d'une plieuse. La figure 58.46 montre un assortiment de tels outils. Les outils de manipulation ne devraient en aucun cas *remplacer* les autres protections de la machine. Ils ne peuvent que compléter la sécurité.

Les *poussoirs ou les blocs de poussée* comme ceux représentés à la figure 58.47 peuvent servir à introduire le matériau dans une machine, une scie par exemple. Lorsqu'il devient nécessaire d'approcher les mains très près de la lame, ils peuvent apporter une marge de sécurité supplémentaire et éviter des blessures.

LES DÉTECTEURS DE PRÉSENCE

Paul Schreiber

L'évolution générale dans les domaines de la microélectronique et de la technologie des détecteurs donne des raisons d'espérer une amélioration de la sécurité au travail grâce à la mise sur le marché de détecteurs de présence et d'approche fiables, robustes, à maintenance réduite et économiques. Le présent article décrit la technologie des détecteurs, les différentes méthodes de détection, les conditions et restrictions applicables à l'emploi des systèmes de détecteurs, ainsi que certains travaux de recherche et de normalisation effectués en Allemagne.

Les caractéristiques des détecteurs de présence

La mise au point et les essais pratiques des détecteurs de présence constituent l'un des principaux défis à relever dans le cadre des efforts techniques en vue d'améliorer la sécurité au travail et la protection des personnes en général. Les détecteurs de présence sont des détecteurs capables de signaler, de façon fiable et certaine, la présence à proximité ou l'approche d'une personne. Cet avertissement doit être donné rapidement, de manière à permettre une manœuvre d'évitement, un freinage ou la mise à l'arrêt d'une machine fixe avant que le contact annoncé se produise. La taille des personnes, leur position ou les vêtements qu'elles portent ne doivent affecter en rien la fiabilité du capteur. Les détecteurs doivent également assurer un fonctionnement sûr et être robustes et économiques pour pouvoir être employés dans les conditions les plus difficiles, comme sur les chantiers de construction et pour les applications mobiles, avec un minimum de maintenance. Les détecteurs doivent être comme les coussins gonflables, c'est-à-dire sans entretien et toujours prêts à servir. Compte tenu de la réticence de certains utilisateurs à entretenir des équipements qu'ils ne jugent pas essentiels, il devrait être possible de laisser les détecteurs sans entretien pendant plusieurs années. Une autre caractéristique qui sera très probablement exigée des détecteurs de présence consiste dans la possibilité de détecter des obstacles autres que les êtres humains et d'avertir l'opérateur en temps voulu pour qu'il puisse prendre des mesures préventives et réduire ainsi les frais de réparation de matériels endommagés. Cette raison d'installer des détecteurs de présence ne devrait pas être sous-estimée.

Les applications des détecteurs

Un nombre incalculable d'accidents mortels ou graves, et que l'on estime inévitables parce que dus au hasard, pourraient être évités, ou leurs conséquences réduites au minimum, si les détecteurs de présence étaient mieux acceptés comme mesure de prévention dans le domaine de la sécurité au travail. De tels accidents défraient trop souvent la chronique: ici, quelqu'un a été heurté par une chargeuse en train de reculer; là, une personne que l'opérateur n'avait pas vue a été écrasée par une pelleteuse. Les camions effectuant une marche arrière dans une rue, dans une cour d'usine ou sur un chantier sont à l'origine de nombreux accidents corporels. En raison de la rationalisation extrême du travail dans les entreprises modernes, on ne prévoit plus, pour accompagner les conducteurs, de deuxième conducteur ou d'autres personnes qui pourraient les guider lors d'une marche arrière. Ces exemples d'accidents peuvent facilement être étendus à d'autres matériels mobiles comme les chariots élévateurs. Mais il existe également un besoin urgent de prévoir des détecteurs sur les équipements semi-mobiles ou entièrement fixes pour éviter les accidents. Ainsi, les parties arrière des grandes machines de chargement sont considérées par les spécialistes de la sécurité comme des zones potentiellement dangereuses où l'installation de détecteurs peu onéreux apporterait une amélioration. Les nombreux modèles de détecteurs de présence peuvent être adaptés de façon imaginative à d'autres véhicules et gros équipements mobiles et assurer une protection contre les types d'accidents considérés, qui occasionnent en général des dégâts étendus et des blessures sérieuses, voire mortelles.

La généralisation progressive des solutions innovatrices semble indiquer que les détecteurs de présence pourraient devenir la référence en matière de sécurité dans d'autres applications, mais ce n'est pas le cas partout. Les progrès les plus décisifs, en raison du nombre des accidents et de l'importance des dégâts matériels, devraient concerner la surveillance de l'arrière des véhicules de livraison et des poids lourds, ainsi que les domaines de pointe des «nouvelles technologies», en l'occurrence les machines robotisées de l'avenir.

La diversité des domaines d'application des détecteurs de présence et des tâches exécutées — par exemple les cas où l'on tolère certains objets (même mobiles, dans des conditions bien précises) situés dans le champ de détection et qui ne doivent pas déclencher un signal — nécessite des détecteurs avec lesquels une technologie d'évaluation «intelligente» complète les mécanismes de détection. Cette technologie, appelée à des développements certains, peut être élaborée selon des méthodes faisant appel à l'intelligence artificielle (Schreiber et Kuhn, 1995). Les applications des détecteurs restent fortement limitées en raison d'un manque d'universalité. Il existe des rideaux et barrages lumineux, des tapis de

contact, des détecteurs infrarouges passifs, des détecteurs de mouvement par ultrasons et radar à effet Doppler, des détecteurs à impulsions ultrasonores, radar et lumineuses, et des lasers à balayage. Les caméras de télévision classiques reliées à des écrans ne font pas partie de cette liste parce que ce ne sont pas des détecteurs de présence, au contraire des caméras qui sont automatiquement activées lorsqu'une présence humaine est décelée.

La technologie des détecteurs

Les études actuelles sur les détecteurs concernent principalement: 1) l'optimisation de l'utilisation des effets physiques (infrarouge, lumière, ultrasons, radar, etc.); et 2) l'autosurveillance. Des travaux de développement intensif sont consacrés aux possibilités d'utilisation des lasers à balayage comme instruments de navigation pour les robots mobiles. Cela nécessite de résoudre les problèmes posés par deux tâches en principe partiellement distinctes: la navigation du robot et la protection des personnes et des matériels présents, pour éviter qu'ils ne soient heurtés, écrasés ou saisis (Freund, Dierks et Rossmann, 1993). Les futurs robots mobiles ne pourront pas conserver, en matière de sécurité, le principe de «séparation spatiale du robot et des personnes», qui est aujourd'hui appliqué strictement aux robots industriels fixes, et la fiabilité de fonctionnement des détecteurs de présence prévus joue donc un rôle prépondérant. La mise en œuvre d'une nouvelle technologie pose souvent des problèmes d'acceptation, et on peut supposer que la présence généralisée de robots mobiles, capables de se déplacer et de saisir des objets au milieu du personnel d'une usine, dans les lieux de passage du public, voire dans les habitations ou les espaces de loisirs, ne sera acceptée que s'ils sont équipés de détecteurs de présence très perfectionnés et très fiables. Il sera impératif d'éviter à tout prix des accidents spectaculaires si l'on ne veut pas exacerber d'éventuelles réticences. Le niveau actuel des dépenses pour la mise au point de ce type de détecteurs appliqués à la sécurité du travail n'est pas à la hauteur de cette préoccupation. Pour faire des économies substantielles, il faudrait développer et tester les détecteurs de présence en même temps que les robots mobiles et les systèmes de navigation, et non pas après.

En ce qui concerne les véhicules à moteur, les questions de sécurité revêtent de plus en plus d'importance. Les innovations en vue d'améliorer la sécurité des utilisateurs comprennent les ceintures de sécurité à trois points, les sièges pour enfants, les coussins gonflables et le système antiblocage des roues, vérifiés par des essais d'impact à grande échelle. Ces mesures de protection représentent une proportion accrue des coûts de production. Les développements futurs en matière de protection des utilisateurs concernent les coussins gonflables latéraux et les systèmes de détection radar pour mesurer la distance par rapport au véhicule précédent.

La sécurité extérieure des véhicules à moteur — c'est-à-dire la protection des tiers — fait l'objet d'une attention croissante. Une protection latérale est devenue récemment obligatoire, surtout pour les camions, afin de protéger les motocyclistes, les cyclistes et les piétons contre les risques de chute sous les roues arrière. La prochaine étape devrait logiquement être la surveillance de la zone située à l'arrière des véhicules lourds par des détecteurs de présence et l'installation de systèmes d'avertissement à l'arrière. Cette mesure aurait pour effet secondaire positif de procurer le financement nécessaire au développement, aux essais et à la mise sur le marché de détecteurs pour la sécurité au travail qui se caractériseraient par un prix raisonnable, des performances optimales, une capacité d'autosurveillance, une absence d'entretien et une bonne fiabilité. Le processus d'essais qui accompagnerait la mise en place à grande échelle de détecteurs et de systèmes de détecteurs favoriserait considérablement l'innovation dans d'autres secteurs (pelles mécaniques, chargeuses et machines mobiles diverses de gros gabarit avec lesquelles les déplacements en marche arrière peuvent représenter la moitié du temps d'utilisation). Le remplacement des robots fixes par des robots mobiles constitue également une voie de développement pour les détecteurs de présence. Des améliorations pourraient par exemple être apportées aux détecteurs employés actuellement sur les robots mobiles de manutention de matériaux ou les «chariots d'atelier sans conducteur», qui suivent des itinéraires fixes et n'exigent par conséquent que des mesures de sécurité limitées. L'utilisation de détecteurs de présence est la prochaine étape logique de l'amélioration de la sécurité dans le domaine du transport des matériaux et des personnes.

Les méthodes de détection

Pour évaluer et atteindre les objectifs mentionnés ci-dessus, on peut fait appel à différents principes physiques, associés à des méthodes de mesure et d'autosurveillance électroniques ainsi que, dans une certaine mesure, à des procédures informatiques à hautes performances. La facilité et la sûreté avec lesquelles fonctionnent apparemment les machines automatisées (robots), si répandues dans les films de science-fiction, deviendront peut-être réalité grâce aux techniques d'imagerie et aux algorithmes évolués de reconnaissance des formes, en association avec des méthodes de mesure des distances analogues à celles employées par les lasers à balayage. Il existe un paradoxe, dont il faut s'accommoder, selon lequel tout ce qui paraît simple à l'être humain est difficile pour les automates. Par exemple, une tâche complexe telle qu'une partie d'échecs de haut niveau (qui met en jeu le cerveau antérieur) est plus facile à reproduire et à faire exécuter par une machine qu'une tâche aussi simple que la marche, la coordination main-œil ou la coordination d'autres mouvements (régies par les cerveaux moyen et postérieur). Certains de ces principes, méthodes et procédures applicables à la mise en œuvre des détecteurs sont décrits ci-après. Outre ces exemples, il existe un grand nombre de procédures particulières, pour des tâches très spécialisées, qui opèrent notamment en associant différents types d'effets physiques.

Rideaux et barrages lumineux. Ces dispositifs font partie des premiers détecteurs de présence mis au point. Ils ont une géométrie de surveillance ponctuelle, c'est-à-dire qu'une personne ayant franchi la barrière n'est plus détectée. La main d'un opérateur, ou la présence d'outils ou de pièces tenus dans la main de l'opérateur, par exemple, sont détectés avec rapidité et fiabilité par ces dispositifs. Ils contribuent largement à la sécurité des machines (comme les presses et les poinçonneuses) où le matériau doit être introduit à la main. Leur fiabilité doit être statistiquement très élevée, étant donné que si la main ne se présente que deux ou trois fois par minute, c'est environ un million d'opérations qui sont effectuées en quelques années à peine. L'autosurveillance réciproque entre émetteur et récepteur a été portée à un tel niveau technique qu'elle représente aujourd'hui une norme pour toutes les autres méthodes de détection de présence.

Tapis de contact (à contacteurs). Les tapis et les sols à contact électrique ou pneumatique peuvent être du type passif ou actif (avec pompe). A l'origine, ils étaient largement utilisés pour des fonctions de service (ouverture de portes), avant d'être remplacés par des détecteurs de mouvement. La tendance est à l'extension de l'application des détecteurs de présence à toutes sortes de zones dangereuses. Le développement de la fabrication automatisée, par exemple, dans laquelle l'opérateur, au lieu de commander directement la machine, se borne à en surveiller le fonctionnement, a suscité une demande de détecteurs appropriés. La normalisation de cette application est bien avancée (DIN, 1997) et des limitations particulières (agencement, dimensions, zone morte maximale autorisée) ont nécessité le développement d'un savoir-faire spécifique.

Les tapis de contact trouvent d'intéressantes possibilités d'emploi dans les systèmes à robots multiples contrôlés par ordinateur. L'opérateur active un ou deux contacts, ce qui permet au détecteur de présence de connaître sa position exacte et d'en informer l'ordinateur, qui gère les systèmes de commande des robots grâce à un système anticollision intégré. Lors d'un essai effectué par l'Institut fédéral allemand pour la sécurité (BAU), un sol formé de tapis à contact électrique de faibles dimensions a été installé sous la zone de travail d'un bras de robot (Freund, Dierks et Rossmann, 1993). Ce détecteur de présence avait la forme d'un damier. Le secteur activé indiquait à l'ordinateur la position de l'opérateur (voir figure 58.48) et lorsque celui-ci se rapprochait trop du robot, le robot s'écartait. Sans ce détecteur de présence, le robot ne pourrait pas déterminer la position de l'opérateur et celui-ci ne pourrait être protégé.

Réflecteurs (détecteurs de mouvement et détecteurs de présence). Quels que soient leurs mérites, les détecteurs décrits ci-dessus ne sont pas des détecteurs de présence au sens large. Pour que leur utilisation sur les véhicules lourds et les grands équipements mobiles, principalement en vue d'assurer la sécurité du travail, puisse être envisagée, il est nécessaire que deux caractéristiques importantes soient réunies: 1) la possibilité de surveiller une zone depuis une position donnée; et 2) un fonctionnement fiable et ne nécessitant pas de mesures complémentaires concernant l'objet à détecter, comme l'installation de dispositifs réfléchissants. Pour que l'équipement puisse déceler la présence d'une personne pénétrant dans la zone surveillée, et ce jusqu'à ce qu'elle ait quitté cette zone, il est nécessaire également qu'il détecte une personne restant parfaitement immobile. C'est ce qui distingue les détecteurs de mouvement des détecteurs de présence, du moins en ce qui concerne une utilisation avec des équipements mobiles: les détecteurs de mouvement sont presque toujours déclenchés lorsque le véhicule commence à se déplacer.

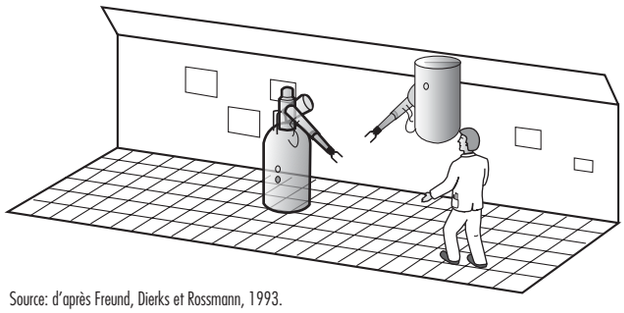
Détecteurs de mouvement. Les deux principaux types de détecteurs de mouvement sont: 1) les détecteurs infrarouges passifs, qui réagissent au plus petit changement du faisceau infrarouge dans la zone surveillée (le plus petit faisceau détectable est d'environ 10^{-9} W, avec une plage de longueur d'onde d'environ 7 à 20 µm); 2) les détecteurs à ultrasons et à micro-ondes à effet Doppler, qui déterminent les caractéristiques du déplacement d'un objet en fonction des changements de fréquence. L'effet Doppler augmente par exemple la fréquence du sifflet d'une locomotive pour un observateur pendant qu'elle approche et diminue cette fréquence lorsque la locomotive s'éloigne. L'application de cet effet permet de construire des détecteurs d'approche relativement simples, le récepteur n'ayant qu'à surveiller la fréquence du signal des bandes voisines en guettant l'apparition de la fréquence Doppler.

Vers le milieu des années soixante-dix, l'emploi de détecteurs de mouvement a pris une place prédominante dans les fonctions de service comme l'ouverture des portes, la protection contre le vol et la protection des objets. Pour un usage fixe, la détection d'une personne approchant d'une zone dangereuse constituait un élément suffisant pour donner l'alerte en temps voulu ou pour arrêter une machine. C'est sur cette base que l'on a entrepris d'étudier les possibilités d'utilisation des détecteurs de mouvement, en particulier les détecteurs infrarouges passifs pour la sécurité au travail (Mester et coll., 1980). Etant donné qu'une personne habillée a généralement une température supérieure à celle de son environnement (tête 34 °C, mains 31 °C), la détection d'une personne qui s'approche est relativement plus facile que celle d'un objet inanimé. C'est ainsi que des éléments de machine peuvent se déplacer dans la zone surveillée sans déclencher le détecteur.

La méthode passive (sans émetteur) présente des avantages et des inconvénients. L'avantage est qu'un détecteur infrarouge passif n'ajoute ni bruit ni problèmes de brouillage électrique. Pour la protection contre le vol et la protection d'objets, il est particulièrement important que le détecteur ne soit pas facile à repérer. En revanche, un capteur limité à un simple récepteur peut difficilement contrôler sa propre efficacité, ce qui est essentiel pour la sécurité au travail. Pour remédier à cet inconvénient, des essais ont porté sur de petits émetteurs d'infrarouges modulés (5 à 20 Hz) qui étaient installés dans la zone surveillée et qui ne déclenchaient pas le capteur, mais dont le rayonnement était enregistré avec une amplification électronique fixe réglée sur la fréquence de modulation. Cette modification faisait d'un détecteur passif un détecteur actif, ce qui permettait également de vérifier la précision géométrique de la zone surveillée. Les miroirs peuvent avoir des zones aveugles, et l'orientation d'un détecteur passif peut être compromise par les divers incidents de l'activité d'une usine. La figure 58.49 montre une installation d'essai avec un détecteur infrarouge passif surveillant une zone de forme pyramidale. Compte tenu de leur longue portée, les détecteurs infrarouges passifs sont employés, par exemple, dans les allées d'un espace de stockage.

Ces essais ont montré que, d'une manière générale, les détecteurs de mouvement ne convenaient pas pour la sécurité au tra-

Figure 58.48 • Une personne et deux robots dans des enveloppes modélisées



Source: d'après Freund, Dierks et Rossmann, 1993.

Figure 58.49 • Détecteur infrarouge passif employé comme détecteur d'approche dans une zone dangereuse

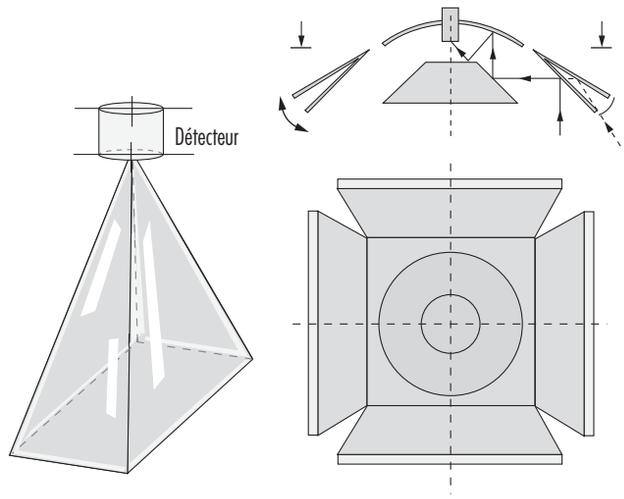
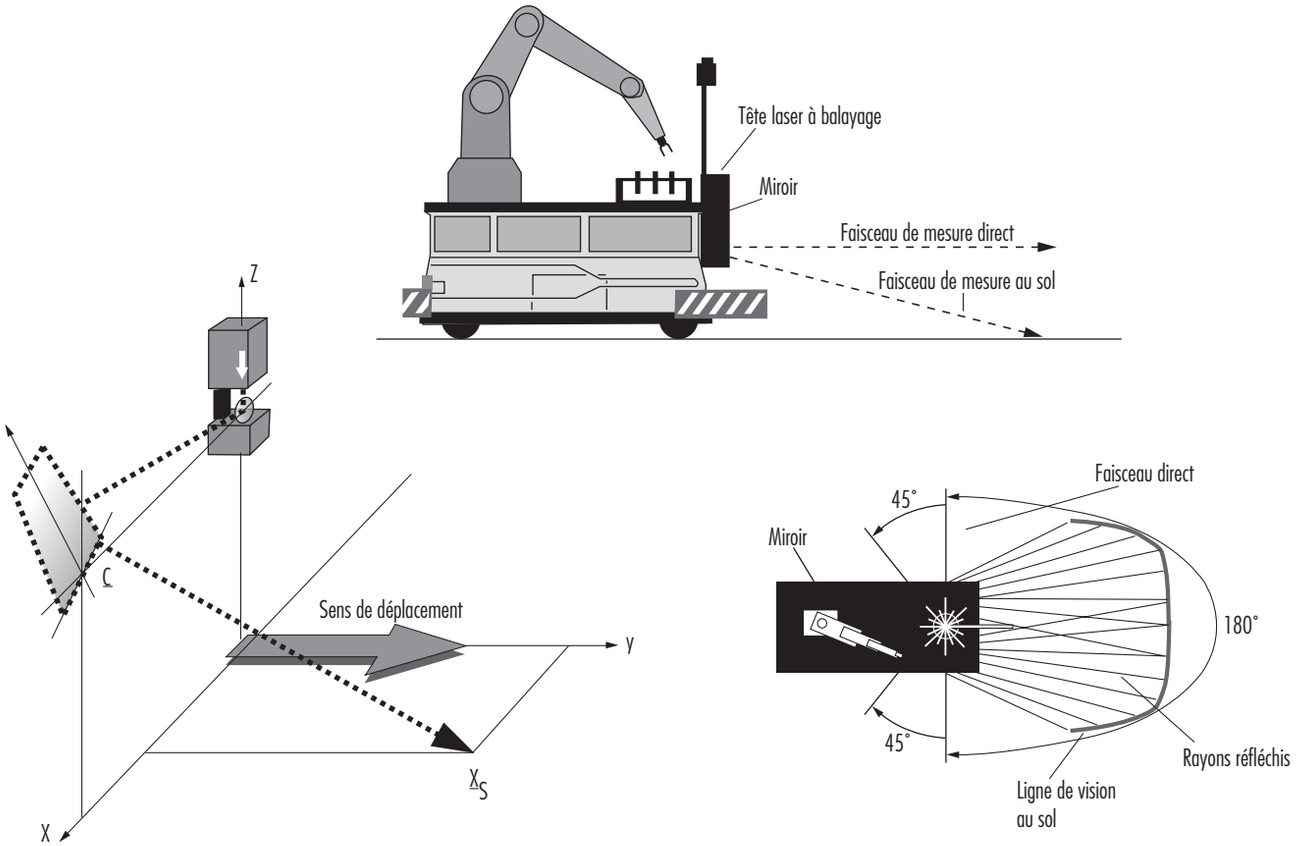


Figure 58.50 • Robot mobile à balayage par laser pour la navigation et la détection de présence



Source: d'après Freund, Dierks et Rossmann, 1993.

vail. La surveillance nocturne des salles d'un musée ne peut pas être comparée à celle des zones dangereuses d'un atelier.

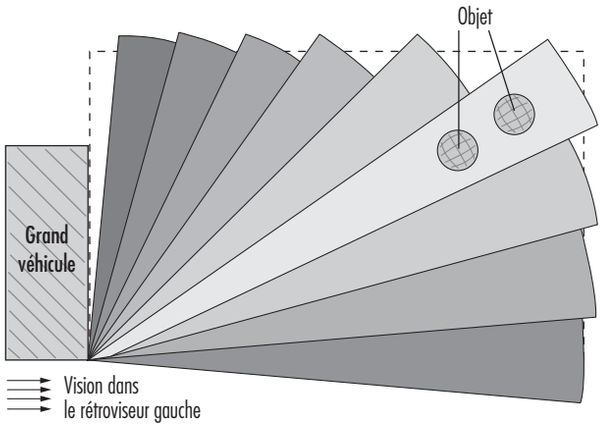
Détecteurs à impulsions ultrasonores, radar ou lumineuses. Les détecteurs fonctionnant sur le principe impulsion/écho — c'est-à-dire ceux qui mesurent le temps de retour d'impulsions ultrasonores, radar ou lumineuses — offrent d'importantes possibilités d'application comme détecteurs de présence. Avec les lasers à balayage, les impulsions peuvent balayer une zone avec une périodicité élevée (habituellement par rotation), horizontalement par exemple; grâce à un ordinateur, on peut donc obtenir un profil de distance des objets ayant réfléchi la lumière sur la ligne ainsi définie. Si l'on ne se contente pas d'une ligne unique, mais qu'on veuille tout l'espace situé à l'avant du robot mobile jusqu'à une hauteur de 2 m, par exemple, il faut traiter d'énormes quantités de données pour décrire l'environnement. Le détecteur de présence «idéal» de l'avenir sera constitué d'une combinaison des deux procédés suivants:

1. Un procédé de reconnaissance des formes, composé d'une caméra et d'un ordinateur, celui-ci pouvant également être un «réseau de neurones».
2. Un procédé de balayage laser pour mesurer les distances. Ce procédé consiste à relever, dans un espace tridimensionnel, un certain nombre de points sélectionnés par le processus de reconnaissance des formes, à indiquer les distances et à détecter les mouvements à partir de la vitesse et de la direction.

La figure 58.50 montre, dans le cadre du projet BAU cité plus haut (Freund, Dierks et Rossmann, 1993), l'utilisation d'un laser à balayage sur un robot mobile qui accomplit également certaines tâches de navigation grâce à un faisceau de détection de direction et assure une protection contre les collisions avec des objets se trouvant à proximité immédiate au moyen d'une détection de présence assurée par un faisceau de mesure au sol. Avec ces fonctions, le robot mobile est capable de se diriger par pilotage libre automatisé actif (c'est-à-dire qu'il sait contourner les obstacles). Techniquement, on emploie pour cela la rotation à 45° du balayage vers l'arrière des deux côtés (à gauche et à droite du robot), en plus de la rotation à 180° vers l'avant. Ces faisceaux, par l'intermédiaire d'un miroir spécial, font office de rideau lumineux orienté vers le sol en avant du robot et donnent à celui-ci une ligne de vision au sol. S'il reçoit une réflexion laser de cette zone, le robot s'arrête. Des systèmes à balayage laser et lumineux homologués pour la sécurité au travail ont déjà été proposés sur le marché; ils ont encore un important potentiel d'évolution.

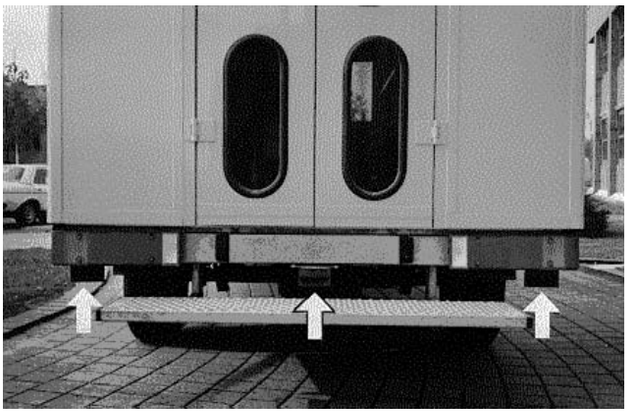
Les détecteurs à ultrasons et radar, qui déterminent la distance sur la base du temps écoulé entre le signal et la réponse, sont moins exigeants du point de vue technique et donc plus économiques à produire. La zone de détection a une tête arrondie, avec une ou plusieurs zones latérales plus petites disposées symétriquement. La vitesse de propagation du signal (330 m/s pour le son et 300 000 km/s pour les ondes électromagnétiques) détermine la rapidité de traitement de l'électronique employée.

Figure 58.51 • Disposition de la tête de détection et de la zone surveillée à l'arrière d'un camion



Source: d'après Langer et Kurfürst, 1985.

Figure 58.52 • Camion de tonnage moyen équipé d'un système avertisseur de recul (Microsonic GmbH, Dortmund)



Dispositifs avertisseurs de recul. A la Foire-Exposition de Hanovre de 1985, le BAU a exposé les résultats d'un avant-projet sur l'emploi de détecteurs à ultrasons pour sécuriser la zone située à l'arrière des gros véhicules (Langer et Kurfürst, 1985). Une maquette à échelle réelle de la tête de détection, constituée de détecteurs Polaroid™, était installée sur la paroi arrière d'un camion de livraison. La figure 58.51 montre le principe de son fonctionnement. Du fait de son grand diamètre, ce détecteur produit des zones de surveillance de longue portée et d'angle relativement réduit (environ 18°), qui sont juxtaposées et réglées sur des portées maximales différentes du signal. En pratique, cet agencement permet de définir toutes les géométries désirées, qui sont balayées par les détecteurs environ quatre fois par seconde pour détecter la présence ou l'arrivée de personnes. D'autres systèmes avertisseurs arrière en démonstration possédaient plusieurs détecteurs parallèles.

Cette démonstration spectaculaire a rencontré un grand succès à la Foire-Exposition. Elle a montré que la sécurisation de la zone arrière des gros véhicules faisait l'objet d'études dans de nombreux organismes, notamment les comités spécialisés des associations professionnelles (Berufsgenossenschaften), les compagnies assurant les véhicules municipaux, les autorités de contrôle de l'industrie et les fabricants de détecteurs, ces derniers s'intéressant plutôt aux voitures particulières et concentrant leurs efforts sur les systèmes destinés à faciliter les manœuvres sur les parkings pour éviter que les carrosseries subissent des dommages. Un comité ad hoc a été créé spontanément pour promouvoir les systèmes de détection vers l'arrière; il a entrepris en premier lieu de dresser la liste des besoins en matière de sécurité au travail. Dans les dix années qui ont suivi, de nombreux efforts ont été consacrés au problème de la surveillance vers l'arrière — qui représente peut-être l'application la plus importante des détecteurs de présence —, mais il n'y a toujours pas eu d'avancée majeure.

Les détecteurs à ultrasons ont été employés dans de nombreux projets, notamment pour équiper des grues de triage de bois, des pelles hydrauliques, des véhicules municipaux spéciaux et d'autres véhicules utilitaires, ainsi que des chariots élévateurs et des chargeuses (Schreiber, 1990). Les dispositifs avertisseurs de recul présentent une importance particulière pour les gros engins qui fonctionnent fréquemment en marche arrière. Les détecteurs de présence à ultrasons sont utilisés par exemple pour la protection de véhicules spéciaux sans conducteur, comme les machines robotisées de manutention. Par rapport aux pare-chocs caoutchoutés, ces détecteurs ont une plus grande portée qui permet un freinage avant le contact entre la machine et un obstacle. Les détecteurs correspondants pour les voitures particulières constituent des développements avec des contraintes nettement moins sévères.

Entre-temps, le Comité DIN de normalisation technique des systèmes de transport a élaboré la norme 75031, «Dispositifs de détection d'obstacles en marche arrière» (DIN, 1995). Les spécifications et les essais ont été définis pour deux distances: 1,8 m pour les camions de livraison, et 3 m — une zone d'avertissement supplémentaire — pour les poids lourds. La zone surveillée est déterminée par la reconnaissance de corps cylindriques. La distance de 3 m correspond sensiblement à la limite de ce qui est techniquement réalisable à l'heure actuelle, étant donné que les détecteurs à ultrasons doivent être enfermés dans des enveloppes métalliques en raison des conditions difficiles dans lesquelles ils doivent fonctionner. Les caractéristiques d'autosurveillance du système de détecteurs sont fixées, la géométrie requise pour la zone de surveillance ne pouvant être obtenue qu'avec un système de trois détecteurs ou plus. La figure 58.52 montre un dispositif avertisseur de recul composé de trois détecteurs à ultrasons. Les caractéristiques du dispositif avertisseur de recul dans la cabine du conducteur et les modalités des signaux d'alarme sont fixées également. Les dispositions de la norme DIN 75031 sont reprises dans le rapport technique international ISO/TR 12155, *Véhicules utilitaires. Dispositifs de détection d'obstacles pendant la marche arrière. Exigences et essais* (ISO, 1994a). Plusieurs fabricants de détecteurs ont mis au point des prototypes conformes à cette norme.

Conclusion

Depuis le début des années soixante-dix, plusieurs institutions et fabricants ont travaillé au développement et à la réalisation de détecteurs de présence. Pour l'application particulière de l'avertisseur de recul, les dispositions existantes sont la norme DIN 75031 et le rapport ISO/TR 12155. La Deutsche Post poursuit des essais d'une importance majeure. Plusieurs fabricants ont équipé chacun cinq camions de taille moyenne avec ces dispositifs. Il est très important pour la sécurité au travail que ces essais donnent des résultats concluants. Comme nous l'avons précisé au début de cet article, la disponibilité de détecteurs de présence en nombre suffisant pose un défi majeur pour la technologie de la sécurité dans les nombreuses applications mentionnées. Il faut que ces équipements puissent être réalisés à un faible prix de revient si

l'on veut que les dommages aux équipements, aux machines et aux produits et surtout les lésions corporelles, souvent graves, appartiennent désormais au passé.

LES APPAREILLAGES DE CONTRÔLE, DE COUPURE ET DE COMMUTATION D'ÉNERGIE

René Troxler

Les appareils de contrôle, de coupure et de commutation doivent toujours être considérés en relation avec les *systèmes techniques*, expression qui désigne, dans le présent article, les machines, les installations et les équipements. Tout système technique accomplit une tâche spécifique. Des appareils de contrôle et de commutation assurant la sécurité voulue sont nécessaires pour que cette tâche soit réalisable, voire envisageable, sans risques. Ces appareils servent à établir, contrôler, interrompre ou retarder la circulation ou les effets des énergies électrique, hydraulique, pneumatique ou potentiellement dangereuse.

L'isolation et la réduction de l'énergie

Les dispositifs de coupure servent à interrompre l'alimentation en énergie. Le dispositif doit normalement assurer une déconnexion effective, et pouvant être déterminée sans équivoque, de l'alimentation en énergie. La déconnexion de l'alimentation devrait également être toujours associée à une réduction de l'énergie emmagasinée dans toutes les parties de l'installation. Si celle-ci est alimentée par plusieurs sources, elles doivent toutes pouvoir être déconnectées correctement. Les personnes qualifiées pour intervenir sur le type d'énergie concerné et travaillant de ce côté de l'installation utilisent les dispositifs de coupure pour se protéger contre les dangers de cette énergie. Pour des raisons de sécurité, ces personnes s'assurent toujours qu'aucune énergie potentiellement dangereuse ne subsiste dans le système technique, par exemple en vérifiant l'absence de potentiel dans le cas de l'électricité. Seuls des spécialistes qualifiés peuvent manipuler sans danger certains dispositifs de coupure, et on doit donc prendre des dispositions pour que les personnes non autorisées ne puissent y avoir accès (voir figure 58.53).

Les dispositifs de coupure générale

Un dispositif de coupure générale déconnecte l'installation de son alimentation en énergie. Contrairement aux dispositifs de coupure, il peut être actionné sans danger même par des non-spécialistes. Il sert à déconnecter les installations inutilisées à un moment donné et à empêcher leur utilisation par des personnes non autorisées. Il sert également à déconnecter les installations pour l'entretien, les dépannages, les nettoyages, les réglages et les remplacements d'équipements, dans la mesure où ces travaux peuvent être effectués en l'absence d'énergie. Naturellement, lorsqu'un dispositif de coupure générale possède également les caractéristiques d'un dispositif de coupure, il peut aussi assurer ou partager cette fonction (voir figure 58.54).

Le dispositif de coupure de sécurité

Un dispositif de coupure de sécurité ne déconnecte pas la totalité de l'installation de sa source d'énergie. Il supprime uniquement l'énergie des parties de l'installation qui sont critiques pour un sous-système opérationnel particulier. Il est possible de prévoir des interventions de courte durée sur certains sous-systèmes opérationnels — par exemple pour des réglages, des modifications de réglages, des changements d'équipements, des réparations ou des nettoyages périodiques, ainsi que pour l'exécution de mouvements et de séquences d'opérations indispensables aux réglages, aux modifications de réglages, aux changements d'équipements ou aux essais. Les équipements et installations complexes de production ne peuvent pas être mis à l'arrêt au moyen de la coupure générale dans ces cas, parce qu'il serait alors impossible, après la réparation, de remettre en service l'installation complète au stade où son fonctionnement avait été interrompu. En outre, dans les grands systèmes techniques, le dispositif de coupure générale est rarement situé à l'endroit où doit avoir lieu l'intervention. Un dispositif de coupure de sécurité doit donc répondre à un certain nombre d'exigences, notamment:

Figure 58.53 • Dispositifs de coupure électriques et pneumatiques

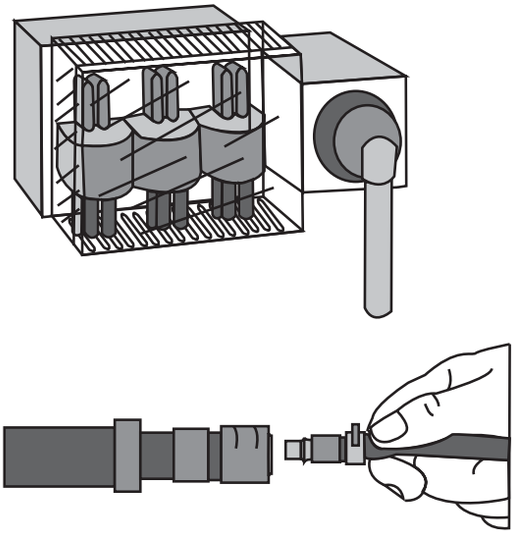


Figure 58.54 • Exemples de dispositifs de coupure générale électriques et pneumatiques

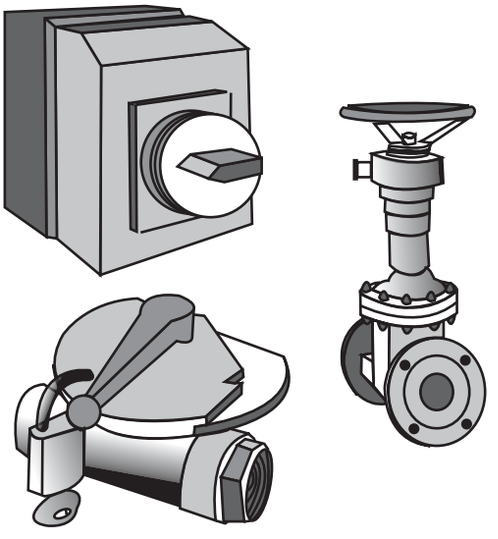
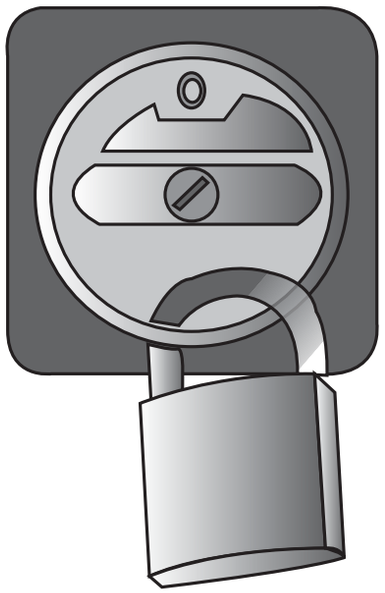


Figure 58.55 • Dispositif de coupure de sécurité



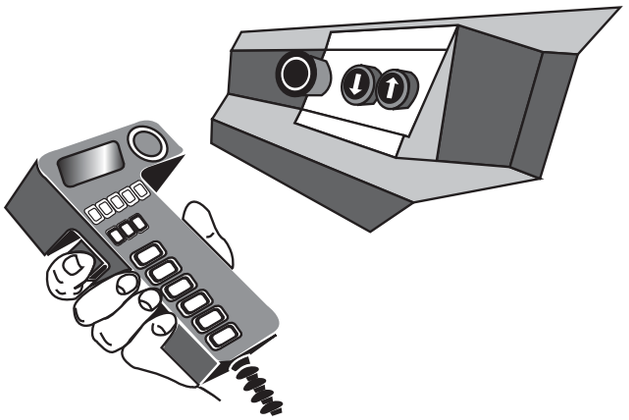
- Il doit interrompre la circulation d'énergie de manière fiable et de telle sorte qu'aucun mouvement ou processus dangereux ne puisse être déclenché par la transmission ou l'apparition accidentelles de signaux de commande.
- Il doit être installé à l'emplacement précis des interventions dans des zones dangereuses des sous-systèmes opérationnels. Si nécessaire, ces dispositifs peuvent être installés en plusieurs endroits, par exemple à différents étages, dans plusieurs salles, ou en différents points d'accès aux machines ou aux équipements.
- Son dispositif de commande doit comporter une position «arrêt» bien visible et qui doit apparaître uniquement après l'interruption effective de la circulation d'énergie.
- Une fois en position «arrêt», ce dispositif de commande doit pouvoir être protégé contre les réenclenchements non autorisés: *a)* lorsqu'il n'est pas possible de surveiller correctement les zones dangereuses depuis la zone de contrôle; *b)* lorsque les personnes se trouvant dans la zone dangereuse ne peuvent pas voir facilement et constamment le dispositif de commande; et *c)* lorsqu'un verrouillage ou un marquage est imposé par la législation ou le règlement interne.
- Le dispositif ne doit déconnecter qu'un seul des éléments fonctionnels d'un système technique étendu dans les cas où les autres éléments fonctionnels peuvent continuer à opérer sans danger pour les personnes effectuant l'intervention.

Lorsque le dispositif de coupure générale d'une installation est en mesure de répondre à toutes les caractéristiques exigées d'un dispositif de coupure de sécurité, il peut assurer également cette fonction, mais cette solution ne sera à l'évidence fiable que pour les systèmes techniques les plus simples (voir figure 58.55).

Les dispositifs de commande des sous-systèmes opérationnels

Ces dispositifs de commande permettent de déclencher et de contrôler en toute sécurité les mouvements et les séquences d'opérations des sous-systèmes opérationnels. Ils peuvent être nécessaires pour les réglages en vue de l'exécution de séquences d'essai, pour la régulation, lorsqu'il faut corriger des défauts de fonctionnement ou dégager des zones obstruées, ou pour la formation en vue de démonstrations de leur fonctionnement. En pareils cas, une remise en route normale de l'installation est impossible, car elle exposerait les opérateurs à des mouvements ou des processus déclenchés par la transmission ou l'apparition accidentelles de signaux de commande. Un dispositif de commande de sous-système opérationnel doit répondre aux exigences ci-après:

Figure 58.56 • Dispositifs de commande mobile et fixe pour sous-systèmes

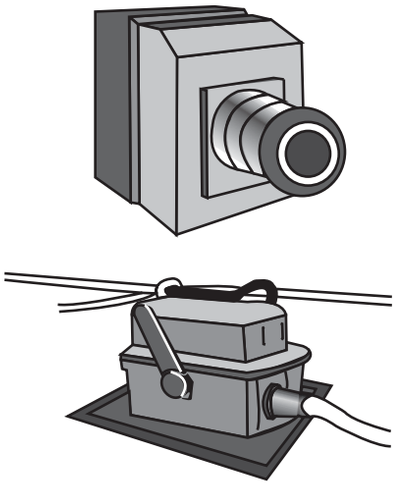


- Il doit permettre d'exécuter sans danger les mouvements et les processus nécessaires au niveau du sous-système. Certains mouvements sont exécutés selon le cas à vitesse réduite, progressivement ou à puissance réduite; le processus est en règle générale interrompu immédiatement lorsque le tableau de commande n'est plus actionné.
- L'emplacement des tableaux et organes de commande doit être choisi de manière que les opérateurs puissent les actionner sans danger et que les processus contrôlés soient entièrement visibles.
- Lorsque plusieurs tableaux de commande contrôlant plusieurs processus sont regroupés au même endroit, ils doivent être signalés clairement et disposés logiquement, avec une délimitation nette.
- Les dispositifs de commande des sous-systèmes opérationnels ne doivent être activés que lorsque le mode de fonctionnement normal est effectivement mis à l'arrêt, c'est-à-dire lorsqu'on s'est assuré qu'aucune commande de ce mode ne peut être activée.
- Il doit être possible d'interdire l'utilisation non autorisée des sous-systèmes opérationnels, par exemple grâce à une clé ou à un code spéciaux, sans lesquels la fonction en question ne peut être exécutée (voir figure 58.56).

Les dispositifs d'arrêt d'urgence

Les dispositifs d'arrêt d'urgence sont nécessaires lorsque le fonctionnement normal des systèmes techniques peut créer des dangers qu'il n'est pas possible de prévenir au niveau de la conception du système ou par la prise de mesures de sécurité appropriées. Dans les sous-systèmes opérationnels, le dispositif d'arrêt d'urgence fait souvent partie de l'appareillage de commande. Lorsqu'il est actionné, il déclenche des opérations qui ramènent aussi rapidement que possible le système à l'état de sécurité. En ce qui concerne les priorités de sécurité, la protection des personnes est primordiale. La protection contre les dommages matériels joue un rôle secondaire, à moins que ces dommages ne puissent à leur

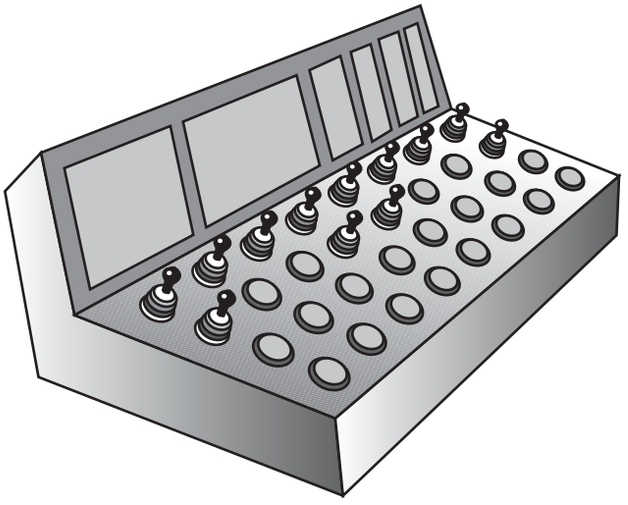
Figure 58.57 • Dispositif d'arrêt d'urgence



tour mettre des personnes en danger. Le dispositif d'arrêt d'urgence doit répondre aux exigences ci-après:

- Il doit rétablir aussi rapidement que possible un fonctionnement sûr de l'installation.
- Son tableau de commande doit être facile à reconnaître et il doit être conçu et placé de manière que les personnes en danger puissent l'actionner sans difficulté et qu'il soit à la portée du personnel de secours.
- Les processus d'urgence qu'il déclenche ne doivent pas créer de nouveaux dangers. En particulier, ils ne doivent pas libérer des dispositifs de serrage, déconnecter des fixations magnétiques ou bloquer des systèmes de sécurité.
- Après le déclenchement d'un arrêt d'urgence, l'installation ne doit pas pouvoir redémarrer automatiquement lors de la réinitialisation du tableau de commande du dispositif, mais uniquement à la suite d'une action délibérée sous la forme d'une commande de remise en marche (voir figure 58.57).

Figure 58.58 • Représentation schématique d'un pupitre de commande

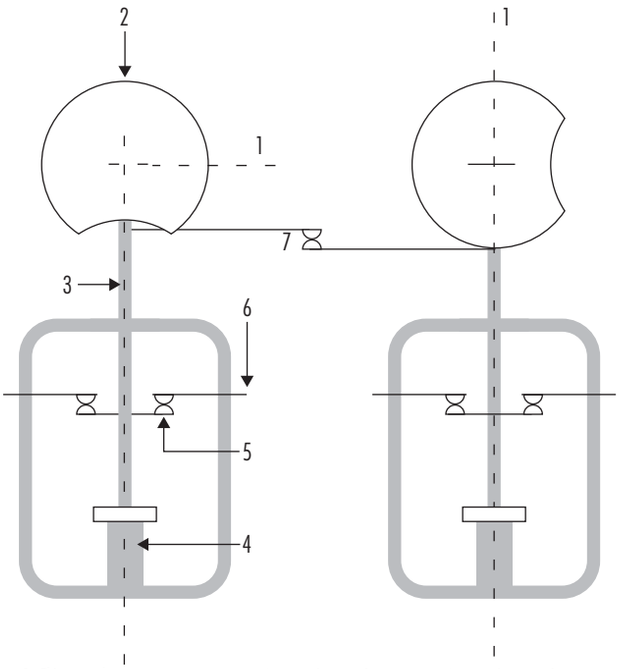


Les dispositifs de commande de fonctions

Les dispositifs de commande de fonctions servent à mettre le système technique en fonctionnement normal et à lancer, exécuter et interrompre les mouvements et processus prévus dans ce mode. Ces dispositifs servent exclusivement au cours du fonctionnement normal de l'installation, c'est-à-dire lorsque toutes les fonctions prévues se déroulent sans incidents. Ils sont donc employés par les opérateurs du système. Les dispositifs de commande de fonctions doivent répondre aux exigences ci-après:

- Leurs tableaux de commande doivent être accessibles, d'emploi facile et sans danger.
- Ces tableaux de commande doivent être agencés de manière claire et rationnelle. Ainsi, l'actionnement des boutons de commande doit correspondre de manière «rationnelle» aux mouvements commandés, haut, bas, droite et gauche (cette notion de correspondance «rationnelle» entre les commandes et leurs effets peut varier selon les lieux et elle est parfois définie par la réglementation).
- Ces tableaux de commande doivent comporter des inscriptions claires et intelligibles utilisant des symboles faciles à comprendre.
- Les processus qui nécessitent toute l'attention de l'utilisateur pour être exécutés sans danger ne doivent pas pouvoir être déclenchés par des signaux de commande produits par erreur, ou par l'actionnement involontaire des dispositifs de commande correspondants. Le traitement des signaux des tableaux de commande doit être suffisamment fiable et le dispositif de commande doit être conçu de manière à rendre impossible un déclenchement involontaire (voir figure 58.58).

Figure 58.59 • Schéma d'un interrupteur de position à commande et coupure automatiques



Les interrupteurs de position

Les interrupteurs de position empêchent la mise en marche d'une installation tant que les conditions de sécurité surveillées ne sont pas satisfaites et ils interrompent son fonctionnement dès qu'une de ces conditions n'est plus remplie. Ils servent par exemple à surveiller les portes des compartiments de sécurité, à vérifier la position des protections ou à s'assurer que les limites de vitesse ou de course ne sont pas dépassées. Les interrupteurs de position doivent par conséquent répondre aux exigences de sécurité et de fiabilité ci-après:

- L'appareillage utilisé pour la surveillance doit émettre le signal protecteur avec une fiabilité élevée. Ainsi, les interrupteurs mécaniques à action automatique permettent d'interrompre la circulation du signal avec une grande fiabilité.
- Cet appareillage doit être actionné avec une fiabilité élevée lorsqu'une condition de sécurité n'est pas satisfaite (par exemple, une tige d'un interrupteur de position à interruption automatique enfoncée mécaniquement et automatiquement en position interruption).
- Il doit être impossible de désactiver sans raison l'interrupteur de position, du moins involontairement et sans un certain effort. On peut utiliser un interrupteur mécanique à commande automatique avec interruption automatique lorsque l'interrupteur et l'organe de commande sont solidement fixés (voir figure 58.59).

Les circuits de contrôle de sécurité

Plusieurs des appareils de commutation de sécurité décrits ci-dessus assurent la fonction de sécurité non pas directement, mais par l'émission d'un signal qui est ensuite transmis et traité par un circuit de contrôle de la sécurité avant d'atteindre les parties de l'installation qui exercent la fonction de sécurité proprement dite. Un dispositif de coupure de sécurité, par exemple, provoque indirectement la déconnexion de l'énergie aux points critiques, tandis qu'un dispositif de coupure générale arrête directement l'alimentation électrique.

Les circuits de contrôle de sécurité doivent assurer une transmission fiable des signaux et, dans ce but, il convient de prendre en compte les principes ci-après:

- La sécurité doit être garantie même lorsque l'énergie extérieure est absente ou insuffisante, par exemple en cas de conduite déconnectée ou de fuite.
- Les signaux de protection sont plus fiables lorsqu'ils sont obtenus par l'interruption du signal, par exemple au moyen de contacteurs de sécurité à ouverture des contacts ou de relais à contacts à ouverture.
- La fonction de protection des amplificateurs, transformateurs et équipements similaires est obtenue avec plus de fiabilité en l'absence d'énergie extérieure. Ce genre de mécanismes comprend, par exemple, les appareils de commutation électromagnétiques ou les vannes en position fermée au repos.
- Les branchements réalisés par erreur ou les fuites dans le circuit de contrôle de la sécurité ne doivent pas conduire à des démarrages intempestifs ni empêcher les mises à l'arrêt (court-circuit entre les circuits d'arrivée et de retour, fuites à la terre ou liaison à la masse).
- Les influences extérieures dont l'effet sur le système demeure conforme aux prévisions ne doivent pas gêner la fonction de sécurité du circuit de contrôle.

Les composants employés dans les circuits de contrôle de la sécurité doivent remplir leur fonction avec une très grande fiabilité. Ceux d'entre eux qui ne répondent pas à cette exigence doivent être mis en œuvre selon le principe d'une redondance contrôlée et diversifiée au maximum.

LES APPLICATIONS DE L'INFORMATIQUE À LA SÉCURITÉ

Dietmar A.J. Reinert et Karlheinz Meffert

Depuis quelques années, les microprocesseurs occupent une place toujours plus importante dans la technologie de la sécurité. Etant donné qu'il est désormais possible d'avoir un ordinateur complet, c'est-à-dire un processeur, une mémoire et des périphériques, sur un seul composant (ordinateurs «monopuce»), la technologie des microprocesseurs n'est plus réservée au contrôle des machines complexes, mais elle est employée aussi pour des systèmes de protection relativement simples (par exemple, barrage immatériel, commandes bimanuelles et protections des extrémités). Les logiciels de contrôle de ces systèmes comprennent entre un millier et plusieurs dizaines de milliers d'instructions, avec plusieurs centaines de branchements logiques. Ils fonctionnent en temps réel et sont le plus souvent écrits en langage assembleur.

L'introduction de systèmes contrôlés par ordinateur dans la technologie de la sécurité a occasionné, pour tous les grands équipements, non seulement de coûteux projets de recherche et de développement, mais aussi des contraintes significatives destinées à renforcer la sécurité (les technologies aérospatiale, militaire et nucléaire sont des exemples d'applications à grande échelle). Le domaine de la grande production industrielle a été très peu abordé jusqu'à présent. Cela s'explique en partie par le fait que la rapidité des cycles d'innovation qui caractérise la conception des machines industrielles ne permet qu'un transfert très limité des connaissances résultant de projets de recherche ayant pour objectif les essais finals de dispositifs de sécurité à grande échelle. Cette situation rend d'autant plus souhaitable la mise au point de procédures d'évaluation rapides et économiques (Reinert et Reuss, 1991).

Dans le présent article, nous examinons en premier lieu les machines et les installations dans lesquelles des systèmes informatisés assurent maintenant déjà des tâches de sécurité, en prenant des exemples d'accidents qui se produisent surtout au niveau de la protection des machines, pour illustrer le rôle particulier des ordinateurs dans la technologie de la sécurité. Ces accidents donnent certaines indications sur les précautions à prendre pour que le développement actuel de l'utilisation d'équipements de sécurité commandés par ordinateur ne contribue pas à une augmentation du nombre des accidents. La dernière partie de l'article décrit les grandes lignes d'une procédure qui devrait permettre de donner, même aux petits systèmes informatiques, un niveau de sécurité technique suffisant, pour un investissement raisonnable et dans des délais acceptables. Les principes exposés dans cette dernière partie sont actuellement repris dans les procédures de normalisation au niveau international et ils auront des répercussions dans tous les domaines de la technologie de la sécurité qui font appel aux ordinateurs.

Exemples d'utilisation de logiciels et d'ordinateurs dans les systèmes de protection des machines

Les quatre exemples suivants montrent l'importance croissante de l'utilisation des logiciels et des ordinateurs par l'industrie dans le domaine de la sécurité.

Les dispositifs individuels d'alarme se composent en général d'un poste de réception central et de plusieurs appareils individuels d'alarme. Ceux-ci sont portés par des personnes appelées à travailler seules. Si l'une de ces personnes isolées se trouve en danger, elle peut se servir de l'appareil pour déclencher une alarme, en transmettant un signal radio au poste de réception. Ce déclenchement volontaire peut être complété par un mécanisme de déclenchement automatique activé par des détecteurs intégrés

à l'appareil individuel. Les appareils individuels et le poste de réception sont fréquemment contrôlés par des micro-ordinateurs; si l'une des fonctions de l'ordinateur cessait d'être assurée, l'alarme pourrait ne pas se déclencher en cas de danger. Des mesures doivent donc être prises pour détecter et rectifier en temps voulu ces défauts de fonctionnement.

Les presses d'imprimerie à journaux sont de très grosses machines. Les bandes continues de papier sont généralement préparées par une machine distincte qui assure sans interruption les changements de bobine. Les pages imprimées sont pliées et traitées ensuite par d'autres machines pour aboutir en fin de chaîne à des palettes chargées. Bien que ces installations soient automatisées, il existe deux points où des interventions manuelles sont nécessaires: 1) l'amorçage du papier dans le circuit; 2) le dégagement des bourrages provoqués par la déchirure du papier aux points dangereux des rouleaux. La technologie de contrôle des installations doit donc permettre un fonctionnement au ralenti ou pas à pas, limité à un circuit ou dans le temps, pendant le réglage des presses. Compte tenu de la complexité des opérations de pilotage, chaque poste d'impression individuel doit posséder son propre automate programmable. Une défaillance du contrôle d'un poste d'impression survenant alors que les grilles de protection sont ouvertes ne doit conduire ni au démarrage intempestif d'une machine arrêtée, ni au dépassement du régime de ralenti choisi.

Dans les usines et les entrepôts de grandes dimensions, des véhicules sans conducteur, robotisés et à guidage automatique, se déplacent sur des pistes spéciales. Ces pistes peuvent être traversées à tout moment par des personnes et il peut se produire qu'on y dépose du matériel par inadvertance, puisqu'elles ne sont pas séparées matériellement des autres voies de passage. Il faut donc prévoir un système assurant l'arrêt du véhicule pour prévenir toute collision dangereuse avec une personne ou un obstacle. Sur les systèmes les plus récents, cette prévention des collisions est assurée par des dispositifs à balayage ultrasonore ou laser associés à des pare-chocs de sécurité. Comme ces systèmes sont commandés par ordinateur, il est possible de configurer plusieurs zones de détection permanente, de manière que le véhicule puisse adapter sa réaction à la zone dans laquelle il détecte une personne. Les défaillances des dispositifs de protection ne doivent pas avoir pour effet de provoquer des collisions avec des personnes.

Les massicots sont des machines qui compriment, puis tranchent d'épaisses piles de papier. Ils sont contrôlés par des commandes bimanuelles. L'opérateur doit introduire les mains dans la zone dangereuse après chaque coupe. Une protection invisible, habituellement un barrage immatériel, est employée en association avec la commande bimanuelle et un système de sécurité intégré pour éviter les accidents corporels au moment de l'introduction du papier. La quasi-totalité des grands massicots modernes sont contrôlés par des micro-ordinateurs à redondance multiple. La sécurité de fonctionnement de la commande bimanuelle et du barrage immatériel doit également être garantie.

Les accidents liés à des installations commandées par ordinateur

Des accidents liés aux logiciels et aux ordinateurs sont signalés dans presque toutes les applications industrielles (Neumann, 1994). Dans la plupart des cas, les pannes d'ordinateur n'entraînent pas de lésions corporelles. De toute manière, ces incidents ne sont rendus publics que lorsqu'ils présentent un intérêt général. Les incidents ou les accidents en rapport avec des ordinateurs ou des logiciels et ayant entraîné des lésions corporelles représentent donc une proportion relativement élevée de tous les cas rendus publics. Malheureusement, lorsqu'il s'agit d'accidents moins spectaculaires, la recherche des causes ne fait pas l'objet d'investigations aussi poussées que dans le cas des accidents qui frappent l'opinion et qui surviennent en général dans de grandes installations. Dans les exemples qui suivent, on a choisi de décrire quatre cas représentatifs d'incidents ou d'accidents en rapport avec des systèmes de commande par ordinateur utilisés à d'autres fins que les protections sur des machines, afin de donner une idée des éléments à prendre en compte pour l'application des techniques de sécurité.

Les accidents causés par des défaillances aléatoires des matériels

L'incident suivant a eu pour origine une accumulation de défaillances aléatoires du matériel, associée à des erreurs de programmation. A la suite de la surchauffe d'un réacteur dans une usine chimique, les vannes de décharge ont été ouvertes et le contenu du réacteur a été évacué dans l'atmosphère. Cet incident s'est produit peu de temps après l'émission d'un signal indiquant un niveau d'huile trop bas dans un réducteur. Une enquête minutieuse révéla que peu de temps après l'amorçage de la réaction par le catalyseur — ce qui aurait nécessité un refroidissement supplémentaire au niveau du réacteur — l'ordinateur, sur la base du signal de faible niveau d'huile dans le réducteur, avait bloqué à une valeur fixe toutes les grandeurs placées sous son contrôle. Le débit d'eau froide a donc été maintenu à un niveau insuffisant et il en est résulté une surchauffe du réacteur. Des examens complémentaires ont révélé que l'indication de faible niveau d'huile avait été émise par un composant défectueux. Le logiciel avait réagi correctement, en déclenchant une alarme et en figeant toutes les variables de l'exploitation. Il s'agissait là d'une conséquence de l'étude de l'analyse des risques et de l'exploitabilité (Hazards and Operability Analysis (HAZOP)) (Knowlton, 1986) effectuée avant l'événement et qui exigeait que les variables contrôlées ne soient pas modifiées en cas de défaillance. Le programmeur n'ayant pas une connaissance détaillée de la procédure, cette exigence avait été interprétée comme signifiant que les dispositifs d'actionnement contrôlés (dans ce cas, des vannes) ne devaient pas être modifiés et l'on ne s'était pas préoccupé d'une éventuelle montée de la température. Le programmeur n'avait pas tenu compte du fait qu'après avoir reçu un signal erroné, le système pouvait se trouver dans une situation dynamique nécessitant l'intervention active de l'ordinateur pour éviter un accident. La situation ayant conduit à l'accident était de surcroît tellement improbable qu'elle n'avait pas été analysée en détail dans l'étude HAZOP (Levenson, 1986). Cet exemple fournit une transition vers une deuxième catégorie de causes d'accidents liés aux logiciels et aux ordinateurs. Il s'agit des défauts systématiques qui sont présents dans une installation dès le début, mais qui ne se manifestent que dans certaines situations très particulières que le programmeur n'a pas envisagées.

Les accidents causés par des erreurs de procédure

Au cours d'essais sur le terrain pour l'inspection finale de robots, un technicien avait emprunté la cassette d'un robot voisin et l'avait remplacée par une cassette différente sans en informer son collègue. De retour à son poste, le collègue avait introduit la mauvaise cassette. Comme il se tenait à côté du robot et qu'il s'attendait à une certaine séquence de mouvements, la séquence différente qui se produisit en raison de l'échange de programme provoqua une collision entre le robot et l'homme. Cet accident est un exemple type d'erreur de procédure. La part de ces erreurs dans les incidents et les accidents est actuellement en augmentation en raison de la complexité accrue des applications de mécanismes de sécurité commandés par ordinateur.

Les accidents causés par des défaillances systématiques du matériel ou des logiciels

Une torpille à tête explosive devait être tirée lors d'un exercice par un navire de guerre en haute mer. En raison d'un défaut de son système de propulsion, la torpille resta dans son tube de lance-

ment. Le commandant décida alors de revenir à son port d'attache pour récupérer l'engin. Peu de temps après le début du voyage de retour, la torpille explosa. L'analyse de l'accident révéla que les concepteurs de l'engin avaient dû intégrer à celui-ci un système l'empêchant de revenir à son point de lancement après le tir et de détruire ainsi le navire qui l'avait lancé. Le système adopté était le suivant: une fois la torpille lancée, on vérifiait, à l'aide du système de navigation inertielle, si sa course s'était infléchie de 180°. Si la torpille détectait qu'elle avait pivoté de 180°, elle explosait immédiatement, à une distance supposée sans danger pour le navire lanceur. C'est ce système de détection qui avait été activé sur la torpille qui n'avait pas été correctement lancée, ce qui explique l'explosion de celle-ci après que le navire eut modifié sa route de 180°. Il s'agit d'un exemple type d'accident occasionné par une lacune du cahier des charges. La condition énonçant qu'il devait être impossible à la torpille de détruire son propre navire si celui-ci modifiait sa route n'avait pas été formulée avec suffisamment de précision. La précaution avait donc été programmée de manière erronée, et l'erreur n'était apparue que dans une situation particulière, non envisagée par le programmeur.

Le 14 septembre 1993, un Airbus A 320 de la Lufthansa s'est écrasé à l'atterrissage à Varsovie (voir figure 58.60). Une enquête approfondie révéla que des modifications apportées à la logique d'atterrissage de l'ordinateur de bord à la suite de l'accident d'un Boeing 767 de la Lauda Air en 1991 étaient en partie responsables de ce nouvel accident. Lors de l'accident de 1991, l'inversion de poussée, qui dévie une partie des gaz des moteurs pour freiner l'avion à l'atterrissage, s'est déclenchée alors que l'appareil était encore en l'air, provoquant un piqué impossible à contrôler. Pour l'éviter, un verrouillage électronique de l'inversion de poussée avait été intégré aux Airbus. Avec ce système, l'inversion de poussée entrait en action uniquement à la réception d'un signal émis par des détecteurs installés sur les deux trains pour indiquer une compression des amortisseurs du fait du contact des roues avec le sol. Sur la base d'informations inexactes, les pilotes de l'avion de Varsovie s'attendaient à un fort vent latéral. Ils donnèrent donc une légère inclinaison à l'appareil, qui ne toucha le sol que par le seul train droit, laissant le côté gauche partiellement délesté. En raison du verrouillage de l'inversion de poussée, l'ordinateur de bord empêcha pendant neuf secondes le pilote d'exécuter les manœuvres qui auraient permis à l'avion d'atterrir en sécurité malgré des circonstances défavorables. Cet accident démontre très clairement que des modifications apportées aux systèmes informatiques peuvent conduire à de nouvelles situations dangereuses si la portée de leurs conséquences éventuelles n'est pas prévue.

L'exemple de l'incident suivant montre, lui aussi, les effets désastreux que peut avoir la modification d'une seule instruction sur un système informatique. On détermine la teneur en alcool du sang par des tests chimiques effectués sur un sérum sanguin clarifié, dont les globules ont été préalablement éliminés par centrifugation. La concentration d'alcool est par conséquent supérieure (d'un facteur de 1,2) à celle présente dans le sang entier, plus épais. Il convient donc de diviser par 1,2 les valeurs obtenues avec le sérum pour déterminer les valeurs en parties par millier à considérer sur les plans légal et médical. Lors d'un test interlaboratoires effectué en 1984, les concentrations d'alcool dans le sang relevées par différents instituts de recherche lors de tests identiques avec du sérum devaient être comparées entre elles. Comme il ne s'agissait que d'une comparaison, l'instruction de diviser par 1,2 fut supprimée du programme dans l'un des instituts pendant la durée de l'expérience. Après l'achèvement du test interlaboratoires, une instruction de multiplication par 1,2 fut introduite par erreur à cette étape du programme. Environ 1 500 valeurs erronées furent ainsi calculées entre août 1984 et mars 1985. Cette erreur eut des conséquences pour la carrière professionnelle de conducteurs de camions dont l'alcoolémie se situait entre 1 et 1,3%, étant donné qu'une valeur de 1,3% est sanctionnée, sur le plan légal, par un retrait de longue durée du permis de conduire.

Figure 58.60 • L'Airbus de la Lufthansa après sa chute à Varsovie en 1993

Les accidents dus aux contraintes liées au travail ou à l'environnement

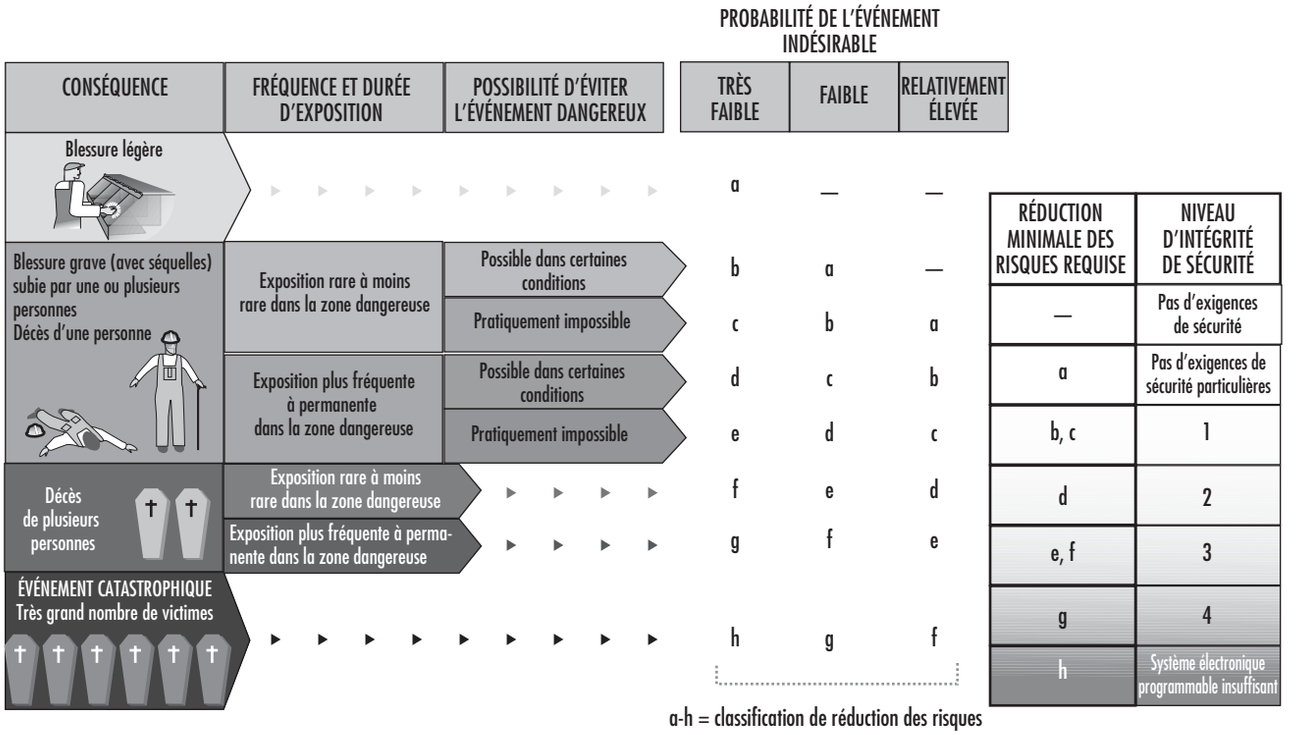
Suite à une perturbation dans la collecte des déchets dans la zone d'action d'une poinçonneuse-grignoteuse à commande numérique, l'opérateur actionna «l'arrêt programmé». Alors qu'il tentait de retirer les déchets avec ses mains, le vérin de la machine se mit en mouvement malgré l'arrêt programmé et l'opérateur fut grièvement blessé. L'analyse de l'accident montra qu'il ne s'agissait pas d'une erreur du programme. Il s'avéra impossible de reproduire le démarrage intempestif. De semblables anomalies ayant déjà été constatées auparavant sur d'autres machines du même type, il paraît plausible d'expliquer cet accident par des interférences électromagnétiques. Des accidents de même nature avec des robots industriels ont été rapportés au Japon (Neumann, 1995).

Un incident sur la sonde spatiale Voyager 2, survenu le 18 janvier 1986, met encore davantage en évidence l'influence des contraintes de l'environnement sur les systèmes contrôlés par ordinateur. Six jours avant de parvenir au point de son parcours le plus proche d'Uranus, la sonde avait transmis des images recouvertes de grandes lignes noires et blanches. Une analyse précise montra qu'un unique bit d'un mot d'instruction du sous-système de données de vol était à l'origine de la panne, observée lors de la compression des images dans la sonde. Le bit en question avait vraisemblablement été décalé dans la mémoire par l'impact d'une particule cosmique. La transmission sans erreur des photographies compressées ne put reprendre que deux jours plus tard, grâce à un programme de secours capable d'ignorer l'élément de mémoire défectueux (Laeser, McLaughlin et Wolff, 1987).

Résumé des accidents présentés

Les accidents analysés montrent que certains risques qui pourraient être négligés lorsqu'on utilise des techniques électromécaniques simples prennent de l'importance en cas de recours à l'informatique. Les ordinateurs permettent de gérer des fonctions de sécurité complexes et propres à des situations déterminées et il est donc particulièrement important que toutes ces fonctions soient définies sans ambiguïté, sans erreur et de manière complète et vérifiable. Les erreurs de spécification sont difficiles à découvrir et, dans les systèmes complexes, elles sont fréquemment à l'origine d'accidents. Des commandes programmables sont habituellement

Figure 58.61 • Méthode qualitative de détermination des risques



introduites afin de permettre une adaptation souple et rapide à l'évolution des marchés commerciaux. Mais les modifications, notamment dans le cas de systèmes complexes, ont des effets secondaires difficiles à prévoir. Toutes les modifications doivent donc être soumises à une procédure de gestion des changements rigoureusement formalisée, avec une séparation nette entre les fonctions de sécurité et les sous-systèmes ne relevant pas de ce domaine pour faciliter le contrôle des conséquences des modifications pour la technologie de la sécurité.

Les ordinateurs fonctionnent avec de faibles niveaux électriques et sont par conséquent sensibles aux interférences provenant de sources de rayonnement extérieures. Etant donné que la modification d'un seul signal sur plusieurs millions peut entraîner un défaut de fonctionnement, la question de la compatibilité électromagnétique en relation avec les ordinateurs mérite une attention particulière.

La maintenance des systèmes contrôlés par ordinateur devient toujours plus complexe et donc plus difficile à appréhender. L'ergonomie des logiciels d'interface utilisateur et de configuration prend donc une importance accrue pour la technologie de la sécurité.

Aucun système informatique ne peut être testé à 100%. La vérification complète d'un mécanisme de contrôle simple à 32 ports d'entrées binaires et 1 000 options de branchement différentes nécessite $4{,}3 \times 10^{12}$ tests. A raison de 100 tests exécutés et évalués par seconde, une vérification complète demanderait plus de 1 300 ans (à raison de 365 jours par an et 24 heures par jour).

Les procédures et les mesures pour l'amélioration des dispositifs de sécurité contrôlés par ordinateur

Au cours des dix dernières années, des procédures ont été mises au point qui ont permis de maîtriser certaines difficultés liées à l'utilisation de l'informatique à des fins de sécurité. Ces procédures visent les défaillances informatiques décrites dans la présente partie. Les descriptions d'utilisations de logiciels et d'ordinateurs pour la protection des machines et les analyses des accidents montrent que l'étendue des dommages et les risques associés à différentes applications sont extrêmement variables. Il apparaît clairement que les précautions à prendre pour améliorer les matériels et les logiciels utilisés dans les technologies de sécurité devraient être définies en fonction du risque.

La figure 58.61 décrit une méthode qualitative pour déterminer la réduction du risque qu'il est nécessaire d'obtenir grâce à l'utilisation de systèmes de sécurité, en fonction de l'importance et de la fréquence des dommages (Bell et Reinert, 1992). Les types de défaillances informatiques analysés sous le titre ci-dessus, «Les accidents liés à des installations commandées par ordinateur», peuvent être rapprochés de ce que l'on appelle les niveaux d'intégrité de la sécurité — c'est-à-dire les dispositifs techniques de réduction des risques.

La figure 58.62 indique clairement qu'il est nécessaire que l'efficacité des mesures prises dans un cas donné pour réduire les erreurs dans les logiciels et les matériels augmente avec le risque (DIN, 1994; CEI, 1998).

L'analyse des accidents décrits plus haut montre que la défaillance des protections contrôlées par ordinateur n'est pas seulement provoquée par des défauts aléatoires de certains éléments, mais également par des conditions de fonctionnement particulières que le programmeur a négligé de prendre en compte. Les conséquences, qui ne sont pas immédiatement perceptibles, des modifications apportées aux programmes au cours de la maintenance du système constituent une nouvelle source d'erreurs. Il peut exister, dans les systèmes de sécurité contrôlés par microprocesseurs, des défauts qui, bien qu'introduits lors du développement du système, ne donnent lieu à des situations dangereuses qu'en cours de fonctionnement. Les mesures de précaution contre

LES APPLICATIONS DE LA SÉCURITÉ

58

Rédacteurs
Kenneth Gerecke
et Charles T. Pope

Table des matières

L'ANALYSE DES SYSTÈMES

Manh Trung Ho

Un *système* peut être défini comme un ensemble de composants interdépendants combinés de manière à assurer une fonction donnée dans des conditions spécifiques. Une machine est un exemple tangible et particulièrement concret de système répondant à cette définition, mais il existe d'autres types de systèmes, impliquant des hommes et des femmes au sein d'une équipe, d'un atelier ou d'une usine, qui sont nettement plus complexes et moins faciles à définir. La notion de *sûreté* suggère l'absence de danger ou de risques d'accidents ou de lésions. Pour lever toute ambiguïté, on emploiera l'expression *événement indésirable* qui a une acception plus générale. La sûreté absolue, au sens de l'impossibilité que survienne un incident plus ou moins malheureux, relève de l'utopie. Si l'on veut rester réaliste, on doit rechercher une probabilité, non pas nulle mais très faible, d'événements indésirables.

Un système donné ne peut être considéré comme sûr ou non que par rapport aux résultats qu'on en attend. Dans ces conditions, le niveau de sûreté d'un système peut être défini ainsi: «Pour un ensemble donné d'événements indésirables, le niveau de sûreté (ou d'absence de sûreté) d'un système est déterminé par la probabilité que ces événements se produisent sur une période de temps donnée.» Les exemples suivants peuvent être retenus en tant qu'événements indésirables dans le cadre de cet exposé: décès d'une ou de plusieurs personnes, blessures graves, blessures légères, dommages à l'environnement, effets nocifs sur des êtres vivants, destruction d'installations ou de bâtiments, dégâts de grande ampleur ou limités à des matériels ou à des équipements.

But de l'analyse de sûreté des systèmes

L'analyse de sûreté des systèmes a pour objet de déterminer les facteurs ayant une incidence sur la probabilité des événements indésirables, d'étudier comment ces événements peuvent se produire et, en dernier lieu, d'élaborer des mesures de prévention de nature à en réduire la probabilité.

La phase analytique du problème peut être subdivisée en deux aspects principaux:

1. Identification et description des types de dysfonctionnements ou d'inadaptations.
2. Identification des séquences de dysfonctionnements se combinant entre eux (ou avec des événements plus «normaux») pour aboutir finalement à l'événement indésirable lui-même, et évaluation de leur probabilité.

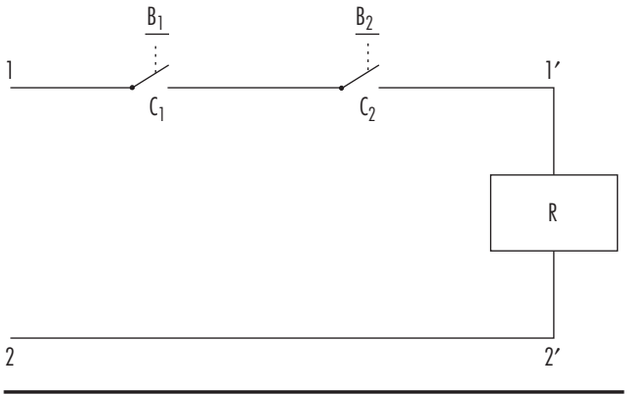
Une fois étudiés les différents dysfonctionnements et leurs conséquences, les analystes de la sûreté des systèmes peuvent tourner leur attention vers les mesures préventives. La recherche dans ce domaine repose alors directement sur les conclusions précédentes. Cette investigation des moyens de prévention suit les deux grands aspects de l'analyse de la sûreté des systèmes.

Les méthodes d'analyse

La sûreté des systèmes peut être analysée avant ou après l'événement (a priori ou a posteriori). Dans les deux cas, la méthode employée peut être soit prospective, soit rétrospective. L'analyse a priori a lieu avant l'événement indésirable. L'analyste choisit un certain nombre d'événements et entreprend de rechercher les différentes étapes susceptibles d'y conduire. Au contraire, l'analyse a posteriori intervient après l'événement indésirable. Son but est de fournir des orientations pour l'avenir et, en particulier, de tirer les conclusions qui pourraient être utiles pour des analyses a priori ultérieures.

Bien que l'on puisse penser qu'une analyse a priori soit bien plus utile qu'une analyse a posteriori, dans la mesure où elle précède l'incident, toutes deux sont en fait complémentaires. Le choix de la méthode dépend de la complexité du système en cause et de ce que l'on connaît déjà à son sujet. Dans le cas de systèmes concrets comme des machines ou des installations industrielles, on a pour habitude de se fonder sur l'expérience antérieure pour la préparation d'une analyse a priori détaillée. Toutefois, même dans ce cas, l'analyse n'est pas nécessairement infaillible et elle tirera sans aucun doute avantage d'une analyse a posteriori ultérieure fondée essentiellement sur une étude des incidents survenus en cours d'exploitation. Pour les systèmes plus complexes impliquant des personnes, comme les équipes de travail, les ateliers ou les usines, une analyse a posteriori prend encore plus d'importance. En pareils cas, l'expérience antérieure ne suffit pas toujours pour une analyse a priori détaillée et fiable.

Figure 58.1 • Circuit de commande bimanuelle



Une analyse a posteriori peut évoluer en une analyse a priori lorsque l'analyste va au-delà du processus unique ayant conduit à l'incident et commence à s'intéresser aux différentes circonstances pouvant logiquement conduire à cet incident ou à d'autres de même nature.

Une analyse a posteriori peut également se transformer en analyse a priori lorsqu'on met l'accent non pas sur l'événement (dont la prévention est le principal but de l'analyse en cours), mais sur des incidents moins graves. Ces incidents, par exemple des problèmes techniques, des dégâts aux matériels ou des accidents potentiels ou mineurs, de faible importance en eux-mêmes, peuvent être les signes avant-coureurs d'événements plus graves. Bien qu'effectuée après les incidents mineurs, l'analyse devient alors une analyse a priori en ce qui concerne des événements plus graves qui n'ont pas encore eu lieu.

Il existe deux méthodes possibles pour étudier le mécanisme ou la logique d'une séquence de deux événements ou plus:

1. La méthode prospective, ou inductive, qui commence par les causes en vue d'en prédire les effets.
2. La méthode rétrospective, ou déductive, qui observe les effets et remonte aux causes.

La figure 58.1 est le schéma d'un circuit de commande qui impose d'appuyer simultanément sur deux boutons (B_1 et B_2) pour activer le bobinage du relais (R) et mettre en route la machine. Cet exemple peut servir à illustrer de façon concrète les méthodes prospective et rétrospective employées dans l'analyse de la sûreté des systèmes.

La méthode prospective

Dans la méthode prospective, l'analyste commence par: 1) dresser une liste des défauts, des dysfonctionnements et des inadaptations; 2) étudier leurs effets; 3) déterminer si ces effets présentent ou non

Tableau 58.1 • Dysfonctionnements possibles d'un circuit de commande bimanuelle et conséquences

Défauts	Conséquences
Rupture du fil entre 2 et 2′	Impossibilité de mettre en marche la machine*
Fermeture accidentelle de B_1 (ou B_2)	Pas de conséquence immédiate
Contact involontaire en C_1 (ou C_2) suite à une obstruction mécanique	Pas de conséquence immédiate, mais risque d'une possibilité de démarrage de la machine par simple pression sur le bouton B_2 (ou B_1)**
Court-circuit entre 1 et 1′	Activation de la bobine du relais R — démarrage accidentel de la machine***

* Incident influençant directement la fiabilité du système. ** Incident provoquant une grave diminution du niveau de sécurité du système. *** Incident dangereux, à éviter.
Voir texte et figure 58.1.

une menace pour la sécurité. Dans le cas de la figure 58.1, les défauts possibles sont les suivants:

- rupture du fil entre 2 et 2′ ;
- fermeture accidentelle de B_1 (ou B_2);
- contact involontaire en C_1 (ou C_2) suite à une obstruction mécanique;
- court-circuit entre 1 et 1′ .

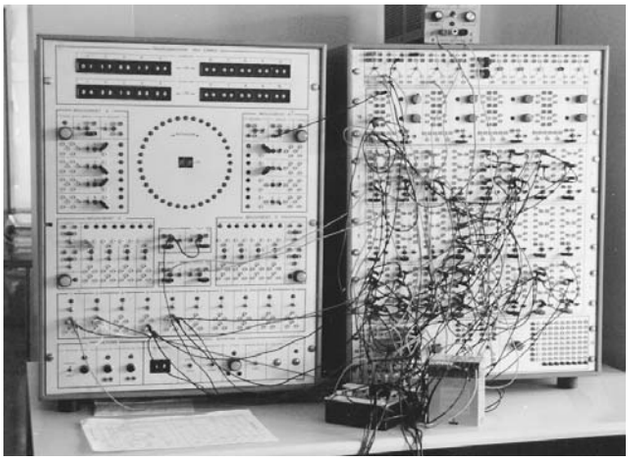
L'analyste peut alors déduire les conséquences de ces défauts et exposer ses conclusions sous forme de tableau (voir tableau 58.1).

Dans le tableau 58.1, les conséquences dangereuses ou susceptibles de diminuer sensiblement le niveau de sûreté du système peuvent être désignées par des signes conventionnels comme ***.

Note: Dans le tableau 58.1, une rupture du fil entre 2 et 2′ (voir figure 58.1) donne lieu à une situation qui n'est pas considérée comme dangereuse. Elle n'a pas d'effet direct sur la sûreté du système; en revanche, sa fiabilité est directement affectée par la probabilité de ce genre d'incident.

La méthode prospective convient particulièrement à la simulation. La figure 58.2 représente un simulateur analogique destiné à étudier la sûreté des circuits commandés par pression. La simulation de ce circuit de commande permet de vérifier que, en l'absence de défaut, le circuit est effectivement capable d'assurer la fonction voulue sans enfreindre les critères de sécurité. De plus, le simulateur donne à l'analyste la possibilité d'introduire des défauts dans les différents composants du circuit, d'observer leurs conséquences et de distinguer ainsi les circuits correctement conçus (faible nombre ou absence de défauts dangereux) des circuits mal conçus. Ce type d'analyse peut être effectué sur ordinateur.

Figure 58.2 • Simulateur pour l'étude des circuits de commande de presses



La méthode rétrospective

Dans la méthode rétrospective, l'analyste part de l'événement indésirable, incident ou accident, et remonte aux événements précédents pour déterminer ceux qui sont susceptibles d'aboutir aux événements à éviter. Dans la figure 58.1, l'événement à éviter en dernière instance serait la mise en marche involontaire de la machine.

- La mise en marche de la machine peut être provoquée par une activation incontrôlée du bobinage du relais (R).
- Cette activation peut elle-même être provoquée par un court-circuit entre 1 et 1′, ou par la fermeture involontaire et simultanée des contacts C_1 et C_2.
- La fermeture involontaire de C_1 peut être la conséquence d'un blocage mécanique de C_1 ou d'une pression accidentelle sur B_1. Le même raisonnement s'applique à C_2.

Il est possible de représenter les conclusions de cette analyse sur un diagramme arborescent (raison pour laquelle la méthode rétrospective est appelée «analyse par arbre des causes»), comme celui figurant à la figure 58.3.

Ce diagramme emploie des opérateurs logiques, dont les plus importants sont «OU» et «ET». L'opérateur «OU» signifie que [X_1] se produira si soit [A], soit [B] (ou les deux) se produisent. L'opérateur «ET» signifie que pour que [X_2] se produise, il faut à la fois que [C] et [D] se soient produits (voir figure 58.4).

La méthode rétrospective est souvent employée dans l'analyse a priori des systèmes concrets, notamment dans les industries chimique, aéronautique, spatiale et nucléaire. Elle s'est également avérée extrêmement utile dans les enquêtes sur les accidents industriels.

Bien que très différentes, les méthodes prospective et rétrospective sont complémentaires. La méthode prospective est fondée sur un ensemble de défauts ou de dysfonctionnements; la valeur d'une telle analyse dépend donc largement de la pertinence des dysfonctionnements pris en compte au départ. Sous cet éclairage, la méthode rétrospective paraît plus systématique. Si l'analyste connaît les types d'accidents ou d'incidents qui peuvent se produire, il peut théoriquement appliquer cette méthode pour remonter à l'ensemble des dysfonctionnements ou combinaisons de dysfonctionnements susceptibles d'y conduire. Toutefois, du fait que les comportements dangereux d'un système ne sont pas forcément connus d'avance, la méthode prospective permet de les découvrir, au moyen d'une simulation par exemple. Une fois ces comportements identifiés, la méthode rétrospective permet d'en analyser les dangers de façon plus détaillée.

Les problèmes de l'analyse de la sûreté des systèmes

Les méthodes analytiques que l'on vient de décrire ne sont pas de simples processus mécaniques qu'il suffit d'appliquer de façon automatique pour parvenir à des conclusions utiles à l'amélioration de la sûreté d'un système. Les analystes rencontrent au contraire un certain nombre de problèmes au cours de leur travail, et l'utilité de leurs analyses dépend pour une grande part de la manière dont ils s'y prennent pour les résoudre. Nous exposons ci-après certains des problèmes classiques qui peuvent se présenter.

Figure 58.3 • Séquence d'événements possible

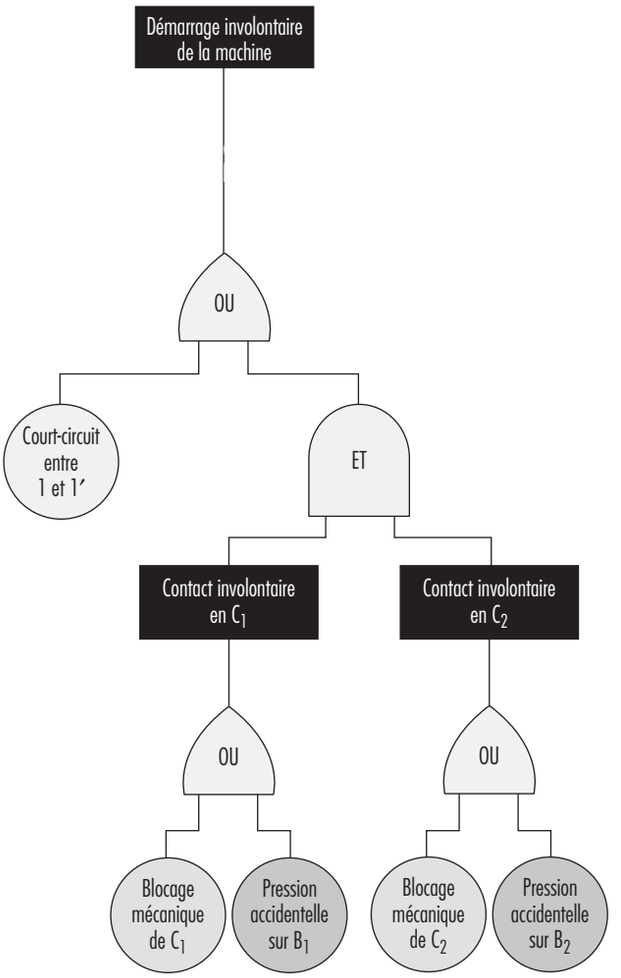
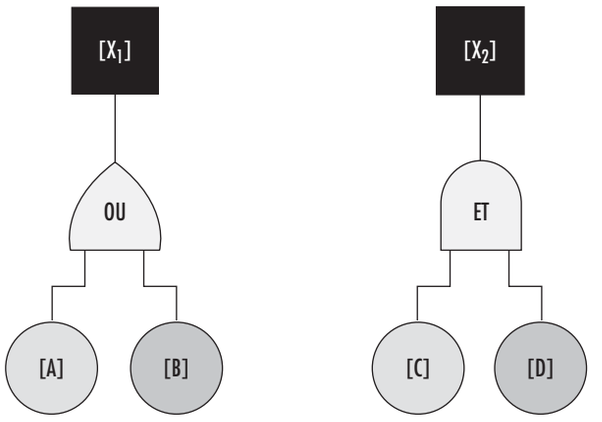


Figure 58.4 • Représentation de deux opérations logiques



La compréhension du système à étudier et de ses conditions de fonctionnement

Les problèmes fondamentaux de toute analyse de la sûreté des systèmes sont la définition du système à étudier, de ses limites et des conditions dans lesquelles il est censé devoir fonctionner tout au long de son existence.

Si l'analyste prend en compte un sous-système trop restreint, cela peut conduire à adopter une série de mesures préventives aléatoires (situation dans laquelle tout est organisé de façon à éviter certains types d'événements, alors que d'autres dangers non moins graves sont ignorés ou sous-estimés). Si, au contraire, le système pris en compte est trop étendu ou trop général par rapport à un problème donné, on arrive à un flou excessif du concept et des responsabilités, qui ne permet pas d'adopter les mesures préventives nécessaires.

Un exemple type du problème de la définition du système à étudier est celui de la sûreté des machines ou des installations industrielles. Dans ce genre de situation, l'analyste peut être tenté de ne tenir compte que de l'équipement lui-même, en négligeant le fait qu'il va être utilisé ou commandé par une ou plusieurs personnes. Ce type de simplification suffit parfois. Cependant, ce qu'il convient d'analyser, ce n'est pas le seul sous-système correspondant à la machine, mais le système complet travailleur plus machine aux différentes étapes de la durée de vie du matériel (y compris, par exemple, transport et manutention, montage, essais et réglages, utilisation normale, maintenance, démontage et, dans certains cas, destruction). A chaque étape, la machine fait partie d'un système spécifique, dont le but et les modes de fonctionnement ou de dysfonctionnement sont totalement différents de ceux du système dans les autres étapes. Elle doit par conséquent être conçue et fabriquée de manière à permettre d'assurer la fonction prévue dans de bonnes conditions de sécurité à chacune de ces étapes.

Plus généralement, en ce qui concerne les études de sûreté dans les entreprises, il existe plusieurs niveaux de systèmes: la machine, le poste de travail, l'équipe, le service, l'usine et l'entreprise dans son ensemble. Selon le niveau considéré, les types de dysfonctionnements possibles et les mesures préventives correspondantes sont très différents. Une bonne politique de prévention doit prendre en compte les dysfonctionnements pouvant survenir aux divers niveaux.

Les conditions de fonctionnement du système peuvent être définies selon les modalités de fonctionnement attendues du système et l'environnement auquel il pourra être exposé. Cette définition devrait être suffisamment réaliste pour tenir compte des conditions effectives probables de fonctionnement. Un système qui ne serait très sûr que dans une plage de fonctionnement extrêmement limitée pourra devenir moins sûr si l'utilisateur n'est pas en mesure de le maintenir dans la plage théorique prescrite. Un système vraiment sûr devrait donc être suffisamment robuste pour supporter des variations raisonnables de ses conditions de fonctionnement et il devrait tolérer certaines erreurs simples, mais prévisibles, de la part des opérateurs.

La modélisation du système

Il est souvent nécessaire d'élaborer un modèle pour analyser la sûreté d'un système. Ce travail peut soulever certains problèmes qui méritent d'être examinés.

Pour un système restreint et relativement simple comme une machine classique, le modèle peut presque être construit directement à partir de la description des éléments matériels et de leur fonction (moteurs, transmissions, etc.) et de la manière dont ils sont liés entre eux. Le nombre des modes de défaillance possibles des éléments est, de même, limité.

Les machines modernes, comme les ordinateurs ou les robots, qui contiennent des composants complexes tels que microprocesseurs et circuits électroniques à très forte intégration, posent un problème particulier. Ce problème n'a pas été complètement

résolu du point de vue de la modélisation ou de la prédiction des différents modes de défaillance possibles, en raison du nombre très élevé de transistors par puce et de la diversité des logiciels.

Lorsque le système à analyser est une organisation humaine, un problème intéressant de la modélisation est celui du choix et de la définition de certains éléments immatériels ou non complètement matériels. On peut, par exemple, représenter un poste de travail particulier par un système comprenant des travailleurs, des logiciels, des tâches, des machines, des matériaux et un environnement (l'élément «tâche» peut s'avérer difficile à définir, car ce qui compte au fond n'est pas la tâche prescrite, mais la tâche telle qu'elle est réellement exécutée).

Lorsqu'il modélise les organisations humaines, l'analyste peut choisir de subdiviser le système considéré en un sous-système d'information et en un ou plusieurs sous-systèmes d'action. L'analyse des défaillances aux différentes étapes du sous-système d'information (acquisition, transfert, traitement et utilisation des informations) peut se révéler très instructive.

Les problèmes associés aux niveaux d'analyse multiples

Des problèmes associés aux niveaux d'analyse multiples apparaissent souvent parce que l'analyste, partant d'un événement indésirable, peut remonter à des incidents toujours plus éloignés dans le temps. Selon le niveau d'analyse considéré, la nature des dysfonctionnements qui surviennent varie, ce qui est également vrai pour les mesures préventives. Il importe de pouvoir décider du niveau auquel arrêter l'analyse et du niveau auquel prendre les mesures préventives. Considérons l'exemple d'un cas simple d'accident résultant d'une défaillance mécanique provoquée par l'utilisation répétée d'une machine dans des conditions anormales. Il peut s'agir d'un manque de formation de l'opérateur ou d'une mauvaise organisation du travail. Selon le niveau d'analyse considéré, l'action préventive requise consistera à remplacer la machine par un autre modèle capable de supporter des conditions d'utilisation plus sévères, à n'utiliser la machine que dans des conditions normales, à modifier la formation des opérateurs, ou à réorganiser le travail.

L'efficacité et la portée d'une mesure préventive dépendent du niveau auquel elle est introduite. Une action préventive à proximité immédiate de l'événement indésirable est plus susceptible d'avoir une incidence directe et rapide, mais ses effets peuvent être limités. En remontant raisonnablement dans l'analyse des événements, il devrait être possible, en revanche, de trouver des types de dysfonctionnement communs à de nombreux accidents. Une mesure préventive prise à ce niveau aura une portée nettement plus étendue, mais son efficacité sera peut-être moins directe.

Compte tenu qu'il existe plusieurs niveaux d'analyse, il peut également y avoir de nombreuses formes d'action préventive, dont chacune apporte sa propre contribution au travail de prévention. Il s'agit là d'un point extrêmement important et il suffit de se référer à l'accident qui vient d'être décrit pour en prendre conscience. Si l'on propose de remplacer la machine par un autre modèle capable de supporter des conditions d'utilisation plus sévères, on met l'accent, en matière de prévention, sur la machine. Si l'on décide que la machine ne doit être utilisée que dans des conditions normales, cela signifie que l'accent est mis sur l'opérateur. De même, l'accent peut être mis sur la formation du personnel, l'organisation du travail, ou simultanément sur la machine, l'utilisateur, la fonction de formation et la fonction d'organisation.

Pour un niveau d'analyse donné, un accident apparaît souvent comme la conséquence d'une combinaison de plusieurs dysfonctionnements ou inadaptations. Selon que l'on agira sur un dysfonctionnement ou un autre, ou sur plusieurs simultanément, les modalités de la mesure préventive adoptée seront différentes.

LA SÉCURITÉ DANS L'UTILISATION DES OUTILS À MAIN ET DES OUTILS À MOTEUR PORTATIFS

US Department of Labor — Occupational Safety and Health Administration;
édité par Kenneth Gerecke

Les outils font tellement partie de notre vie quotidienne que nous avons parfois tendance à oublier qu'ils peuvent présenter des risques. Tous sont fabriqués selon les règles de sécurité, mais il peut arriver qu'un accident se produise avant que les risques d'un outil aient été reconnus. Les travailleurs doivent apprendre à reconnaître les risques que présentent les différents types d'outils et à respecter certaines précautions pour les éviter. Le port d'équipements de protection individuelle appropriés, lunettes et gants par exemple, est recommandé pour se protéger contre les risques potentiels de l'utilisation d'outils à moteur portatifs et d'outils à main.

Les outils à main

On appelle outils à main les outils non actionnés par un moteur; ils comprennent un large éventail de matériels, de la hache à la clé de mécanicien. Les risques les plus importants que présentent ces outils sont liés à une utilisation impropre, au choix d'un outil ne convenant pas à la tâche ou à un entretien défectueux. Voici une liste non limitative des risques associés à l'utilisation d'outils à main:

- Le fait d'utiliser un tournevis en guise de burin peut provoquer la rupture et la projection de l'extrémité de sa tige et blesser l'utilisateur ou d'autres personnes.
- Si le manche en bois d'un outil, marteau ou hache par exemple, présente du jeu, des éclats ou des fissures, la tête de l'outil peut être projetée et frapper l'utilisateur ou une autre personne.
- Une clé dont les mâchoires sont évasées peut échapper.
- Les outils de choc comme les burins, les coins ou les chasse-goupilles sont dangereux lorsqu'ils ont des têtes émoussées qui risquent de se briser sous le choc et de projeter des fragments coupants.

L'employeur est responsable de la sécurité des outils et matériels fournis à ses employés, mais il appartient à ceux-ci de les utiliser et de les entretenir correctement. Les lames de scie, les couteaux et autres outils tranchants ne devraient pas être dirigés vers les zones de passage ou les autres travailleurs se trouvant à proximité. Le tranchant des couteaux et ciseaux devrait être entretenu, certains outils émoussés pouvant devenir plus dangereux que lorsqu'ils sont aiguisés (voir figure 58.5).

La sécurité exige que les sols soient aussi propres et aussi secs que possible pour éviter les glissades accidentelles lorsqu'on se sert d'un outil à main dangereux ou qu'on se trouve à proximité d'une personne qui en utilise. Bien que les étincelles produites par les outils à main en fer ou en acier n'aient pas, en principe, une température suffisante pour constituer des sources d'inflammation, il est recommandé, lorsqu'on travaille avec des matériaux inflammables ou à proximité de ceux-ci, d'employer des outils antiétincelants en bronze, en plastique, en aluminium ou en bois.

Figure 58.5 • Tournevis

Les outils à moteur

Les outils à moteur sont dangereux en cas de mauvaise utilisation. Il existe plusieurs types d'outils à moteur, que l'on classe habituellement selon leur source d'énergie (électriques, pneumatiques, à carburant liquide, hydrauliques, à vapeur ou à poudre explosive). Les travailleurs devraient posséder la qualification ou la formation requises pour l'utilisation de chacun des outils à moteur nécessaires à leur travail. Ils devraient connaître les risques potentiels associés à l'utilisation de ces outils et observer les précautions générales ci-après pour s'en préserver:

- Ne jamais transporter un outil par son cordon ou son flexible.
- Ne jamais tirer sur le cordon ou le flexible pour débrancher l'outil de sa prise.
- Tenir les cordons et les flexibles à l'écart des sources de chaleur, de l'huile et des arêtes vives.
- Débrancher les outils lorsqu'on ne les utilise pas, pour procéder à leur entretien et pour remplacer des accessoires tels que lames, pointes et disques.
- Les spectateurs devraient rester à bonne distance de la zone de travail.
- Maintenir les pièces à l'aide de serre-joints ou d'un étau de manière à libérer les deux mains pour l'utilisation de l'outil.
- Eviter les mises en route accidentelles. Ne pas laisser les doigts sur l'interrupteur lors du transport d'un outil raccordé. Si l'outil est doté d'un dispositif de verrouillage en marche, celui-ci doit être débloqué lorsque l'alimentation est coupée, de manière que l'outil ne démarre pas automatiquement au moment où l'alimentation est rétablie.
- Les outils devraient être entretenus, aiguisés et nettoyés avec soin pour assurer un fonctionnement optimal. Les opérations de lubrification et de changement d'accessoires devraient être effectuées conformément aux instructions du fabricant.
- Les travailleurs devraient adopter une bonne position et un bon équilibre lors de l'utilisation d'outils motorisés. Ils devraient porter une tenue adaptée à leur travail en gardant toujours à l'esprit que les vêtements amples, les cravates et les bijoux peuvent se prendre dans des organes mobiles.
- Tous les outils électriques endommagés devraient être retirés du service et repérés par une étiquette indiquant «Ne pas utiliser» pour éviter les électrocutions.

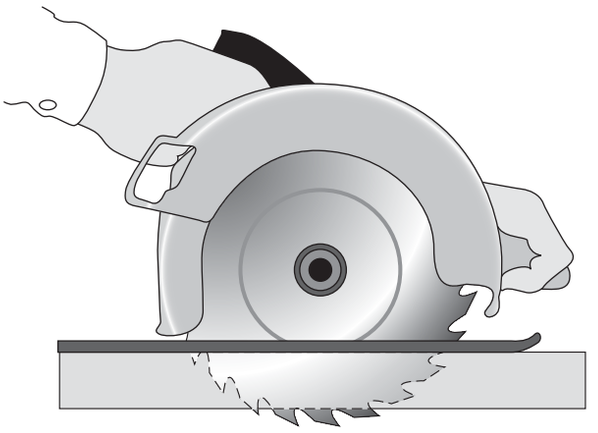
Les protecteurs

Les parties dangereuses en mouvement devraient être munies de protecteurs. Les parties mécaniques comme les courroies, engrenages, arbres, poulies, roues dentées, axes, tambours, volants, chaînes ou autres pièces à mouvement alternatif, rotatif ou autre devraient être protégées lorsque les travailleurs risquent d'être exposés à leur contact. On devra, si nécessaire, disposer des protecteurs pour éviter que les opérateurs et les autres personnes ne soient exposés aux risques liés:

- à la zone d'opération;
- aux points d'entraînement par pincement;
- aux pièces à mouvement rotatif ou alternatif;
- aux projections de copeaux ou d'étincelles, ainsi qu'aux vapeurs et aux gouttelettes de fluides de coupe.

Les protecteurs ne devraient jamais être enlevés pendant l'utilisation de l'outil. Les scies circulaires portatives, par exemple, devraient être équipées d'une cape recouvrant la partie non travaillante de la lame. Un protecteur inférieur rétractable devrait recouvrir les dents de la lame à l'exception de la zone au contact du matériau. Ce protecteur devrait revenir automatiquement en position de sécurité lorsque l'outil est retiré. La figure 58.6 montre une scie électrique avec sa cape de protection.

Figure 58.6 • Scie circulaire avec cape de protection



Les interrupteurs et les commandes de sécurité

Les équipements ci-après sont des exemples d'outils motorisés à main qui devraient être équipés d'un interrupteur à arrêt par relâchement:

- perceuses (voir figure 58.7), taraudeuses et outils de scellement;
- meuleuses horizontales, verticales ou d'angle, à meules de plus de 5 cm de diamètre;
- ponceuses à disque ou à bande;
- scies sauteuses et scies sabres.

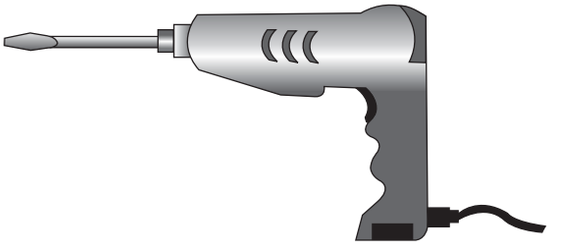
Ces outils peuvent également être équipés de commandes verrouillables, à condition de pouvoir être arrêtés par un simple mouvement du ou des doigts avec lesquels on les met en marche. Les outils portatifs à moteur ci-après peuvent être équipés uniquement d'un interrupteur marche-arrêt commandé:

- ponceuses vibrantes;
- ponceuses à disque d'un diamètre de disque ne dépassant pas 5 cm;
- meuleuses d'un diamètre de disque ne dépassant pas 5 cm;
- défonceuses et rabots;
- trancheuses, grignoteuses et cisailles à stratifiés;
- scies à chantourner et scies sauteuses dont la lame mesure moins de 6,4 mm de large.

Les outils portatifs à moteur pour lesquels un interrupteur à arrêt par relâchement est indispensable comprennent également:

- les scies circulaires d'un diamètre de lame supérieur à 5,1 cm;
- les tronçonneuses à chaîne;
- les outils à percussion sans système de blocage des accessoires.

Figure 58.7 • Perceuse électrique



Les outils électriques

Les travailleurs appelés à se servir d'outils électriques devraient être conscients de plusieurs risques. Le plus grave est le risque d'électrocution, suivi de risques de brûlures et de commotions électriques. Dans certaines conditions, même un courant limité peut être à l'origine d'une fibrillation cardiaque susceptible d'entraîner la mort. Un choc électrique peut également provoquer une chute du haut d'une échelle ou d'un poste de travail en hauteur.

Pour limiter les risques de blessures à la suite de chocs électriques, les outils devraient être protégés par l'un au moins des dispositifs ci-après:

- *Mise à la terre* par câble à trois conducteurs (dont un de terre). Les câbles à trois fils comprennent deux fils sous tension et un de mise à la terre. Une extrémité du fil de terre est reliée à l'enveloppe métallique de l'outil, et l'autre à la terre, par l'intermédiaire de la broche mâle de la prise. Chaque fois qu'un adaptateur est utilisé pour brancher l'outil sur une prise à deux fils, le fil de l'adaptateur doit être relié à une terre sûre. La broche mâle ne doit jamais être enlevée.
- *Double isolation*. Le travailleur et l'outil sont protégés de deux manières: 1) par l'isolation normale des fils; 2) par un boîtier faisant obstacle au passage du courant électrique jusqu'à l'opérateur en cas de fonctionnement défectueux.
- *Alimentation par transformateur basse tension.*
- *Branchement par l'intermédiaire de disjoncteurs de défaut à la terre*. Ces appareils, fixes ou portatifs, coupent instantanément le circuit lorsque le courant cherche un passage à la terre à travers le corps du travailleur ou les objets reliés à la terre.

Lorsqu'on utilise des outils électriques, il conviendrait d'appliquer les pratiques de sécurité générales ci-après:

- Respecter les limites d'utilisation préconisées.
- Le port de gants et de chaussures de sécurité est recommandé.
- Les outils non utilisés devraient être conservés dans un endroit sec.
- Les outils ne devraient pas être employés si des fils ou des connecteurs sont effilochés, pliés ou endommagés.
- Les outils électriques ne devraient pas être utilisés dans les lieux humides.
- Les zones de travail devraient être bien éclairées.

Les meuleuses

Les meules et disques abrasifs montés sur les outils de meulage, de coupe, de polissage et de brossage posent des problèmes de sécurité particuliers en raison des risques de rupture et de projection de fragments.

Avant montage, les disques et meules abrasifs devraient être attentivement examinés et sonnés (essai au son) en leur appliquant de petits coups à l'aide d'un instrument léger et non métallique pour vérifier qu'ils ne présentent pas de fissures ou autres défauts. Une meule fissurée ou qui émet un son mat risque d'éclater en service. Elle doit donc être mise au rebut. Une meule saine et sans défauts produit un son métallique clair: elle «sonne».

Pour éviter une fissuration de la meule, l'utilisateur doit s'assurer qu'elle coulisse librement sur son axe. L'écrou de l'axe devrait être suffisamment serré pour maintenir la meule en place sans déformer les flasques. Les recommandations du fabricant doivent être respectées. L'utilisateur devrait également vérifier que la vitesse de rotation ne dépasse pas les caractéristiques de la meule. Compte tenu du risque de désintégration ou d'éclatement de la meule au démarrage, le travailleur ne devrait jamais rester face à elle pendant sa montée en vitesse. Les outils de meulage portatifs devraient être équipés de carters de protection protégeant l'opérateur non seulement de la surface en mouvement de la meule, mais aussi contre les projections d'éclats en cas de rupture. En outre, lors de l'utilisation d'une meuleuse à moteur, il convient de:

- Porter une protection oculaire.
- Couper l'alimentation électrique en dehors des périodes d'utilisation.
- Ne jamais bloquer une meuleuse portative dans un étau.

Les outils pneumatiques

Les outils pneumatiques qui fonctionnent à l'air comprimé comprennent les burins, les perceuses, les marteaux et les ponceuses. Quoique ces outils présentent différents dangers potentiels, le principal est celui d'être heurté par un de leurs accessoires, ou par une des fixations que le travailleur pose avec l'outil. Une protection des yeux est nécessaire et une protection du visage recommandée pour l'utilisation d'outils pneumatiques. Le bruit représente également un danger. Lorsqu'on se sert d'outils bruyants comme les marteaux pneumatiques, il est impératif de porter correctement une protection auditive adaptée au risque encouru.

Le travailleur utilisant un outil pneumatique devrait s'assurer que le flexible d'air est bien raccordé et qu'il ne risque pas de se débrancher. Un cordon de faible longueur ou un dispositif d'immobilisation du flexible d'air sur l'outil constitueront une sécurité supplémentaire. Si le flexible a un diamètre supérieur à 13 mm, il est conseillé d'installer une valve de surdébit à la source d'alimentation en air, afin de couper automatiquement l'arrivée d'air en cas de rupture du flexible. En règle générale, il convient d'appliquer aux flexibles les mêmes précautions qu'aux câbles électriques, dans la mesure où ils sont sujets aux mêmes types de détériorations ou de heurts accidentels et où ils présentent le même risque de faire trébucher les personnes.

Les pistolets à air comprimé ne devraient jamais être dirigés vers une personne, ni surtout être pointés «à bout portant» sur soi-même ou quelqu'un d'autre. Une agrafe ou une retenue devraient être installées pour éviter que l'accessoire, ciseau ou burin, ne soit accidentellement chassé du canon. Il est conseillé de placer des écrans pour que les personnes travaillant à proximité soient protégées contre les débris projetés par les burins, les pistolets à riveter, les marteaux pneumatiques, les agrafeuses ou les perceuses pneumatiques.

Les pistolets «airless» destinés à pulvériser des peintures ou des liquides sous des pressions élevées (70 bars ou plus) devraient être équipés de dispositifs visuels automatiques ou manuels empêchant leur mise en service tant que ce dispositif n'a pas été libéré manuellement. Les marteaux-piqueurs lourds peuvent causer une fatigue et des tensions musculaires qu'il est possible d'alléger en les équipant de robustes poignées en caoutchouc assurant une bonne prise. Les travailleurs employant un marteau-piqueur devraient porter des lunettes et des chaussures de sécurité pour se protéger en cas de dérapage ou de chute de l'outil. Un écran facial est également recommandé.

Les outils à moteur thermique

Ces outils fonctionnent généralement à l'aide de petits moteurs à combustion interne utilisant de l'essence. Les dangers les plus graves que présentent ces outils sont les émanations de carburant, qui peuvent s'enflammer ou exploser et émettre des gaz toxiques. On veillera à manipuler, transporter et stocker l'essence uniquement dans des récipients homologués pour les liquides inflammables, et on respectera les précautions applicables à ces liquides. Avant de remplir le réservoir de ces outils, l'utilisateur devrait arrêter le moteur et le laisser refroidir pour éviter une inflammation accidentelle des vapeurs dangereuses. Si un outil à moteur thermique est utilisé dans un local fermé, il est nécessaire d'assurer une ventilation efficace ou de porter un équipement de protection pour éviter une exposition au monoxyde de carbone. On

prendra soin d'équiper la zone concernée d'extincteurs d'incendie.

Les outils de scellement à charge explosive

Ces outils fonctionnent comme des armes à feu et devraient être traités avec le même soin. Ils sont en fait si dangereux qu'ils ne devraient être utilisés que par des personnes ayant reçu une formation spéciale. Une protection correcte des oreilles, des yeux et du visage est indispensable pour travailler avec ces outils. Tous les modèles d'outils à charge propulsive devraient être conçus pour différentes charges, de manière à laisser à l'utilisateur le choix de la puissance strictement nécessaire au travail à effectuer.

L'orifice de l'outil devrait être équipé d'un écran ou d'une protection perpendiculaire au canon pour protéger l'utilisateur des projections d'éclats ou de débris qui peuvent présenter un danger au moment du tir. L'outil devrait être conçu de manière à ne pas pouvoir fonctionner sans ce genre de dispositif de sécurité. Pour éviter tout fonctionnement accidentel, le tir devrait exiger deux mouvements distincts: l'un pour amener l'outil en position, l'autre pour appuyer sur la détente. Il est nécessaire que l'outil puisse fonctionner uniquement lorsqu'on l'appuie contre la surface de travail avec une force supérieure d'au moins 2,5 kg à son propre poids.

En cas de raté, l'utilisateur devrait attendre au moins 30 secondes avant de tenter un nouveau tir. En cas de nouvel échec, il devrait attendre 30 secondes supplémentaires, afin de limiter le risque d'explosion de la cartouche défectueuse, puis retirer la charge avec précaution. La cartouche défectueuse devrait être plongée dans l'eau, ou mise au rebut par tout autre moyen sûr défini par l'entreprise.

En cas d'apparition d'un défaut sur un outil à charge propulsive en cours d'utilisation, l'outil devrait immédiatement être étiqueté et retiré du service jusqu'à ce qu'il soit réparé comme il convient. Voici quelques précautions à prendre pour utiliser et manipuler ces outils dans les conditions de sécurité:

- Les outils à charge propulsive ne devraient pas être employés dans les atmosphères explosives ou inflammables, sauf si un permis spécial a été délivré par une personne autorisée.
- Avant d'utiliser l'outil, le travailleur devrait l'examiner afin de vérifier qu'il est propre, que toutes les pièces mobiles fonctionnent librement et que le canon n'est pas obstrué.
- L'outil ne devrait jamais être dirigé sur une personne.
- L'outil ne devrait être chargé que s'il est prévu de l'utiliser immédiatement. Un outil chargé ne devrait jamais rester sans surveillance, surtout s'il est accessible à des personnes non autorisées.
- Les mains devraient être tenues à l'écart de la bouche du canon.

Lors de la pose de fixations à l'aide d'un outil de scellement à charge propulsive, les mesures de sécurité suivantes devraient être prises:

- Ne pas enfoncer une fixation dans un matériau qu'elle risque de traverser de part en part.
- Ne pas enfoncer une fixation dans des matériaux comme la brique ou le béton à moins de 75 mm ou, dans de l'acier, à moins de 13 mm d'une arête ou d'un angle.
- Ne pas enfoncer de fixations dans des matériaux très durs ou cassants qui risquent de se fragmenter, d'éclater ou de faire ricocher la fixation.
- Utiliser un guide d'alignement lors de la pose de fixations dans des trous existants. Ne pas enfoncer de fixations dans un orifice endommagé par un tir antérieur.

Les outils hydrauliques

Le fluide employé dans les outils hydrauliques devrait être approuvé pour l'utilisation prévue et conserver ses caractéristiques aux températures extrêmes auxquelles il sera exposé. Les pressions de service recommandés par le fabricant pour une utilisation sûre des flexibles, clapets, tuyauteries, filtres et autres accessoires ne devraient pas être dépassées. S'il existe un risque de fuites à haute pression dans une zone où peuvent être présentes des sources d'inflammation telles que flammes ou surfaces chaudes, on devrait envisager l'emploi d'huiles incombustibles.

Les vérins

Tous les vérins — à crémaillère, à vis et hydrauliques — devraient comporter un dispositif les empêchant de dépasser la hauteur prévue. La limite de charge indiquée par le fabricant devrait être inscrite en permanence sur le vérin à un endroit bien visible et ne jamais être dépassée. On placera si nécessaire des cales de bois sous la base afin de mettre le vérin de niveau et le stabiliser. Si la surface à soulever est métallique, on placera un bloc de bois dur ou d'un autre matériau équivalent de 25 mm d'épaisseur entre la surface d'assise et la tête métallique du vérin pour limiter les risques de glissement. Un vérin ne devrait jamais servir à soutenir une charge soulevée. Une fois la charge soulevée, elle devrait être immédiatement soutenue par des cales.

Pour installer un vérin, on vérifiera les points ci-après:

1. Sa base devrait reposer sur une surface ferme et plane.
2. Le vérin devrait être correctement centré.
3. Sa tête devrait s'appuyer contre une surface plane.
4. La force de levage devrait être uniformément répartie.

Une bonne maintenance des vérins est essentielle à la sécurité. Tous les vérins devraient être examinés avant chaque utilisation et lubrifiés périodiquement. Les vérins qui ont supporté des charges excessives ou subi des chocs anormaux devraient être examinés attentivement, afin de vérifier qu'ils ne sont pas endommagés. Les vérins hydrauliques exposés au gel devraient être remplis d'un liquide antigel approprié.

Résumé

Les travailleurs qui emploient des outils à main et des outils à moteur et qui sont exposés à des objets ou matériaux abrasifs ou susceptibles de tomber ou d'être projetés, ainsi qu'aux risques présentés par des poussières, fumées, brouillards, vapeurs ou gaz dangereux, devraient disposer des équipements individuels nécessaires pour se protéger. Les risques associés à l'utilisation des outils à moteur peuvent être évités si les travailleurs respectent cinq règles fondamentales:

1. Conserver les outils en bon état par une maintenance régulière.
2. Utiliser l'outil adapté à la tâche.
3. Vérifier le bon état de chaque outil avant utilisation.
4. Respecter les instructions du fabricant.
5. Choisir et employer les équipements de protection appropriés.

Il appartient aux employeurs et à leur personnel de coopérer pour maintenir des pratiques de travail conformes à la sécurité. Un outil défectueux ou une situation dangereuse devraient être immédiatement signalés à la personne compétente.

LES PARTIES EN MOUVEMENT DES MACHINES

Tomas Backström et Marianne Döös

Cet article traite des situations et des séquences d'événements conduisant à des accidents dus à un contact avec des parties en mouvement des machines. Les personnes chargées de faire fonctionner et d'entretenir des machines encourent des risques d'accidents graves. Les statistiques américaines montrent qu'aux Etats-Unis, 18 000 amputations et plus de 800 décès sont imputables chaque année à ce type de causes. Selon l'Institut national de la sécurité et de la santé au travail (National Institute for Occupational Safety and Health (NIOSH)), c'est dans la catégorie qui correspond, dans la classification de cet organisme, aux situations dans lesquelles des personnes sont prises sous, entre ou dans des objets que le nombre d'accidents professionnels a été le plus élevé. Ces accidents impliquaient généralement des machines (Etherton et Myers, 1990). On a constaté que les événements du type «contact avec des parties en mouvement d'une machine» étaient à l'origine d'un peu plus de 10% des accidents du travail depuis l'introduction de cette catégorie dans les statistiques suédoises des accidents du travail en 1979.

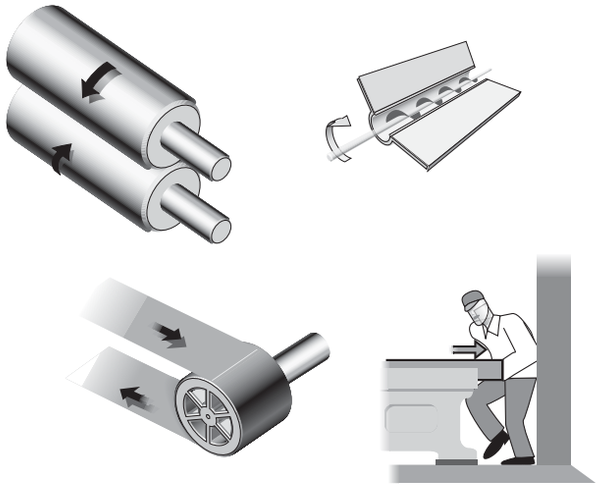
La plupart des machines possèdent des organes mobiles susceptibles de provoquer des lésions. Ces organes peuvent se trouver au point de fonctionnement où un travail comme la coupe, le formage, le perçage ou la déformation est effectué sur un matériau. Ils peuvent se trouver dans les mécanismes transmettant l'énergie aux parties de la machine qui effectuent le travail (volants, poulies, bielles, coupleurs, cames, axes, chaînes, manivelles, pignons, etc.). On les trouve également dans d'autres parties en mouvement des machines, comme les roues des équipements mobiles, les moteurs d'entraînement, les pompes ou les compresseurs. D'autres types de machines comportent des mouvements dangereux, notamment les équipements auxiliaires de manutention et de transport de charges telles que les pièces à usiner, les matériaux, les déchets ou les outils.

Toutes les parties de machines en mouvement pendant l'exécution d'un travail peuvent contribuer à des accidents avec dommages corporels ou matériels. Les mouvements rotatifs et les mouvements rectilignes, de même que leur source d'énergie, peuvent présenter des dangers:

Mouvement rotatif. Les arbres rotatifs, même lisses, peuvent saisir une partie d'un vêtement et entraîner, par exemple, le bras d'une personne vers une position dangereuse. Les arbres rotatifs présentent un danger accru lorsqu'ils possèdent des parties formant saillie ou des surfaces irrégulières ou tranchantes telles que vis de réglage, boulons, fentes, encoches ou arêtes vives. Les parties tournantes des machines créent des «points de pincement» de trois façons différentes:

1. Il y a les points situés entre deux parties tournant en sens inverse sur des axes parallèles, comme les engrenages ou les roues dentées, les rouleaux d'entraînement ou les calandres.
2. Il y a également les points de contact entre les pièces tournantes et les pièces à déplacement linéaire, par exemple entre une courroie de transmission et sa poulie, ou entre une chaîne ou une crémaillère et leurs pignons.
3. Les mouvements des machines rotatives peuvent provoquer des lésions par coupure ou écrasement lorsqu'ils ont lieu à proximité d'objets fixes. De tels accidents peuvent se produire entre une vis de transport et son enveloppe, entre les rayons d'une roue et la table de la machine, ou entre une meule et son touret.

Figure 58.8 • Exemples de mouvements mécaniques pouvant blesser une personne



Mouvements rectilignes. Les mouvements verticaux, horizontaux ou alternatifs peuvent provoquer des blessures de différentes façons: on peut être poussé ou heurté par une pièce de la machine, pris entre cette pièce et un autre objet, coupé par une arête vive ou blessé par pincement entre la partie mobile et un autre objet (voir figure 58.8).

Sources d'énergie. Les sources d'énergie externes utilisées pour entraîner une machine mettent parfois en œuvre des puissances considérables. Ces systèmes peuvent être électriques, à vapeur, hydrauliques, pneumatiques ou mécaniques et ils sont tous susceptibles, en cas de déclenchement intempestif ou de perte de contrôle, d'occasionner de graves dommages corporels ou matériels. Une étude des accidents survenus sur une année (de 1987 à 1988) chez les agriculteurs de neuf villages du nord de l'Inde a révélé que les machines à hacher le fourrage utilisées, qui étaient toutes du même modèle, étaient plus dangereuses lorsqu'elles étaient actionnées par un moteur ou un tracteur. La fréquence relative des accidents impliquant plus qu'une blessure légère (par machine) était de 5,1‰ pour les hacheuses manuelles, contre 8,6‰ pour les hacheuses motorisées (Mohan et Patel, 1992).

Les lésions liées aux mouvements des machines

Les forces associées aux mouvements des machines étant souvent très importantes, on peut présumer qu'elles risquent d'être à l'origine de lésions graves. Cette supposition est confirmée par plusieurs sources. Selon les statistiques britanniques (Health and Safety Executive, 1989), les accidents du type «contact avec une machine en mouvement ou avec des matériaux usinés» représentaient seulement 5% des accidents du travail, mais 10% des accidents mortels ou graves (fractures, amputations, etc.). Les résultats d'études effectuées dans deux usines suédoises de construction automobile vont dans le même sens. Les accidents causés par des mouvements de machines donnaient lieu à deux fois plus de jours d'arrêt de travail, mesurés par les valeurs médianes, que ceux n'impliquant pas de machine. Les accidents liés aux machines différaient également des autres par la partie du corps touchée: selon les résultats, 80% des lésions subies à la suite d'accidents dus à des machines concernaient les mains et les doigts, alors que cette proportion n'était que de 40% pour les autres cas (Backström et Döös, 1995).

S'agissant des risques dans les installations automatisées, la situation se révèle à la fois différente (du point de vue du type d'accident, de la séquence des événements et du degré de gravité des lésions) et plus complexe (à la fois du point de vue technique et sur le plan des qualifications spécialisées requises) que pour les installations employant des machines classiques. Le terme automatisé désigne ici des équipements qui, sans intervention directe de l'être humain, sont capables de déclencher un mouvement d'une machine ou de changer sa direction ou sa fonction. Ces équipements emploient des dispositifs de détection (par exemple, détecteurs de position ou microcontacts) ou une certaine forme de commande séquentielle (comme un programme informatique) pour contrôler et diriger leur travail. Depuis quelques décennies, les automates à logique programmable sont de plus en plus répandus en tant qu'unités de contrôle dans les systèmes de production. L'utilisation de micro-ordinateurs tend désormais à se généraliser pour contrôler les équipements de production dans les pays industriels, tandis que les autres systèmes de commande comme les appareils électromécaniques sont de moins en moins nombreux. Dans l'industrie manufacturière suédoise, l'utilisation des machines à commande numérique a augmenté de 11 à 12% par an dans les années quatre-vingt (Hörte et Lindberg, 1989). Dans la production industrielle moderne, être blessé par des «parties de machines en mouvement» devient de plus en plus synonyme d'être blessé par des «mouvements de machines commandés par ordinateur».

On rencontre des installations automatisées dans des secteurs industriels toujours plus nombreux et le nombre de leurs fonctions va croissant. L'automatisation se répand dans les activités de stockage, de manutention, de traitement des matériaux, de transformation, d'assemblage et d'emballage. La fabrication en série ressemble désormais à la production dans les industries de transformation. Si l'introduction, l'usinage et l'éjection des pièces sont mécanisés, l'opérateur n'a plus besoin de rester dans la zone dangereuse tant la production se déroule sans incident. Des études sur la fabrication automatisée ont révélé que les accidents se produisaient surtout lors des interventions suivant les perturbations de la production. Mais les personnes peuvent être également exposées aux mouvements des machines pendant l'exécution d'autres travaux comme les nettoyages, les réglages, les contrôles et les réparations.

Lorsque la production est automatisée et que le processus n'est plus sous le contrôle direct de l'être humain, les risques de mouvements intempestifs de la machine augmentent. La plupart des opérateurs travaillant sur des groupes ou des lignes de machines reliées entre elles rencontrent ces mouvements inattendus. De nombreux accidents d'automatisation ont pour origine ce genre de mouvements. Un accident d'automatisation est un accident dans lequel le système automatique contrôlait (ou aurait dû contrôler) l'énergie responsable de l'accident, ce qui signifie que la force produisant les lésions corporelles provient de la machine elle-même (c'est-à-dire de l'énergie cinétique de la machine). Dans une étude portant sur 177 accidents d'automatisation en Suède, on a constaté que dans 84% des cas les lésions étaient causées par la «mise en marche intempestive» d'une partie de la machine (Backström et Harms-Ringdahl, 1984). La figure 58.9 montre un exemple type d'accident causé par le mouvement d'une machine commandée par ordinateur.

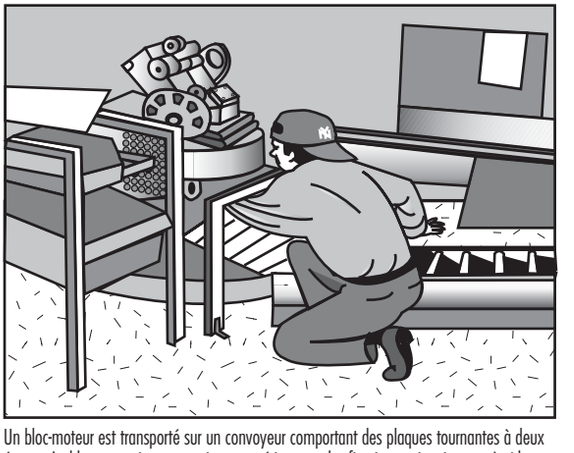
Une des études citées plus haut (Backström et Döös, 1995) a montré qu'il existait un lien de causalité entre le fait que des mouvements de machines sont commandés automatiquement et la plus longue durée des arrêts de travail parmi le personnel correspondant, par rapport aux accidents dus à d'autres types de mouvements de machines, la valeur médiane étant quatre fois supérieure dans l'un des lieux de travail considérés. Le type de lésions dans les accidents d'automatisation était similaire à celui des autres accidents avec des machines (principalement les mains et les doigts), mais avec un degré de gravité tendant à être supérieur (amputations, écrasements et fractures).

Les systèmes de commande par ordinateur, tout comme les systèmes manuels, ne présentent pas une fiabilité absolue. Rien ne garantit qu'un programme informatique fonctionnera sans erreur. L'électronique, de par le faible niveau de ses signaux, peut être sensible à des interférences en l'absence d'une protection adéquate, et les conséquences des défaillances qui peuvent en résulter ne sont pas toujours prévisibles. De plus, les changements apportés à la programmation sont rarement signalés. Une des méthodes employées pour compenser cette lacune est, par exemple, le recours à des systèmes dédoublés, comportant deux chaînes indépendantes de composants fonctionnels, avec une méthode de surveillance qui vérifie que toutes deux donnent la même valeur. L'apparition de valeurs différentes indique une défaillance de l'une des chaînes. Il reste malgré tout possible que les deux chaînes souffrent du même défaut et que toutes deux soient déréglées par la même perturbation, donnant ainsi des valeurs faussement positives (puisque les deux systèmes concordent). Néanmoins, il n'a été possible que dans quelques-uns seulement des cas étudiés d'imputer un accident à une défaillance de l'ordinateur (voir ci-dessous), malgré le fait qu'un même ordinateur contrôle fréquemment toutes les fonctions d'une installation (y compris l'arrêt d'une machine suite à l'activation d'un dispositif de sécurité). Une autre solution envisageable consiste à équiper un système éprouvé avec des composants électromécaniques pour assurer les fonctions de sécurité.

Les problèmes techniques

On peut dire, d'une manière générale, qu'un même accident a de nombreuses causes, qu'elles soient d'ordre technique ou individuel, ou en rapport avec l'environnement ou l'organisation. Aux fins de prévention, la meilleure manière de considérer un accident n'est pas de le traiter comme un événement isolé, mais plutôt comme une séquence d'événements (Backström, 1996). Dans le cas des accidents d'automatisation, on a montré que des problèmes

Figure 58.9 • Exemple type d'accident provoqué par un mouvement de machine commandée par ordinateur



Un bloc-moteur est transporté sur un convoyeur comportant des plaques tournantes à deux étages. Le bloc est maintenu au niveau supérieur par des fixations qui reviennent à vide au niveau inférieur. Le convoyeur s'arrête brusquement. Un ouvrier du montage constate qu'une des fixations s'est coincée de nouveau dans la plaque. Au moment où il tend la main et tire le bloc, un capteur est activé. La plaque entre en rotation et coince la main.

(Illustrateur: Tomas Karlsson.)

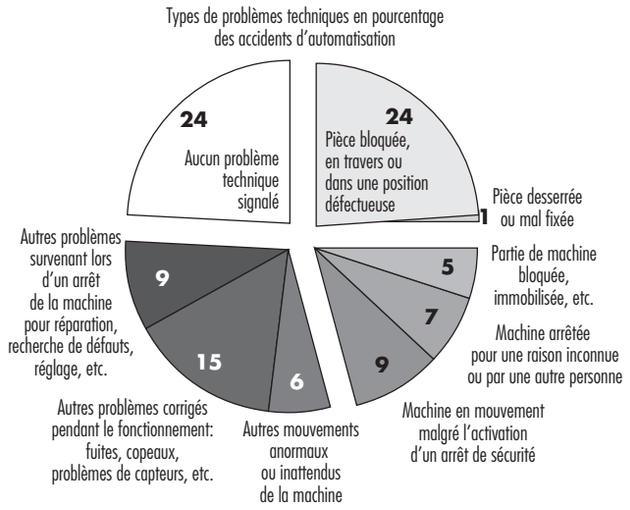
techniques font souvent partie de cette séquence et qu'ils surviennent soit à un stade précoce du processus, soit à un moment proche de l'accident lui-même. Les études qui se sont intéressées aux problèmes techniques impliqués dans des accidents d'automatisation suggèrent qu'ils sont présents dans 75 à 85% des cas. En même temps, il existe habituellement dans chaque cas spécifique d'autres causes, de nature organisationnelle, par exemple. Ce n'est que dans un cas sur dix que l'on a pu attribuer directement à une défaillance technique l'énergie responsable d'un accident, par exemple lorsqu'une machine effectue un mouvement bien qu'elle soit en position d'arrêt. Des chiffres semblables sont mentionnés dans d'autres études. Habituellement, il s'agit d'un problème technique qui provoque un dysfonctionnement du matériel, obligeant l'opérateur à changer de tâche, par exemple pour libérer une pièce bloquée. L'accident survient alors pendant l'intervention, à cause d'une défaillance technique. Un quart des accidents d'automatisation sont précédés d'une perturbation dans la circulation des matériaux, telle que pièce bloquée ou en mauvaise position (voir figure 58.10).

Dans une étude portant sur 127 accidents impliquant l'automatisation, 28 d'entre eux, décrits dans la figure 58.10, ont fait l'objet d'une enquête complémentaire en vue de déterminer les types de problèmes techniques susceptibles d'être incriminés (Backström et Döös, 1997a). Les problèmes identifiés par ces enquêtes provenaient la plupart du temps d'éléments bloqués, défectueux ou usés. Dans deux cas, le problème était dû à une erreur du programme informatique et, dans un autre, à des interférences électromagnétiques. Dans plus de la moitié des cas (17 sur 28), les défauts existaient depuis quelque temps mais n'avaient pas été corrigés. Sur l'ensemble des 28 cas pour lesquels on avait mentionné une défaillance ou une anomalie technique, on ne comptait que 5 cas où le défaut ne s'était *pas* manifesté auparavant. Certains défauts avaient été corrigés, mais étaient réapparus ultérieurement. Certains existaient dès l'installation, tandis que d'autres résultaient de l'usure ou des effets de l'environnement.

Selon la plupart des études, la proportion d'accidents d'automatisation survenus lors d'une intervention à la suite d'un incident dans le processus de production se situe entre un tiers et deux tiers de tous les cas. Ce genre d'intervention est donc généralement considéré comme une activité professionnelle dangereuse. Les différences de fréquence de ces accidents s'expliquent de plusieurs façons, entre autres par des raisons liées au type de production ou à la classification des tâches professionnelles. Dans certaines études sur les incidents, seuls les problèmes et les arrêts de machines en cours de production normale sont pris en compte, alors que d'autres s'intéressent à un éventail de problèmes plus large, par exemple ceux qui surviennent au cours des opérations de préparation du travail.

Une mesure très importante pour la prévention des accidents d'automatisation consiste à élaborer des procédures pour supprimer les causes des incidents de production et éviter ainsi qu'elles ne se reproduisent. Dans une étude spécialisée sur les incidents de production débouchant sur des accidents (Döös et Backström, 1994), on a constaté que l'intervention la plus fréquente à la suite d'un incident consistait à dégager une pièce coincée ou à rectifier la position d'une pièce mal placée. Ce type de problème déclenchait l'une ou l'autre de deux séquences d'événements assez semblables: 1) la pièce était libérée et revenait à sa position correcte, la machine recevait un signal automatique de remise en marche et la personne était blessée par le mouvement déclenché; 2) la personne n'avait pas le temps de dégager ou de repositionner la pièce et était blessée par un mouvement de la machine survenu de manière inattendue ou plus rapidement, ou avec une force supérieure à ce que l'opérateur prévoyait. D'autres interventions sur incidents consistaient à déclencher l'impulsion d'un capteur, à débloquer une pièce de la machine, à effectuer des recherches simples sur les causes d'un défaut ou à préparer un redémarrage (voir figure 58.11).

Figure 58.10 • Types de problèmes techniques impliqués dans des accidents d'automatisation (nombre d'accidents = 127)

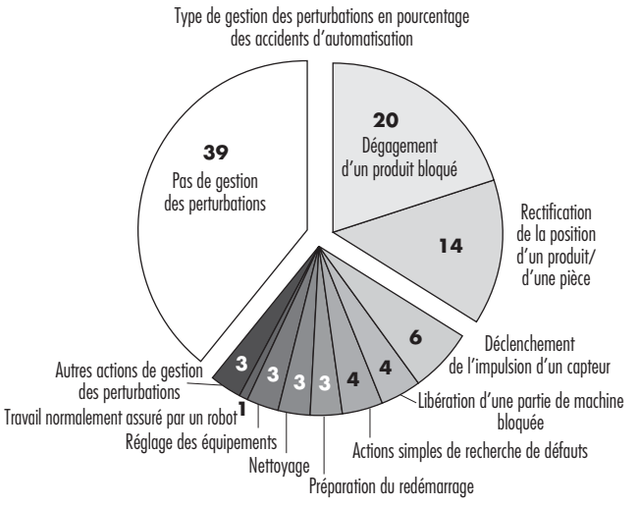


Source: Backström et Döös, 1994.

La sécurité des travailleurs

Les catégories de personnel les plus susceptibles d'être victimes d'accidents d'automatisation varient selon la manière dont le travail est organisé, c'est-à-dire selon les groupes professionnels préposés aux tâches dangereuses. En pratique, il s'agit de la personne habituellement chargée de régler les problèmes et les incidents sur le lieu de travail. Dans l'industrie suédoise moderne, on demande généralement aux opérateurs d'une machine d'effectuer des interventions actives. C'est la raison pour laquelle, dans l'étude précé-

Figure 58.11 • Type de gestion des perturbations au moment de l'accident (nombre d'accidents = 76)



demment citée sur une usine suédoise de construction automobile (Backström et Döös, 1997b), on a constaté que 82% des personnes victimes de lésions causées par des machines automatisées étaient des ouvriers de production ou des opérateurs. Les opérateurs présentaient également une fréquence relative d'accidents plus élevée (15 accidents d'automatisation par an pour 1 000 opérateurs) que les ouvriers de maintenance (6‰). Les résultats des études montrant que les ouvriers de maintenance sont plus touchés s'expliquent au moins en partie par le fait que, dans certaines entreprises, il est interdit aux opérateurs de pénétrer dans les zones d'usinage. Dans d'autres établissements, où la répartition des tâches est différente, d'autres catégories de personnel — les régleurs par exemple — peuvent être chargées de résoudre les problèmes de production.

La mesure corrective la plus fréquemment prise en vue d'augmenter le niveau de sécurité individuelle consiste à protéger la personne contre les mouvements dangereux de la machine à l'aide d'un dispositif de sécurité, tel qu'une barrière. Le principe majeur dans ce cas est celui de la sécurité «passive», c'est-à-dire la mise en place d'une protection ne nécessitant pas d'action de la part du travailleur. Il est cependant impossible de juger de l'efficacité des dispositifs de protection sans une très bonne connaissance des exigences réelles du travail sur la machine en question, connaissance que les opérateurs sont en général les seuls à posséder.

De nombreux facteurs sont susceptibles de rendre inopérante une protection, même apparemment adéquate, d'une machine. Pour faire leur travail, les opérateurs peuvent être amenés à neutraliser ou à contourner un dispositif de sécurité. Dans une étude (Döös et Backström, 1993), on a constaté qu'une neutralisation ou un contournement de ce genre avait eu lieu dans 12 des 75 accidents d'automatisation considérés. Il s'agit souvent de l'excès de zèle d'un opérateur, qui n'est plus disposé à accepter les problèmes de production ou les retards qui en résultent pour le processus de production lorsqu'on se conforme aux instructions pour les interventions à la suite d'un incident. Une manière d'éviter ce problème est de rendre le dispositif de protection imperceptible, de sorte qu'il n'ait pas d'incidence sur les cadences de production, la qualité du produit ou l'exécution des tâches. Mais ce n'est pas toujours possible et si les incidents de production se répètent, des inconvénients, même mineurs, peuvent inciter les travailleurs à ne pas utiliser les dispositifs de protection. Dans ce domaine également, il conviendrait de fixer des procédures pour éliminer les causes des incidents de production et éviter leur répétition. L'absence de moyens permettant de confirmer que les dispositifs de protection fonctionnent réellement selon les spécifications constitue également un facteur de risque non négligeable.

Des anomalies telles que des défauts de raccordement, des signaux de mise en marche qui restent dans le système et occasionnent ultérieurement des démarrages intempestifs, l'accumulation d'une pression d'air et des détecteurs mal fixés sont susceptibles d'entraîner une défaillance de l'équipement de protection.

Résumé

Comme on vient de le montrer, les solutions techniques apportées à certains problèmes peuvent en susciter d'autres. Le fait que des accidents sont causés par des mouvements des machines, phénomène de nature essentiellement technique, ne signifie pas nécessairement qu'ils puissent être supprimés uniquement par des mesures techniques. Les systèmes techniques continueront à connaître des dysfonctionnements et les travailleurs ne réussiront pas à maîtriser dans tous les cas les situations qui en résultent. Les risques continueront d'exister et on ne pourra en conserver le contrôle que par la mise en œuvre de moyens très divers. La législation et les contrôles, les mesures d'organisation prises au niveau de l'entreprise (formation, inspections de sécurité, analyse des risques et rapports sur les incidents et les situations dangereuses), ainsi qu'un souci constant d'amélioration sont des compléments nécessaires aux progrès purement techniques.

LA PROTECTION DES MACHINES

US Department of Labor — Occupational Safety and Health Administration;
édité par Kenneth Gerecke

Il semble que les dangers créés par les parties en mouvement des machines soient presque aussi variés que les types de machines eux-mêmes. Des mesures sont indispensables pour protéger les travailleurs contre les accidents évitables dus aux machines. C'est la raison pour laquelle des dispositifs de protection devraient être prévus pour toute partie d'installation ou de machine susceptible de causer des accidents. Lorsque le fonctionnement d'une machine ou un contact accidentel avec l'une de ses parties risquent de blesser l'opérateur ou les personnes se trouvant à proximité, le danger doit être éliminé ou neutralisé.

Les mouvements et les actions mécaniques

Les risques d'origine mécanique impliquent généralement des pièces mobiles dangereuses dans trois secteurs principaux:

- *la zone de travail ou d'opération*, où le travail est exécuté sur le matériau par une action de coupe, de poinçonnage ou de perçage, par exemple;
- *le système de transmission d'énergie*, c'est-à-dire les organes qui transmettent l'énergie mécanique aux parties travaillantes de la machine. Ils comprennent notamment les volants, poulies, courroies, chaînes, bielles, accouplements, cames, arbres, manivelles et engrenages;

Figure 58.12 • Poinçonneuse mécanique

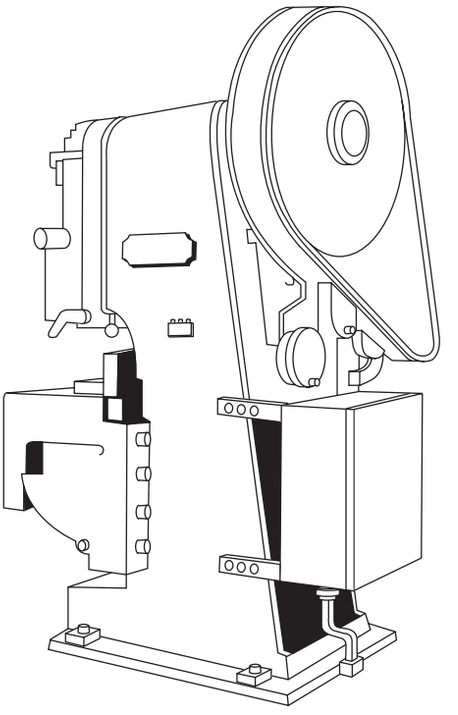
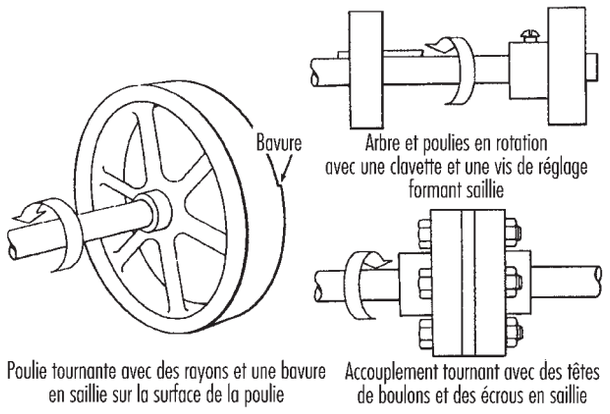


Figure 58.13 • Exemples de parties saillantes dangereuses sur des pièces tournantes



- *les autres organes en mouvement*, c'est-à-dire toute partie de la machine en mouvement au cours du travail (mouvement alternatif, rotatif ou de translation), ainsi que les mécanismes d'alimentation et d'éjection et certains organes auxiliaires.

Il existe une grande diversité de mouvements et d'actions susceptibles de présenter des dangers pour les travailleurs et qui correspondent aux déplacements des organes rotatifs, des bras oscillants, des courroies, des engrenages en prise et de toutes les pièces ayant un effet d'impact ou de cisaillement. Ces différents types de mouvements et d'actions mécaniques se retrouvent dans presque toutes les machines, et leur identification constitue la première étape lorsqu'on étudie la protection des travailleurs contre leurs dangers potentiels.

Les mouvements

Il existe trois types fondamentaux de mouvements: rotatif, alternatif et de translation.

Les *mouvements rotatifs* peuvent être dangereux: même des arbres lisses à rotation lente peuvent happer un vêtement et entraîner un bras ou une main vers une zone dangereuse. Les blessures dues à un contact avec des parties tournantes peuvent être très graves.

Les colliers, accouplements, cames, embrayages, volants, extrémités d'arbres, arbres horizontaux ou verticaux sont des exemples de mécanismes rotatifs courants et potentiellement dangereux

Figure 58.14 • Points de prise courants sur des pièces tournantes

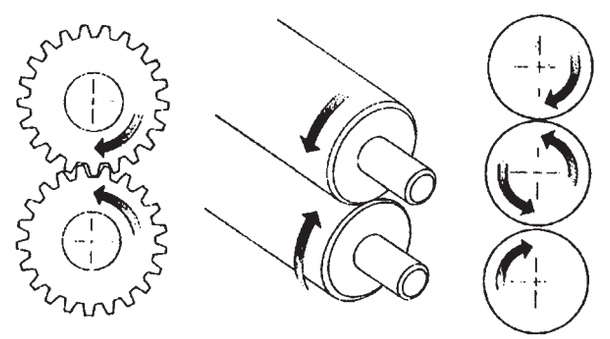
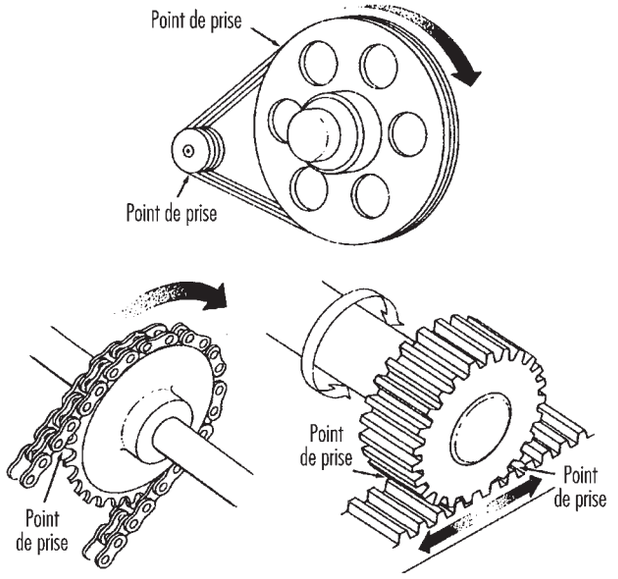


Figure 58.15 • Points de prise entre des éléments tournants et des pièces à mouvement tangentiel



(voir figure 58.12). Ils présentent un danger supplémentaire lorsque des parties en mouvement comportent des boulons, des encoches, des parties rugueuses, des clavettes, des vis de réglage ou d'autres parties saillantes non protégées, comme le montre la figure 58.13.

Des *points d'entraînement par coincement* sont créés par les parties tournantes des machines. Il en existe trois types principaux:

1. Pièces à axes parallèles tournant en sens inverse. Elles peuvent être en contact (créant ainsi une zone de pincement) ou très proches l'une de l'autre (angle rentrant), auquel cas ce sont les matériaux introduits qui créent les points de coince-

Figure 58.16 • Points de prise entre des éléments tournants de machines et des parties fixes

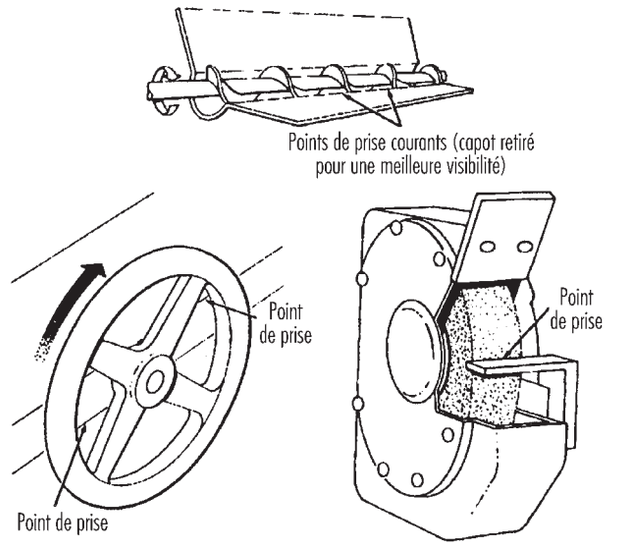
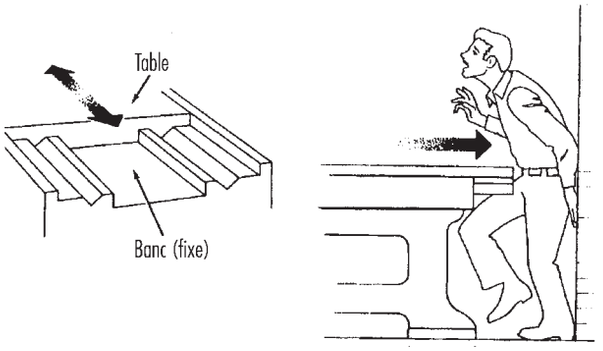


Figure 58.17 • Mouvement alternatif dangereux



ment. Ce danger est fréquent sur les engrenages en prise, les rouleaux, les laminoirs et les calandres, comme le montre la figure 58.14.

2. Un autre type de risque de coincement existe entre des pièces en mouvement rotatif et d'autres à mouvement tangentiel, comme le point de contact entre une courroie de transmission et sa poulie, une chaîne et une roue dentée, ou un pignon et une crémaillère, comme le montre la figure 58.15.
3. Des points de pincement existent également entre des parties rotatives et des parties fixes, ce qui crée un risque de cisaillement, d'écrasement ou d'abrasion. On peut citer l'exemple des volants de commande ou d'inertie comportant des rayons, les transporteurs à vis ou l'espace qui sépare la périphérie d'une meule et un repose-pièce mal réglé (voir figure 58.16).

Les *mouvements alternatifs* peuvent être dangereux dans la mesure où l'opérateur risque d'être heurté par une pièce en mouvement ou coincé entre une partie mobile et une partie fixe. Un exemple est donné à la figure 58.17.

Les *mouvements de translation continue* (mouvements rectilignes) sont une source de danger dans la mesure où l'opérateur peut être heurté par une partie en mouvement ou coincé dans un angle rentrant ou une zone de cisaillement. La figure 58.18 donne un exemple de ce type de mouvement.

Les actions

Il existe quatre grands types d'action: la coupe, le poinçonnage, le cisaillage et le pliage.

L'*action de coupe* implique des mouvements rotatifs, alternatifs ou de translation. Elle crée des dangers dans la zone de travail où il peut se produire des blessures aux doigts, à la tête ou aux

Figure 58.18 • Exemple de mouvement de translation

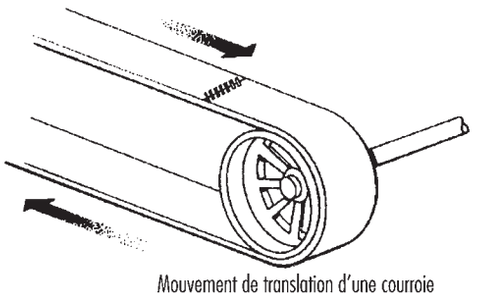
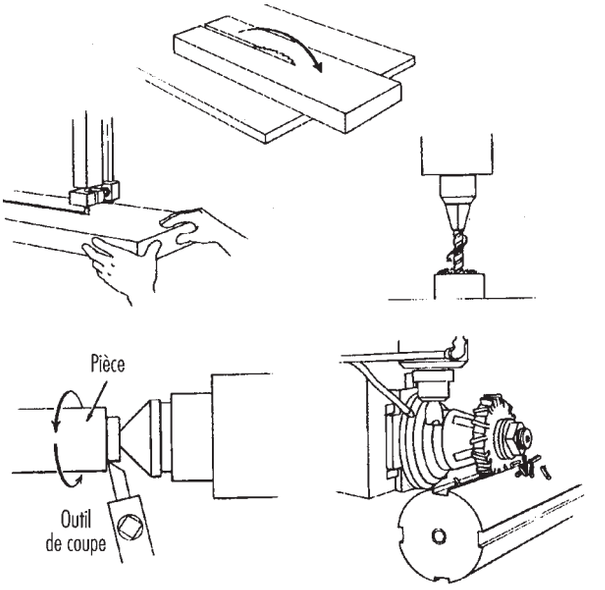


Figure 58.19 • Exemples de risques de lacération



bras et où des copeaux ou des débris peuvent être projetés sur les yeux ou le visage. Les principales machines comportant des risques liés aux opérations de coupe sont les scies à ruban, les scies circulaires, les perceuses et aléseuses, les tours et les fraiseuses (voir figure 58.19).

L'*action de poinçonnage* résulte de l'application d'une force à un coulisseau pour l'ébauchage, l'étirage ou l'estampage de métaux ou d'autres matériaux. Le danger de ce type d'action se présente dans la zone de travail où la pièce est introduite, maintenue et extraite à la main. Les machines les plus courantes de cette caté-

Figure 58.20 • Représentation d'une opération de poinçonnage

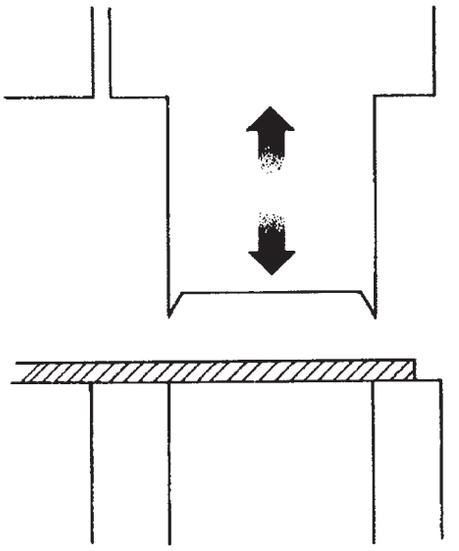
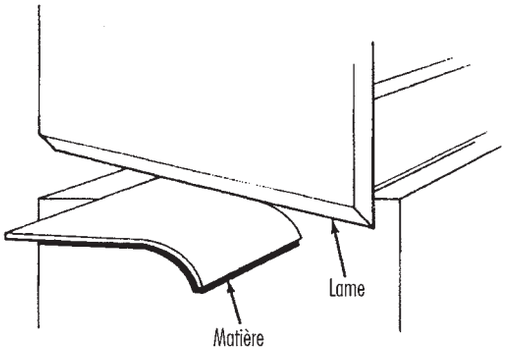


Figure 58.21 • Opération de cisaillage



gorie sont les presses de divers types et les marteaux pilons (voir figure 58.20).

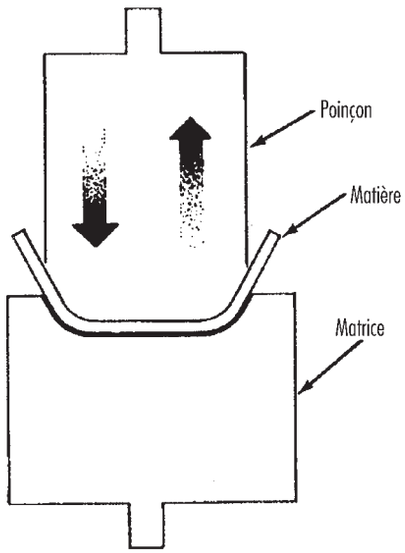
L'*action de cisaillage* consiste à appliquer une force à un coulisseau ou à une lame pour la découpe ou le cisaillage de métaux ou d'autres matériaux. Il existe un risque de cisaillement dans la zone de travail, c'est-à-dire là où la pièce est introduite, maintenue et extraite. Les machines généralement utilisées pour ces opérations sont les cisailles mécaniques, hydrauliques ou pneumatiques (voir figure 58.21).

L'*action de pliage* résulte de l'application d'une force à un coulisseau pour former, étirer ou estamper un métal ou un autre matériau. Il existe un risque de lésion dans la zone de travail lorsque la pièce est introduite, maintenue et extraite. Les machines de cette catégorie sont les presses, les plieuses et les presses à cintrer (voir figure 58.22).

Les caractéristiques requises des dispositifs de protection

Pour protéger les travailleurs contre les risques mécaniques, ces dispositifs devraient répondre aux caractéristiques générales minimales suivantes:

Figure 58.22 • Opération de pliage



Eviter le contact. Le dispositif de protection devrait empêcher que les mains, les bras ou toute autre partie du corps ou encore des vêtements n'entrent en contact avec des organes mobiles dangereux, en éliminant toute possibilité pour les opérateurs ou autres travailleurs de s'approcher de ces organes.

Garantir la sécurité. On devrait veiller à ce que les travailleurs ne puissent pas enlever ou neutraliser facilement le dispositif de protection. Les barrières, écrans et autres dispositifs de sécurité devraient être réalisés en matériaux durables, capables de supporter les conditions d'utilisation normales et être solidement fixés à la machine.

Protéger contre les chutes d'objets. La protection devrait être conçue pour empêcher que des objets étrangers ne puissent atteindre des parties en mouvement et les endommager ou ne soient transformés en projectiles dangereux.

Ne pas créer de nouveaux dangers. Une protection ne remplit pas son rôle si elle crée par elle-même un danger, par exemple un point de cisaillement ou une arête tranchante. Les bords des protecteurs devraient être roulés (ou boulonnés) de manière à éliminer les arêtes vives.

Ne pas créer d'interférences. Les protections qui gênent les travailleurs dans l'exécution de leurs tâches risquent d'être rapidement neutralisées ou ignorées. Dans la mesure du possible, les travailleurs devraient pouvoir lubrifier les machines sans devoir détacher ou retirer leurs protecteurs. Le fait, par exemple, de placer le réservoir d'huile à l'extérieur de la protection, avec une tuyauterie aboutissant au point de lubrification, évite de devoir pénétrer dans la zone dangereuse.

La formation aux systèmes de protection

Le plus élaboré des systèmes de protection ne peut assurer une véritable sécurité que si les travailleurs savent pourquoi et comment l'employer. Une formation spécifique et détaillée est un élément important de tout programme de mise en place de protecteurs contre les dangers des machines. Des protecteurs bien étudiés peuvent améliorer la productivité et le rendement en libérant les travailleurs de la crainte d'être blessés. Une formation concernant les protecteurs est nécessaire pour les nouveaux opérateurs et le personnel chargé de la maintenance ou des réglages, lors de la mise en place de protecteurs nouveaux ou modifiés, ou lorsque des travailleurs sont affectés à une nouvelle machine ou une nouvelle fonction. Elle devrait comprendre des cours ou un enseignement pratique portant sur les points suivants:

- description et identification des dangers associés à des machines particulières ainsi que des protecteurs spécifiques contre chacun des dangers rencontrés;
- comment les protecteurs assurent la sécurité, comment les utiliser et pourquoi;
- comment et dans quelles circonstances il est possible de retirer les protecteurs, et qui doit le faire (en général, uniquement le personnel de réparation et de maintenance);
- ce qu'il convient de faire (par exemple aviser la hiérarchie) si un protecteur est endommagé, absent ou hors d'état d'assurer la sécurité voulue.

Les méthodes de mise en sécurité des machines

Il existe de nombreuses manières d'assurer aux machines le niveau de sécurité requis. Le type d'opération, les dimensions ou la forme des matériaux, la méthode de manutention, l'agencement physique de la zone de travail, le type de matériau et les besoins ou les limitations de la production permettront de déterminer la méthode de protection appropriée à une machine particulière. Le concepteur de la machine ou le responsable de la sécurité doivent choisir la protection la plus efficace et la plus pratique possible.

Figure 58.23 • Protection fixe sur une presse mécanique

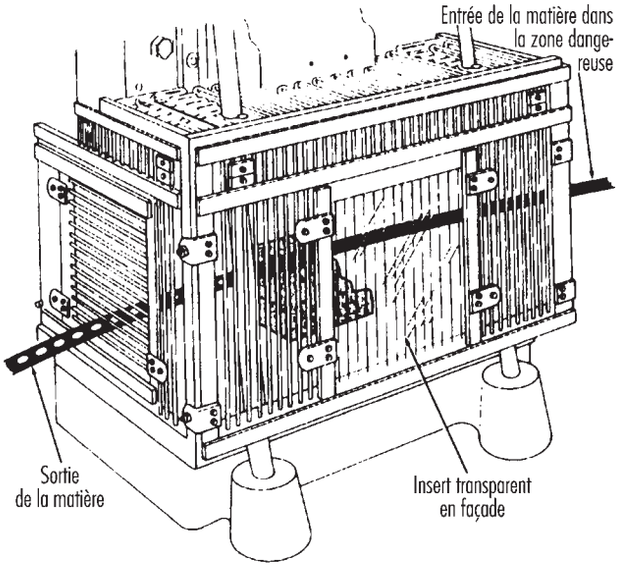
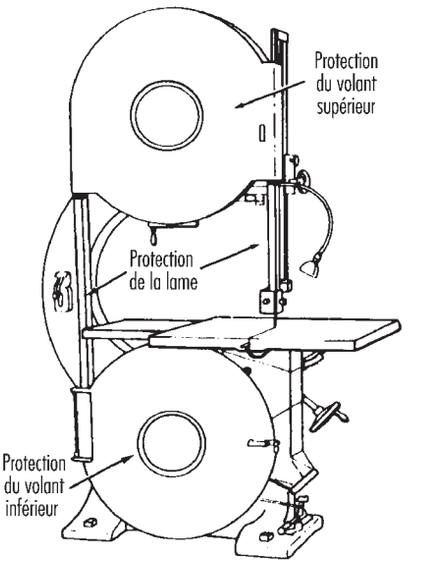


Figure 58.25 • Protection fixe sur une scie à ruban



On peut classer les systèmes de protection en cinq grandes catégories: 1) les protections matérielles, fixes ou mobiles; 2) les dispositifs de sécurité; 3) la protection par séparation (par l'emplacement ou la distance); 4) les dispositifs d'alimentation et d'éjection; 5) les autres systèmes.

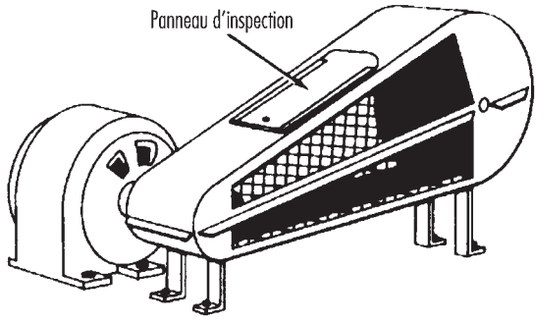
Les protections matérielles

Il existe quatre types principaux de protections formant barrière pour interdire l'accès aux zones dangereuses:

Protecteurs fixes. Un protecteur fixe est un élément permanent de la machine qui ne met en œuvre aucune pièce mobile pour assurer sa fonction. Il peut être réalisé en tôle, en grillage, en treillis métallique, sous forme de barres, en plastique ou dans tout autre matériau capable de résister aux chocs qu'il pourrait recevoir ainsi qu'à un usage prolongé. Les protecteurs fixes sont généralement préférables à tous les autres types de protection en raison de leur relative simplicité et de leur caractère permanent (voir tableau 58.2).

Sur la figure 58.23, un protecteur fixe monté sur une presse enferme complètement la zone d'opération. Le matériau est introduit dans cette zone par le côté de la barrière, les chutes étant évacuées par le bas.

Figure 58.24 • Protection fixe pour courroies et poulies



La figure 58.24 montre un carter fixe encoffrant la courroie et les poulies d'une unité de transmission. Un panneau d'inspection est aménagé au sommet pour réduire au minimum les interventions nécessitant la dépose du carter.

La figure 58.25 montre des carters fixes équipant une scie à ruban. Ils empêchent tout contact avec les volants en rotation. Ces protecteurs ne devraient en principe être ouverts ou retirés que pour les changements de lame ou la maintenance. Il est très important qu'ils soient solidement fixés pendant le fonctionnement de la scie.

Protecteurs à verrouillage. Lorsqu'on ouvre ou qu'on retire des protecteurs à verrouillage, le mécanisme de déclenchement ou l'alimentation en énergie sont automatiquement coupés ou déconnectés, et la machine ne peut pas accomplir son cycle ou être

Figure 58.26 • Protection avec contacteur de sécurité sur un batteur

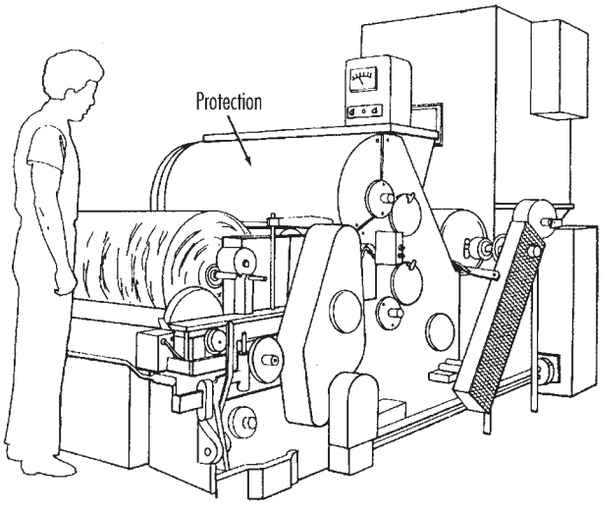
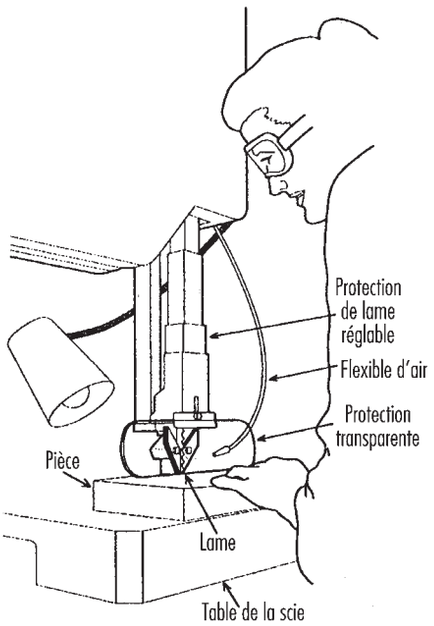


Tableau 58.2 • Protections relatives aux machines

Méthode	Action de protection	Avantages	Limites
Fixe	• Forme une barrière	• Convient à de nombreuses applications spécifiques • Intégration souvent possible • Assure une protection maximale • Ne demande généralement qu'une maintenance minimale • Convient à la production en gros volumes et aux opérations répétitives	• Peut gêner la visibilité • Limitée à certaines opérations spécifiques • Les réglages et les réparations de la machine imposent souvent son démontage et on doit donc prévoir d'autres dispositifs de sécurité pour le personnel de maintenance
Verrouillage	• Coupe ou déconnecte l'alimentation et empêche le démarrage de la machine lorsque la protection est ouverte; doit provoquer l'arrêt de la machine avant que l'opérateur puisse atteindre la zone de danger	• Assure une protection maximale • Laisse accès à la machine pour dégager les bourrages sans perte de temps pour le démontage d'installations fixes	• Impose un réglage et une maintenance minutieux • Peut être facile à désactiver ou à contourner
Réglable	• Forme une barrière pouvant être réglée pour faciliter différentes opérations de production	• Peut être construite en fonction d'applications spécifiques diverses • S'adapte à différentes tailles de matières à usiner	• L'opérateur peut pénétrer dans la zone de danger: la protection peut ne pas être totale en permanence • Peut nécessiter une maintenance ou des réglages fréquents • Peut être rendue inefficace par l'opérateur • Peut gêner la visibilité
Auto-réglable	• Forme une barrière mobile en fonction de la taille des matières pénétrant dans la zone de danger	• Modèles couramment disponibles sur le marché	• N'assure pas toujours une protection maximale • Peut gêner la visibilité • Peut nécessiter une maintenance ou des réglages fréquents

remise en marche tant que le protecteur n'a pas été remis en place. En revanche, la remise en place du protecteur ne devrait pas provoquer le redémarrage automatique de la machine. Ces protections peuvent utiliser l'énergie électrique, mécanique, hydraulique ou pneumatique, ou une combinaison quelconque de ces énergies. Elles ne devraient pas empêcher la marche pas à pas ou la commande par impulsions (c'est-à-dire des mouvements lents et limités) commandées à distance, lorsque ce mode de fonctionnement est prévu.

Figure 58.27 • Protection télescopique sur une scie à ruban



Un exemple de protecteur avec dispositif de verrouillage est montré à la figure 58.26. Sur cette illustration, le mécanisme de battage est recouvert d'un protecteur à verrouillage. Celui-ci ne peut pas être ouvert lorsque la machine est en marche, et la machine ne peut être remise en marche tant que le protecteur demeure ouvert.

Protecteurs réglables. Les protecteurs réglables permettent de tenir compte des dimensions variables des matériaux. La figure 58.27 montre un carter télescopique monté sur une scie à ruban.

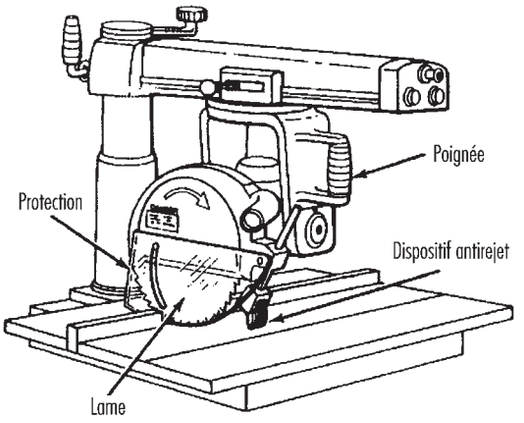
Protecteurs à réglage automatique. Les ouvertures des protecteurs à réglage automatique sont déterminées par le mouvement des matériaux. A mesure que l'opérateur déplace le matériau vers la zone dangereuse, le protecteur est repoussé en dégageant une ouverture juste suffisante pour le passage du matériau. Une fois celui-ci retiré, le protecteur revient en position de repos. Ce type de protection interpose une barrière entre la zone dangereuse et l'opérateur. Ces protecteurs peuvent être réalisés en plastique, en métal ou dans un autre matériau robuste. Ils offrent différents niveaux de protection.

La figure 58.28 montre une scie à bras radial équipée d'une protection à réglage automatique. Lorsque la lame rencontre le matériau, la protection se soulève mais reste en contact avec celui-ci.

Les dispositifs de sécurité

Il existe des dispositifs de sécurité permettant d'arrêter une machine lorsqu'une main ou une partie quelconque du corps est placée par inadvertance dans la zone dangereuse, de retenir les mains de l'opérateur ou de les retirer de la zone dangereuse pendant le fonctionnement, de contraindre l'opérateur à poser simultanément les deux mains sur les commandes de la machine (de manière à maintenir les deux mains et le reste du corps à

Figure 58.28 • Protection à réglage automatique sur une scie à bras radial



l'écart) ou d'actionner une barrière en synchronisation avec le cycle de fonctionnement de la machine, afin d'empêcher toute pénétration dans la zone de danger au cours de la partie dangereuse du cycle. Ces dispositifs de sécurité sont classés selon les grandes catégories ci-après:

Les dispositifs à détection de présence

Trois types de détecteurs arrêtant la machine ou interrompant son cycle de travail si un travailleur est présent dans la zone dangereuse sont décrits ci-après:

Les *détecteurs de présence photoélectriques (optiques)* emploient un système de sources lumineuses et de commandes permettant d'interrompre le cycle de la machine. Si le faisceau lumineux est interrompu, la machine s'arrête. Ces dispositifs ne devraient être utilisés que sur les machines qui peuvent être mises à l'arrêt avant que le travailleur n'entre dans la zone dangereuse. La figure 58.29 montre un détecteur de présence photoélectrique installé sur une plieuse. Il peut être orienté en fonction des besoins de la production.

Figure 58.29 • Dispositif photoélectrique de détection de présence sur une plieuse

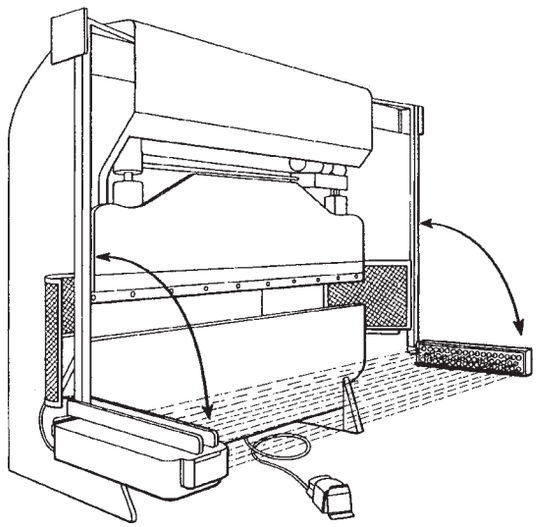
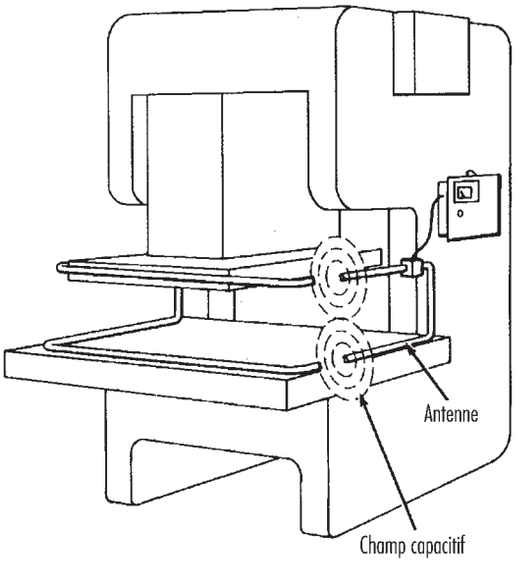


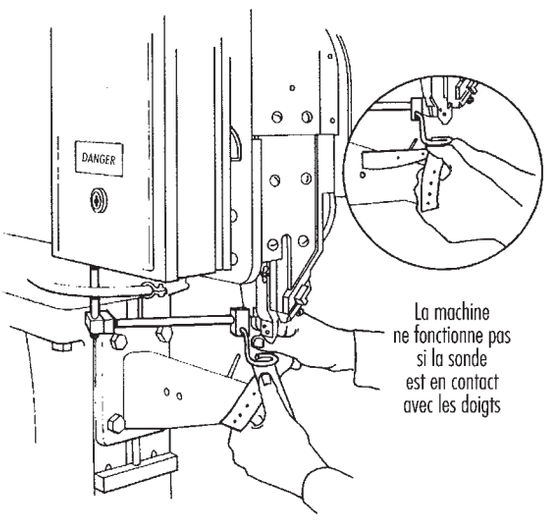
Figure 58.30 • Dispositif de détection de présence à fréquence radio



Les *détecteurs de présence à fréquence radio capacitifs* utilisent un faisceau d'ondes radio intégré au circuit de commande. Si le champ capacitif est interrompu, la machine s'arrête ou refuse de démarrer. Ces dispositifs devraient être réservés aux machines qui peuvent être mises à l'arrêt avant que le travailleur n'atteigne la zone dangereuse. Ils imposent de doter la machine d'un embrayage à friction ou d'un autre système d'arrêt fiable. La figure 58.30 montre un détecteur de ce type monté sur une presse.

Les *détecteurs électromécaniques* possèdent une sonde ou une barre de contact qui descend jusqu'à une distance prédéterminée lorsque l'opérateur enclenche le cycle de la machine. Si un obstacle empêche cette barre de parcourir la totalité de sa course, le circuit de commande refuse d'enclencher le cycle de la machine. La

Figure 58.31 • Détecteur électromécanique sur une machine à poser des œillets



1.2.4 Vérifications dimensionnelles.
1.2.4.1 L'accès à la zone de travail ne doit être possible qu'après l'arrêt de tous les mouvements.
1.2.4.2 Il faut éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
1.2.5 Réglages.
1.2.5.1 Si des mouvements sont exécutés pendant un réglage alors que les protecteurs pour le mode de fonctionnement normal sont retirés, l'opérateur doit être protégé par d'autres moyens.
1.2.5.2 Aucun mouvement ou changement de mouvement dangereux ne doit pouvoir être déclenché à la suite d'un ordre défectueux ou incorrect.
1.2.6 Programmation.
1.2.6.1 Aucun mouvement présentant un risque pour les personnes présentes dans la zone de travail ne doit pouvoir être déclenché pendant la programmation.
1.2.7 Incidents de production.
1.2.7.1 Il faut éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
1.2.7.2 Les déplacements ou l'enlèvement de la pièce ou des débris ne doivent pas provoquer de mouvements ou de situations dangereux.
1.2.7.3 Lorsque l'exécution de mouvements est nécessaire alors que les protecteurs pour le mode de fonctionnement normal sont retirés, ces mouvements doivent être uniquement du type prescrit, et ils ne doivent être exécutés que pendant la période prescrite et lorsqu'il est possible de garantir qu'aucune partie du corps ne se trouve dans ces zones dangereuses.
1.2.8 Recherche de pannes.
1.2.8.1 L'accès aux zones dangereuses des mouvements automatiques doit être impossible.
1.2.8.2 Il faut éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
1.2.8.3 Lors de la manipulation de la pièce défectueuse, tout mouvement de la machine doit être impossible.
1.2.8.4 Il faut éviter les blessures par bris ou chute d'une pièce de la machine.
1.2.8.5 Si, au cours du dépannage, l'exécution de mouvements est nécessaire alors que les protecteurs pour le mode de fonctionnement normal sont retirés, ces mouvements doivent être uniquement du type prescrit, et ils ne doivent être exécutés que pendant la période prescrite et lorsqu'il est possible de garantir qu'aucune partie du corps ne se trouve dans ces zones dangereuses.
1.2.9 Dysfonctionnement et réparation de la machine.
1.2.9.1 La machine ne doit pas pouvoir démarrer.
1.2.9.2 Il doit être possible de manipuler sans danger les différentes parties de la machine manuellement ou à l'aide d'outils.
1.2.9.3 Il ne faut pas qu'il soit possible de toucher des parties sous tension de la machine.
1.2.9.4 Il faut éviter les blessures dues aux émissions de produits liquides ou gazeux.

2. Fraiseuses

2.1 Mode de fonctionnement normal

2.1.1 La zone de travail doit être protégée de manière qu'il soit impossible de placer les mains dans les zones dangereuses des mouvements automatiques ou de s'avancer jusqu'à ces zones, volontairement ou non.
2.1.2 L'enlèvement des copeaux ne doit pas occasionner de blessures dues aux copeaux ou aux parties en mouvement de la machine.
2.1.3 Il faut éviter les blessures dues à un accès aux systèmes d'entraînement.
Il faut éviter les projections de pièces ou de parties de pièces qui pourraient blesser les opérateurs ou les tiers.
Causes possibles:
- blocage insuffisant;
- effort de coupe excessif;
- choc avec l'outil ou des parties de la machine;
- rupture de la pièce;
- défaut des dispositifs de blocage;
- panne électrique.

2.1.4 Il faut éviter les blessures par projection de dispositifs de blocage de la pièce.
2.1.5 Il faut éviter les blessures par projection de copeaux.
2.1.6 Il faut éviter les blessures par projection d'outils ou de parties d'outils.
Causes possibles:
- défauts du matériau;
- vitesse de rotation excessive;
- effort de coupe excessif;
- choc avec la pièce ou des parties de la machine;
- insuffisance de blocage ou de serrage;
- panne électrique.

2.2 Modes de fonctionnement particuliers

2.2.1 Changement de pièces.
2.2.1.1 Lorsqu'on utilise des dispositifs de blocage motorisés, il ne doit pas être possible que des parties du corps soient prises entre les parties de ces dispositifs, pendant leur fermeture, et la pièce.
2.2.1.2 Il faut éviter la mise en marche d'un mouvement (poupée, axe) à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
2.2.1.3 La pièce doit pouvoir être manipulée sans danger manuellement ou à l'aide d'outils.

2.2.2 Changement d'outils.
2.2.2.1 Il faut éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
2.2.2.2 Il faut éviter que les doigts soient emprisonnés lors de la mise en place des outils.
2.2.3 Vérifications dimensionnelles.
2.2.3.1 L'accès à la zone de travail ne doit être possible qu'après l'arrêt de tous les mouvements.
2.2.3.2 Il faut éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
2.2.4 Réglages.
2.2.4.1 Si des mouvements sont exécutés pendant un réglage alors que les protecteurs pour le mode de fonctionnement normal sont retirés, l'opérateur doit être protégé par d'autres moyens.
2.2.4.2 Aucun mouvement ou changement de mouvement dangereux ne doit pouvoir être déclenché à la suite d'un ordre défectueux ou incorrect.
2.2.5 Programmation.
2.2.5.1 Aucun mouvement présentant un risque pour les personnes présentes dans la zone de travail ne doit pouvoir être déclenché pendant la programmation.
2.2.6 Incidents de production.
2.2.6.1 Il faut éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
2.2.6.2 Les déplacements ou l'enlèvement de la pièce ou des débris ne doivent pas provoquer de mouvements ou de situations dangereux.
2.2.6.3 Lorsque l'exécution de mouvements est nécessaire alors que les protecteurs pour le mode de fonctionnement normal sont retirés, ces mouvements doivent être uniquement du type prescrit, et ils ne doivent être exécutés que pendant la période prescrite et lorsqu'il est possible de garantir qu'aucune partie du corps ne se trouve dans ces zones dangereuses.
2.2.7 Recherche de pannes.
2.2.7.1 L'accès aux zones dangereuses des mouvements automatiques doit être impossible.
2.2.7.2 Il faut éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
2.2.7.3 Lors de la manipulation de la pièce défectueuse, tout mouvement de la machine doit être impossible.
2.2.7.4 Il faut éviter les blessures par bris ou chute d'une pièce de la machine.
2.2.7.5 Si, au cours du dépannage, l'exécution de mouvements est nécessaire alors que les protecteurs pour le mode de fonctionnement normal sont retirés, ces mouvements doivent être uniquement du type prescrit, et il ne doivent être exécutés que pendant la période prescrite et lorsqu'il est possible de garantir qu'aucune partie du corps ne se trouve dans ces zones dangereuses.
2.2.8 Dysfonctionnement et réparation de la machine.
2.2.8.1 La machine ne doit pas pouvoir démarrer.
2.2.8.2 Il doit être possible de manipuler sans danger les différentes parties de la machine manuellement ou à l'aide d'outils.
2.2.8.3 Il ne faut pas qu'il soit possible de toucher des parties sous tension de la machine.
2.2.8.4 Il faut éviter les blessures dues aux émissions de produits liquides ou gazeux.

3. Centres d'usinage

3.1 Mode de fonctionnement normal

3.1.1 La zone de travail doit être protégée de manière qu'il soit impossible de placer les mains dans les zones dangereuses des mouvements automatiques ou de s'avancer jusqu'à ces zones, volontairement ou non.
3.1.2 Le magasin à outils doit être protégé de manière qu'il soit impossible de placer les mains dans les zones dangereuses des mouvements automatiques ou de s'avancer jusqu'à ces zones, volontairement ou non.
3.1.3 Le magasin à pièces doit être protégé de manière qu'il soit impossible de placer les mains dans les zones dangereuses des mouvements automatiques ou de s'avancer jusqu'à ces zones, volontairement ou non.
3.1.4 L'enlèvement des copeaux ne doit pas occasionner de blessures dues aux copeaux ou aux parties en mouvement de la machine.
3.1.5 Il convient d'éviter les blessures dues à un accès aux systèmes d'entraînement.
3.1.6 Il ne faut pas qu'il soit possible d'accéder aux zones dangereuses des convoyeurs en fonctionnement (convoyeurs à vis, etc.).
3.1.7 Il faut éviter les projections de pièces ou de parties de pièces qui pourraient blesser les opérateurs ou les tiers.
Causes possibles:
- blocage insuffisant;
- effort de coupe excessif;
- choc avec l'outil ou des parties de la machine;
- rupture de la pièce;
- défaut des dispositifs de blocage;
- remplacement par une pièce ne convenant pas;
- panne électrique.

3.1.8 Il faut éviter les blessures par projection de dispositifs de blocage de la pièce.
3.1.9 Il faut éviter les blessures par projection de copeaux.
3.1.10 Il faut éviter les blessures par projection d'outils ou de parties d'outils.
Causes possibles:
- défauts du matériau;
- vitesse de rotation excessive;
- effort de coupe excessif;
- choc avec la pièce ou des parties de la machine;
- insuffisance de blocage ou de serrage;

- projection de l'outil à l'extérieur du changeur d'outil;
- erreur dans le choix de l'outil;
- panne électrique.

3.2 Modes de fonctionnement particuliers

3.2.1 Changement de pièces.

3.2.1.1 Lorsqu'on utilise des dispositifs de blocage motorisés, il ne doit pas être possible que des parties du corps soient prises entre les parties de ces dispositifs, pendant leur fermeture, et la pièce.

3.2.1.2 Il faut éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.

3.2.1.3 La pièce doit pouvoir être manipulée sans danger manuellement ou à l'aide d'outils.

3.2.1.4 Lors d'un changement de pièces à un poste de bridage, il ne faut pas qu'il soit possible d'intervenir physiquement dans les mouvements automatiques de la machine ou du magasin à pièces. Aucun mouvement ne doit pouvoir être déclenché par la commande tant qu'une personne est présente dans la zone de bridage.
L'introduction automatique de la pièce bridée dans la machine ou le magasin à pièces ne doit avoir lieu que lorsque le poste de bridage est également équipé d'un système de protection correspondant à celui du mode de fonctionnement normal.

3.2.2 Changement d'outils sur la poupée.

3.2.2.1 Il convient d'éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.

3.2.2.2 Il convient d'éviter que les doigts soient emprisonnés lors de la mise en place des outils.

3.2.3 Changement d'outils dans le magasin.

3.2.3.1 Tout mouvement dans le magasin résultant d'une commande défectueuse ou non valide doit être impossible au cours des changements d'outils.

3.2.3.2 Il ne faut pas qu'il soit possible d'atteindre d'autres parties mobiles de la machine à partir du poste de chargement des outils.

3.2.3.3 Il ne faut pas qu'il soit possible d'atteindre les zones dangereuses pendant la poursuite du mouvement du magasin à outils ou pendant la recherche. S'ils se produisent alors que les protecteurs pour le mode de fonctionnement normal sont retirés, ces mouvements doivent être uniquement du type prescrit, et ils ne doivent être exécutés que pendant la période prescrite et lorsqu'il est possible de garantir qu'aucune partie du corps ne se trouve dans ces zones dangereuses.

3.2.4 Vérifications dimensionnelles.

3.2.4.1 L'accès à la zone de travail ne doit être possible qu'après l'arrêt de tous les mouvements.

3.2.4.2 Il faut éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.

3.2.5 Réglages.

3.2.5.1 Si des mouvements sont exécutés pendant un réglage alors que les protecteurs pour le mode de fonctionnement normal sont retirés, l'opérateur doit être protégé par d'autres moyens.

3.2.5.2 Aucun mouvement ou changement de mouvement dangereux ne doit pouvoir être déclenché à la suite d'une commande défectueuse ou non valide.

3.2.6 Programmation.

3.2.6.1 Aucun mouvement présentant un risque pour les personnes présentes dans la zone de travail ne doit pouvoir être déclenché pendant la programmation.

3.2.7 Incidents de production.

3.2.7.1 Il faut éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.

3.2.7.2 Les déplacements ou l'enlèvement de la pièce ou des débris ne doivent pas provoquer de mouvements ou de situations dangereux.

3.2.7.3 Lorsque l'exécution de mouvements est nécessaire alors que les protecteurs pour le mode de fonctionnement normal sont retirés, ces mouvements doivent être uniquement du type prescrit, et ils ne doivent être exécutés que pendant la période prescrite et lorsqu'il est possible de garantir qu'aucune partie du corps ne se trouve dans ces zones dangereuses.

3.2.8 Recherche de pannes.

3.2.8.1 L'accès aux zones dangereuses des mouvements automatiques doit être impossible.

3.2.8.2 Il faut éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.

3.2.8.3 Lors de la manipulation de la pièce défectueuse, tout mouvement de la machine doit être impossible.

3.2.8.4 Il faut éviter les blessures par bris ou chute d'une pièce de la machine.

3.2.8.5 Si, au cours du dépannage, l'exécution de mouvements est nécessaire alors que les protecteurs pour le mode de fonctionnement normal sont retirés, ces mouvements doivent être uniquement du type prescrit, et ils ne doivent être exécutés que pendant la période prescrite et lorsqu'il est possible de garantir qu'aucune partie du corps ne se trouve dans ces zones dangereuses.

3.2.9 Dysfonctionnement et réparation de la machine.

3.2.9.1 La machine ne doit pas pouvoir démarrer.

3.2.9.2 Il doit être possible de manipuler sans danger les différentes parties de la machine manuellement ou à l'aide d'outils.

3.2.9.3 Il ne faut pas qu'il soit possible de toucher des parties sous tension de la machine.

3.2.9.4 Il faut éviter les blessures dues aux émissions de produits liquides ou gazeux.

4. Meuleuses

4.1 Mode de fonctionnement normal

4.1.1 La zone de travail doit être protégée de manière qu'il soit impossible de placer les mains dans les zones dangereuses des mouvements automatiques ou s'avancer jusqu'à ces zones, volontairement ou non.

4.1.2 Il faut éviter les blessures dues à un accès aux systèmes d'entraînement.

4.1.3 Il faut éviter les projections de pièces ou de parties de pièces qui pourraient blesser les opérateurs ou les tiers.
Causes possibles:

- blocage insuffisant;
- effort de coupe excessif;
- vitesse de rotation excessive;
- choc avec l'outil ou des parties de la machine;
- rupture de la pièce;
- défaut des dispositifs de blocage;
- panne électrique.

4.1.4 Il faut éviter les blessures par projection de dispositifs de blocage de la pièce.
4.1.5 Il faut éviter les blessures ou les feux dus aux étincelles.
4.1.6 Il faut éviter les blessures par projection de fragments de meules.
Causes possibles:

- vitesse de rotation excessive;
- effort de coupe excessif;
- défauts du matériau;
- choc avec la pièce ou des parties de la machine;
- blocage défectueux (flasques);
- erreur dans le choix de la meule.

4.2 Modes de fonctionnement particuliers

4.2.1 Changement de pièces.
4.2.1.1 Lorsqu'on utilise des dispositifs de blocage motorisés, il ne doit pas être possible que des parties du corps soient prises entre les parties de ces dispositifs pendant leur fermeture et la pièce.
4.2.1.2 Il faut éviter la mise en marche d'un mouvement d'avance à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
4.2.1.3 Il faut éviter les blessures qui pourraient être causées par la rotation de la meule pendant les manipulations de la pièce.
4.2.1.4 Il faut éviter les blessures par éclatement de la meule.
4.2.1.5 La pièce doit pouvoir être manipulée sans danger manuellement ou à l'aide d'outils.
4.2.2 Changement d'outils (changement de meule).
4.2.2.1 Il faut éviter la mise en marche d'un mouvement d'avance à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
4.2.2.2 Il faut éviter les blessures qui pourraient être causées par la rotation de la meule pendant les opérations de mesure.
4.2.2.3 Il faut éviter les blessures par éclatement de la meule.
4.2.3 Vérifications dimensionnelles.
4.2.3.1 Il faut éviter la mise en marche d'un mouvement d'avance à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
4.2.3.2 Il faut éviter les blessures qui pourraient être causées par la rotation de la meule pendant les opérations de mesure.
4.2.3.3 Il faut éviter les blessures par éclatement de la meule.
4.2.4. Réglages.
4.2.4.1 Si des mouvements sont exécutés pendant un réglage alors que les protecteurs pour le mode de fonctionnement normal sont retirés, l'opérateur doit être protégé par d'autres moyens.
4.2.4.2 Aucun mouvement ou changement de mouvement dangereux ne doit pouvoir être déclenché à la suite d'un ordre défectueux ou incorrect.
4.2.5 Programmation.
4.2.5.1 Aucun mouvement présentant un risque pour les personnes présentes dans la zone de travail ne doit pouvoir être déclenché pendant la programmation.
4.2.6 Incidents de production.
4.2.6.1 Il faut éviter la mise en marche d'un mouvement d'avance à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
4.2.6.2 Les déplacements ou l'enlèvement de la pièce ou des débris ne doivent pas provoquer de mouvements ou de situations dangereux.
4.2.6.3 Lorsque l'exécution de mouvements est nécessaire alors que les protecteurs pour le mode de fonctionnement normal sont retirés, ces mouvements doivent être uniquement du type prescrit, et ils ne doivent être exécutés que pendant la période prescrite et lorsqu'il est possible de garantir qu'aucune partie du corps ne se trouve dans ces zones dangereuses.
4.2.6.4 Il faut éviter les blessures qui pourraient être causées par la rotation de la meule.
4.2.6.5 Il faut éviter les blessures par éclatement de la meule.
4.2.7 Recherche de pannes.
4.2.7.1 L'accès aux zones dangereuses des mouvements automatiques doit être impossible.
4.2.7.2 Il faut éviter la mise en marche d'un mouvement à la suite d'un ordre défectueux ou de l'introduction d'un ordre incorrect.
4.2.7.3 Lors de la manipulation de la pièce défectueuse, tout mouvement de la machine doit être impossible.
4.2.7.4 Il faut éviter les blessures par bris ou chute d'une pièce de la machine.
4.2.7.5 L'opérateur ne doit pas pouvoir être blessé par un contact avec la meule en rotation ou par l'éclatement de cette dernière.
4.2.7.6 Si, au cours du dépannage, l'exécution de mouvements est nécessaire alors que les protecteurs pour le mode de fonctionnement normal sont retirés, ces mouvements doivent être uniquement du type prescrit, et ils ne doivent être exécutés que pendant la période prescrite et lorsqu'il est possible de garantir qu'aucune partie du corps ne se trouve dans ces zones dangereuses.
4.2.8 Dysfonctionnement et réparation de la machine.
4.2.8.1 La machine ne doit pas pouvoir démarrer.
4.2.8.2 Il doit être possible de manipuler sans danger les différentes parties de la machine manuellement ou à l'aide d'outils.
4.2.8.3 Il ne faut pas qu'il soit possible de toucher des parties sous tension de la machine.
4.2.8.4 Il faut éviter les blessures dues aux émissions de produits liquides ou gazeux.

Le personnel

Les dispositions à envisager pour rendre sûres les machines-outils doivent prendre en compte à la fois les personnes intervenant dans les différents modes de fonctionnement et les tiers. Ces derniers comprennent les personnes indirectement concernées par la machine, comme les contremaîtres, les inspecteurs, les aides assurant la manutention des matériaux et les travaux de démontage, ainsi que les visiteurs et autres.

Les conditions et les mesures de sécurité pour les accessoires de machines

Les interventions dans le cadre des modes de fonctionnement particuliers nécessitent des accessoires spécifiques pour assurer l'exécution du travail dans des conditions de sécurité. Le premier type d'accessoires comprend les matériels et équipements employés pour intervenir dans le processus automatique sans que l'opérateur soit obligé d'accéder à une zone dangereuse. Ces accessoires comprennent: 1) les crochets et pinces à copeaux, qui permettent d'enlever ou d'arracher les copeaux de la zone d'usinage à travers les ouvertures aménagées dans les capots de protection; 2) les outils de maintien des pièces, qui servent à l'insertion ou au retrait manuel des pièces dans un cycle automatique.

Certains modes de fonctionnement particuliers, comme les travaux de réparation ou de maintenance, nécessitent une intervention du personnel dans le système. On dispose également dans ces cas d'une grande variété d'accessoires de machines destinés à accroître la sécurité au travail, comme les dispositifs de manutention pour le changement des grosses meules sur les meuleuses ou les élingues spéciales servant au démontage ou à l'installation de pièces lourdes lors des révisions des machines. Ces dispositifs représentent un deuxième type d'accessoires de machines destinés à accroître la sécurité au travail dans les modes de fonctionnement particuliers. On peut considérer que les systèmes de commande du fonctionnement particulier en font également partie. Ces accessoires permettent d'effectuer sans danger certains travaux particuliers, par exemple les dispositifs mis en place sur les axes d'une machine lorsque des mouvements d'avance sont nécessaires, alors que les dispositifs de protection sont ouverts.

Ces systèmes de commande du fonctionnement particulier doivent répondre à des critères de sécurité spécifiques. Ils doivent par exemple garantir que seul le mouvement requis est effectué, qu'il se déroule de la manière souhaitée, et seulement pendant la durée voulue. Ces systèmes doivent donc être conçus pour éviter qu'une action erronée n'entraîne des mouvements ou des situations présentant des dangers.

Les équipements servant à accroître le degré d'automatisation d'une installation peuvent être considérés comme un troisième type d'accessoires de machines destinés à améliorer la sécurité au travail. Des opérations précédemment manuelles sont désormais effectuées automatiquement par la machine en fonctionnement normal, grâce à des équipements comme les chargeurs à portique qui changent automatiquement les pièces sur les machines-outils. Il est relativement facile de sécuriser le fonctionnement automatique normal, parce qu'il n'est pas nécessaire que l'opérateur intervienne dans le déroulement des événements et qu'il demeure possible d'empêcher d'éventuelles interventions en prévoyant des dispositifs de sécurité.

Les conditions et les mesures de sécurité pour l'automatisation des machines-outils

L'automatisation n'a malheureusement pas éliminé les accidents dans les installations de production. Les études montrent simplement qu'ils ont été transférés du fonctionnement normal au fonctionnement particulier, essentiellement parce que l'automatisation du fonctionnement normal a supprimé la nécessité d'intervenir en cours de production et que le personnel n'est donc plus exposé. En revanche, les machines à haut degré d'automatisation sont des systèmes complexes et difficiles à analyser en cas de défauts. Même les spécialistes chargés de remédier à ces défauts ne sont pas toujours en mesure de le faire sans s'exposer à un accident. Les logiciels nécessaires pour piloter ces machines toujours plus perfectionnées augmentent en volume et en complexité, de sorte qu'un nombre croissant d'ingénieurs électriciens et d'ingénieurs chargés des mises en service sont victimes d'accidents. Il n'existe pas de logiciels parfaits, et les modifications qu'on leur apporte entraînent souvent ailleurs d'autres changements, aussi imprévus qu'indésirables. Pour que la sécurité ne soit pas affectée, il convient d'éviter que des influences extérieures ou des défaillances de composants n'entraînent des comportements défectueux et dangereux. Cette condition ne peut être remplie que si le circuit de sécurité est conçu de manière aussi simple que possible et séparé du reste du système de commande. En outre, les éléments ou sous-ensembles utilisés dans les circuits de sécurité doivent être à sécurité intégrée.

Il appartient au concepteur de mettre au point des systèmes répondant aux normes de sécurité. Il est indispensable qu'il tienne soigneusement compte des procédures de travail requises, y compris les modes de fonctionnement particuliers. Des analyses devront être effectuées pour déterminer les procédures de travail sûres à adopter, et le personnel d'exploitation devra se familiariser avec leur emploi. Dans la plupart des cas, un système de commande du fonctionnement particulier sera nécessaire. Le système de commande assure généralement la surveillance ou la régulation d'un mouvement et aucun autre mouvement ne doit être déclenché simultanément (parce que ce n'est pas nécessaire pour cette tâche et que, par conséquent, l'opérateur ne s'y attend pas). Le système de commande n'assure pas nécessairement les mêmes fonctions dans les différents modes de fonctionnement particulier.

Les conditions et les mesures de sécurité dans les modes de fonctionnement normal et particulier

Le fonctionnement normal

La définition d'objectifs en matière de sécurité ne devrait pas faire obstacle au progrès technique, puisqu'il est possible de choisir des solutions adaptées. L'emploi de machines-outils à commande numérique impose de recourir massivement à l'analyse et à l'évaluation des risques et aux concepts de sécurité. Plusieurs objectifs de sécurité, ainsi que les solutions envisageables correspondantes, sont décrits plus en détail dans les lignes qui suivent.

L'objectif de sécurité

- Interdire de pénétrer ou d'introduire les mains dans les zones dangereuses pendant l'exécution de mouvements automatiques.

Les solutions possibles

- Disposer des barrières mécaniques pour éviter qu'il soit possible de pénétrer ou d'introduire les mains dans les zones dangereuses.
- Mettre en place des dispositifs de sécurité réagissant à l'approche (cellules et tapis de détection) et permettant une mise à l'arrêt sûre des machines en cas d'intervention ou d'entrée dans la zone.
- Ne permettre d'accéder aux machines (ou à proximité) ou d'introduire les mains dans les zones dangereuses que lorsque l'ensemble du système est sécurisé, par exemple par la pose de dispositifs de verrouillage sur les portes d'accès.

L'objectif de sécurité

- Supprimer la possibilité d'accidents corporels par libération d'énergie (projection de pièces ou énergie rayonnée).

La solution possible
- Empêcher l'émission d'énergie à partir de la zone dangereuse, par exemple en installant un capot de sécurité de dimensions appropriées.

Le fonctionnement particulier
Les interfaces entre les deux modes de fonctionnement, normal et particulier (dispositifs de verrouillage de portes, cellules et tapis de détection), sont nécessaires pour permettre au système de contrôle de la sécurité de reconnaître automatiquement la présence de personnes. On décrit dans les lignes qui suivent certains modes de fonctionnement particuliers (réglage, programmation) des machines-outils à commande numérique qui nécessitent un examen direct des mouvements à l'emplacement où ils sont exécutés.

Les objectifs de sécurité
- L'exécution des mouvements ne doit pas présenter de dangers pour les personnes concernées. Ils seront exécutés de la manière et à la vitesse prévues et ne se prolongeront pas au-delà du temps prescrit.
- Ils seront déclenchés uniquement lorsqu'on aura l'assurance qu'aucune partie du corps humain ne se trouve dans la zone dangereuse.

La solution possible
- Installer des systèmes de commande du fonctionnement particulier ne permettant que des mouvements contrôlables et exécutables déclenchés par des boutons-poussoirs manuels du type «à acquittement». La vitesse des mouvements se trouve ainsi réduite à un niveau de sécurité, à la condition que l'énergie ait été réduite par un transformateur d'isolement ou un autre dispositif de surveillance similaire.

Conditions requises pour les systèmes de commande concernant la sécurité
L'une des caractéristiques d'un système de commande concernant la sécurité doit être de garantir l'exécution de la fonction sécuritaire à chaque apparition d'un défaut, de manière à faire passer les processus d'un état d'insécurité à un état de sécurité.

Les objectifs de sécurité
- Un défaut dans le système de commande de la sécurité ne doit pas provoquer de situation dangereuse.
- Un défaut dans le système de commande de la sécurité doit être identifié (immédiatement ou par vérification périodique).

Les solutions possibles
- Mettre en place une configuration redondante et diversifiée de systèmes de contrôle électromécaniques, y compris des circuits de test.
- Mettre en place un ensemble redondant et diversifié de systèmes de contrôle par microprocesseurs, élaborés par des équipes différentes. Cette approche est considérée comme la meilleure actuellement, par exemple dans le cas des cellules de détection.

Conclusion
Il apparaît que l'on ne pourra pas arrêter la tendance à une augmentation des accidents dans les deux modes de fonctionnement, normal et particulier, si l'on ne dispose pas d'un concept de sécurité clair et dépourvu d'ambiguïté. Ce constat doit être pris en compte dans la préparation des réglementations et directives de sécurité. De nouvelles directives sous la forme d'objectifs de sécurité sont nécessaires pour dégager des solutions novatrices. Cet objectif permet aux concepteurs de choisir la solution la mieux adaptée à chaque cas et également d'établir, d'une manière suffisamment simple, les caractéristiques de sécurité de leurs machines en décrivant une solution pour chaque objectif de sécurité. Cette solution peut alors être comparée à d'autres solutions existantes et admises, et si elle est meilleure ou à tout le moins équivalente, la nouvelle solution peut être adoptée. On évite ainsi que les progrès ne soient freinés par des réglementations trop restrictives.

LES PRINCIPES DE SÉCURITÉ POUR LES ROBOTS INDUSTRIELS

Toni Retsch, Guido Schmitter et Albert Marty

Les robots sont présents dans tous les secteurs industriels où une productivité élevée est exigée. Leur utilisation impose toutefois la conception et la mise en œuvre des commandes de sécurité appropriées pour éviter d'exposer à des dangers le personnel de production, les programmeurs, les spécialistes de la maintenance et les ingénieurs système.

Pourquoi les robots industriels sont-ils dangereux?
Les robots peuvent être définis comme des «machines automatiques mobiles programmables et capables de fonctionner sans interface humaine ou avec une interface réduite». Ces types de machines sont actuellement utilisés dans des applications très diverses des secteurs industriel et médical, y compris la formation. Les robots industriels sont de plus en plus souvent affectés à des fonctions essentielles comme les nouvelles stratégies de fabrication (FAO, JAT, production allégée, etc.) dans des installations complexes. Le nombre et l'étendue des applications, ainsi que la complexité des équipements et installations créent un certain nombre de risques, notamment:

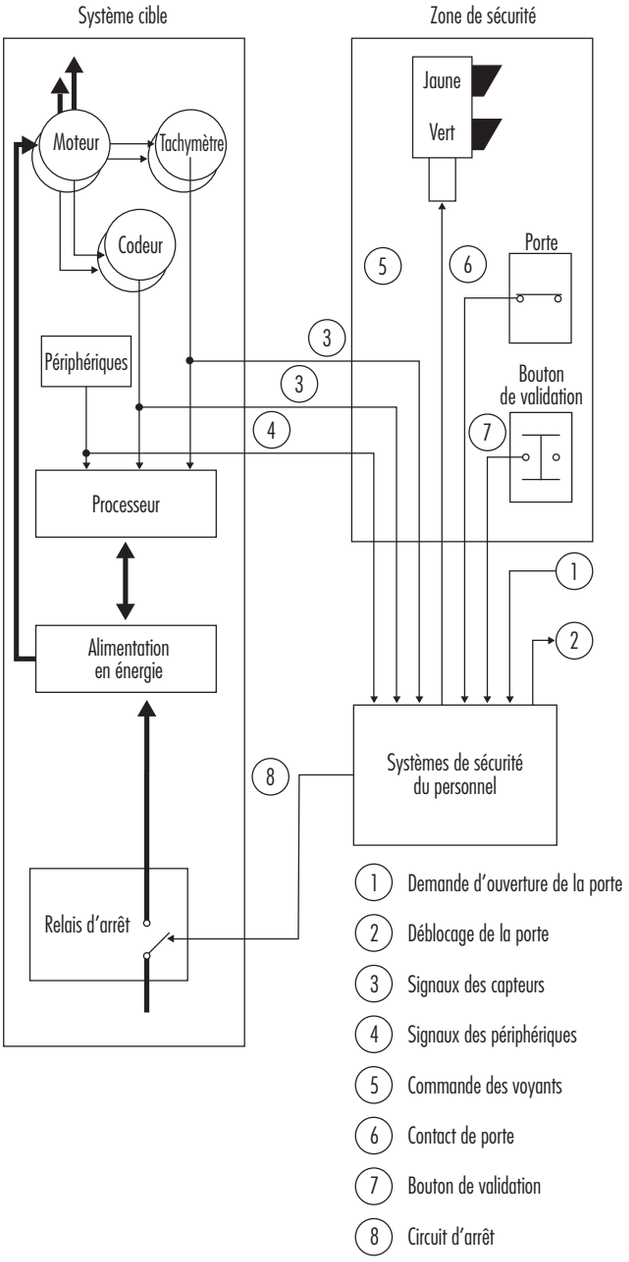
- des mouvements ou séquences de mouvements presque impossibles à suivre, dans la mesure où les mouvements rapides d'un robot dans son rayon d'action empiètent fréquemment sur ceux d'autres machines ou équipements;
- un dégagement d'énergie provoqué par la projection de pièces ou les émissions de rayonnements laser ou de jets d'eau;
- une entière liberté de programmation, tant en direction qu'en vitesse;
- une sensibilité à l'influence de perturbations extérieures (par exemple, compatibilité électromagnétique);
- les facteurs humains.

Des études effectuées au Japon indiquent que plus de 50% des accidents du travail impliquant des robots sont attribuables à des défauts des circuits électroniques du système de contrôle. Selon ces mêmes études, la part de l'erreur humaine est inférieure à 20%. On peut logiquement en conclure que les dangers causés par des défauts du système ne peuvent pas être évités par des mesures comportementales prises par les personnes. Les concepteurs et les opérateurs doivent donc fournir et mettre en œuvre des mesures de sécurité techniques (voir figure 58.82).

Les accidents et les modes de fonctionnement
Les accidents mortels impliquant des robots sont apparus au début des années quatre-vingt. Les statistiques et les enquêtes montrent que la majorité des incidents et accidents ne surviennent pas en fonctionnement normal, c'est-à-dire pendant l'exécution automatique du travail en cause. Avec ces types de machines et d'installations industrielles robotisées, ce sont les modes de fonctionnement particuliers qui sont les plus préoccupants, comme la mise en service, les réglages, la programmation, les essais de production, les vérifications, les recherches de pannes ou la main-

Figure 58.82 • Système de commande pour le réglage d'un robot de soudage mobile

Figure 58.83 • Diagramme en blocs pour un système de sécurité du personnel



tenance. En effet, dans ces modes de fonctionnement, des personnes sont habituellement présentes dans les zones dangereuses. Le concept de sécurité doit protéger le personnel des événements dangereux dans ce type de situation.

Les normes de sécurité internationales

La directive 89/392/CEE de 1989 du Conseil de l'Union européenne sur les machines (voir notamment l'article «Les principes de sécurité pour les machines-outils à commande numérique» dans le présent chapitre) définit les principales exigences en matière de santé et de sécurité en ce qui concerne les machines. Au sens de cette directive, remplacée par la directive 98/37/CE, une machine est un ensemble de pièces et d'organes liés entre eux dont au moins un est mobile et possède donc une fonction. S'agissant des robots industriels, il convient de noter que c'est le système entier, et non pas un élément particulier de la machine, qui doit satisfaire aux prescriptions de sécurité et être équipé des dispositifs de sécurité voulus. L'analyse et l'évaluation des risques sont des méthodes qui permettent de vérifier que ces exigences sont satisfaites (voir figure 58.83).

Les conditions et les mesures de sécurité en fonctionnement normal

L'emploi de la technologie des robots pose des problèmes très délicats en ce qui concerne l'analyse et l'évaluation des risques et les concepts de sécurité. Les exemples et suggestions qui suivent ne sont donc donnés qu'à titre indicatif:

1. Compte tenu d'un objectif de sécurité consistant à rendre impossible de pénétrer ou d'introduire les mains dans les zones dangereuses où des mouvements automatiques sont exécutés, on peut notamment préconiser les solutions suivantes:
   - Disposer des barrières mécaniques pour rendre impossible de pénétrer ou d'introduire les mains dans les zones dangereuses.
   - Employer des dispositifs de sécurité réagissant à l'approche (cellules et tapis de détection) et permettant une mise à l'arrêt sûre des machines lorsqu'on intervient ou qu'on pénètre dans la zone dangereuse.
   - Ne permettre de pénétrer ou d'introduire les mains que lorsque l'ensemble du système est sécurisé, par exemple grâce à l'installation de dispositifs de verrouillage sur les portes d'accès.
2. Compte tenu d'un objectif de sécurité consistant à empêcher qu'une personne ne soit blessée par un dégagement d'énergie (projection de pièces ou énergie rayonnée), on peut proposer les solutions suivantes:
   - Concevoir le système de manière à éviter tout dégagement d'énergie (par exemple, raccordements dimensionnés de manière adéquate, systèmes passifs de verrouillage des préhenseurs dans les mécanismes de changement de préhenseur, etc.).
   - Empêcher l'émission d'énergie à partir de la zone dangereuse, par exemple en installant un capot de sécurité de dimensions appropriées.

3. Des interfaces entre les deux modes de fonctionnements, normal et particulier (dispositifs de verrouillage de portes, cellules et tapis de détection) sont nécessaires pour permettre au système de commande de sécurité de reconnaître automatiquement la présence de personnes.

Les conditions et les mesures de sécurité dans les modes de fonctionnement particuliers

Certains modes de fonctionnement particuliers (réglage, programmation) des robots industriels nécessitent un examen direct des mouvements à l'emplacement où ils sont exécutés. L'objectif de sécurité correspondant est que l'exécution des mouvements ne doit pas présenter de dangers pour les personnes concernées. Il faut que ces mouvements:

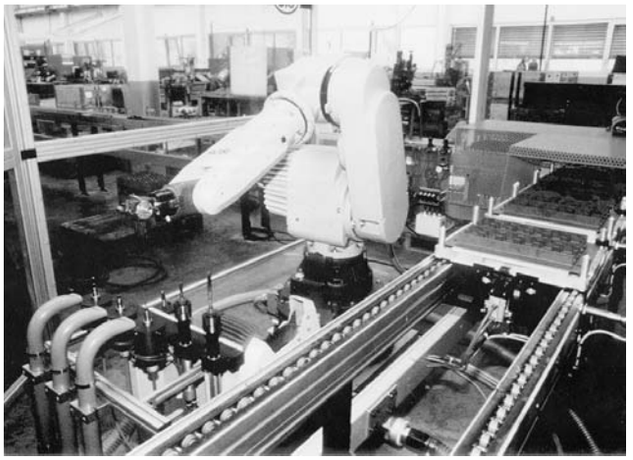
- soient exécutés uniquement de la manière et à la vitesse prévues;
- ne se prolongent pas au-delà du temps prescrit;
- soient déclenchés uniquement lorsqu'on aura l'assurance qu'aucune partie du corps humain ne se trouve dans la zone dangereuse.

Pour répondre à cet objectif, il est conseillé notamment d'installer des systèmes de commande du mode de fonctionnement particulier ne permettant que des mouvements contrôlables et exécutables déclenchés par des commandes «à acquittement». La vitesse des mouvements se trouve ainsi réduite à un niveau de sécurité (réduction de l'énergie par un transformateur d'isolement ou emploi d'un autre équipement de surveillance à sécurité intégrée) et l'état de sécurité est validé avant que la commande puisse être activée (voir figure 58.84).

Les conditions requises pour les systèmes de commande de sécurité

Une des caractéristiques d'un système de commande de sécurité doit être de garantir l'exécution de la fonction sécuritaire à chaque apparition d'un défaut. Les machines robotisées industrielles devraient passer presque instantanément d'un état d'insécurité à un état de sécurité. Les mesures de sécurité nécessaires dans ce but comprennent les objectifs de sécurité suivants:

Figure 58.84 • Robot industriel à six degrés de liberté placé dans une cage de sécurité avec des ouvertures pour le passage des matériaux



- Un défaut dans le système de contrôle ne doit pas provoquer de situation dangereuse.
- Un défaut dans le système de contrôle doit être identifié (immédiatement ou par vérification périodique).

Les solutions suggérées pour la mise en place de systèmes de contrôle fiables sont les suivantes:

- mettre en place une configuration redondante et diversifiée des systèmes de contrôle électromécaniques, y compris des circuits de test;
- mettre en place un ensemble redondant et diversifié de systèmes de contrôle par microprocesseurs, élaborés par des équipes différentes. Cette approche moderne est considérée comme la meilleure actuellement, par exemple dans le cas des cellules de détection.

Les objectifs de sécurité pour la construction et l'utilisation de robots industriels

Les constructeurs et les utilisateurs de robots industriels sont tenus d'installer des systèmes de contrôle modernes. Indépendamment de la responsabilité légale, on peut considérer qu'il existe aussi une obligation morale de faire de la technologie robotique une technologie sûre.

Le mode de fonctionnement normal

Les conditions de sécurité suivantes devraient être assurées lorsque des machines robotisées fonctionnent en mode normal:

- Le champ d'intervention du robot et les zones de travail utilisées par les équipements périphériques doivent être protégés de manière à interdire le passage des mains ou des personnes dans des zones rendues dangereuses par les mouvements automatiques.
- On doit prévoir des protections pour éviter les dommages dus aux projections de pièces ou d'outils.
- Il ne faut pas que des personnes puissent être blessées par des pièces, des outils ou des pièces à usiner éjectés par le robot ou par une libération d'énergie à la suite d'un défaut ou d'une interruption de l'alimentation du préhenseur, d'une vitesse excessive, de collisions ou de défauts des pièces à usiner.
- Il ne faut pas que des personnes puissent être blessées par une libération d'énergie ou par des pièces éjectées par des équipements périphériques.
- Les orifices d'introduction et de retrait doivent être conçus de manière à interdire de placer les mains ou de pénétrer dans des zones rendues dangereuses par les mouvements automatiques. Cette condition doit également être satisfaite lors du retrait des matériaux de production. Lorsque les matériaux sont introduits automatiquement dans le robot, les ouvertures d'introduction et de retrait, ainsi que le transfert des matériaux ne doivent pas créer de zone dangereuse.

Les modes de fonctionnement particuliers

Les conditions de sécurité suivantes devraient être assurées lorsque des machines robotisées fonctionnent selon des modes particuliers:

Lors d'une intervention à la suite d'une panne dans le processus de production, on devra veiller aux points suivants:

- Interdire d'introduire les mains ou de pénétrer dans les zones rendues dangereuses par les mouvements automatiques du robot ou des équipements périphériques.
- Lorsque des personnes ou des parties du corps sont exposées à des mouvements dangereux, éviter les risques dus à un comportement défectueux du système ou à l'introduction d'un ordre intempestif.

- Eviter que le déplacement ainsi que le retrait des matériaux de production ou des déchets n'occasionnent des mouvements ou des situations présentant des dangers.
- Eviter que les équipements périphériques occasionnent des blessures.
- Si des mouvements doivent être exécutés alors que les protecteurs pour le mode de fonctionnement normal sont enlevés, ces mouvements pourront être exécutés uniquement avec l'ampleur et la vitesse prescrites et uniquement pendant la période prescrite. En outre, aucune personne ou partie du corps d'une personne ne doit être présente dans la zone dangereuse.

Les conditions de sécurité ci-après doivent être assurées lors des réglages:
Aucun mouvement dangereux ne doit être déclenché par une commande défectueuse ou par l'introduction d'un ordre incorrect.

- Le remplacement de pièces du robot ou des équipements périphériques ne doit pas provoquer de mouvements ou de situations présentant des dangers.
- Si des mouvements doivent être exécutés pendant les réglages alors que les protecteurs pour le mode de fonctionnement normal sont retirés, ces mouvements pourront être exécutés uniquement avec l'ampleur et la vitesse prescrites et uniquement pendant la période prescrite. En outre, aucune personne ou partie du corps ne doit être présente dans la zone dangereuse.
- Pendant les réglages, les équipements périphériques ne doivent effectuer aucun mouvement dangereux et ne créer aucune situation dangereuse.

Les conditions de sécurité suivantes doivent être assurées pendant la programmation:
- On empêchera qu'il soit possible d'introduire les mains ou de pénétrer dans les zones rendues dangereuses par des mouvements automatiques.
- Si des mouvements doivent être exécutés alors que les protecteurs pour le mode de fonctionnement normal sont retirés, les conditions suivantes doivent être remplies:
  a) seule la commande de déplacement peut être exécutée, et uniquement aussi longtemps qu'elle est émise;
  b) seuls les mouvements contrôlables (c'est-à-dire bien visibles et à vitesse réduite) peuvent être exécutés;
  c) les mouvements ne peuvent être déclenchés que lorsqu'ils ne constituent pas un risque pour le programmeur ou d'autres personnes.
- Les équipements périphériques ne doivent pas constituer un risque pour le programmeur ou d'autres personnes.

La sécurité des opérations de test nécessite les précautions suivantes:
Il doit être impossible d'introduire les mains ou de pénétrer dans les zones rendues dangereuses par des mouvements automatiques.

- Les équipements périphériques ne doivent pas constituer une source de risque.

Pour l'inspection des machines robotisées dans des conditions de sécurité, il convient d'appliquer notamment les procédures suivantes:
- S'il est nécessaire de pénétrer dans le champ d'intervention du robot pour une inspection, cet accès ne doit être autorisé que lorsque le système est à l'état de sécurité.
- On doit éviter les risques dus à un comportement défectueux du système ou à l'introduction d'un ordre intempestif.
- Les équipements périphériques ne doivent présenter aucun danger pour le personnel d'inspection.

Comme la recherche des pannes exige souvent de mettre en marche la machine robotisée alors qu'elle se trouve dans un état potentiellement dangereux, il convient d'appliquer des procédures de travail spécifiques, assurant une sécurité, comme les mesures suivantes:
- Tout accès aux zones rendues dangereuses par des mouvements automatiques doit être interdit.
- On doit empêcher la mise en marche d'un mécanisme d'entraînement à la suite d'un ordre défectueux ou de l'introduction d'un ordre erroné.
- Lors de la manipulation d'une partie défectueuse, tout mouvement du robot doit être interdit.
- On doit empêcher les blessures par projection ou chute de parties de la machine.
- S'il est nécessaire, pendant la recherche des pannes, d'exécuter des mouvements alors que les protecteurs pour le mode de fonctionnement normal sont retirés, ces mouvements pourront être exécutés uniquement avec l'ampleur et la vitesse prescrites, et uniquement pendant la période prescrite. En outre, aucune personne ou partie du corps ne doit être présente dans la zone dangereuse.
- On doit empêcher les lésions par les équipements périphériques.

Les interventions pour corriger un défaut ou pour la maintenance peuvent également nécessiter de mettre en marche la machine alors qu'elle est dans un état d'insécurité, et nécessitent donc les précautions suivantes:
- Il doit être impossible de mettre en marche le robot.
- La manipulation des différentes pièces de la machine, manuellement ou à l'aide d'équipements auxiliaires, doit pouvoir s'effectuer sans exposition à des dangers.
- Il ne doit pas être possible d'entrer en contact avec des parties sous tension.
- On doit empêcher les lésions par émission de liquides ou de gaz.
- On doit empêcher les lésions par les équipements périphériques.

LES SYSTÈMES DE COMMANDE ÉLECTRIQUES, ÉLECTRONIQUES ET ÉLECTRONIQUES PROGRAMMABLES RELATIFS À LA SÉCURITÉ

Ron Bell

Le présent article traite de la conception et de la mise en œuvre de systèmes de commande de sécurité pour tous les types de systèmes électriques, électroniques et électroniques programmables (E/E/EP), y compris les systèmes informatisés. L'approche générale est conforme à la norme 1508 de la Commission électrotechnique internationale (CEI) (CEI, 1998).

Rappel historique

L'utilisation de systèmes informatisés, désignés par le terme générique d'Automates programmables industriels (API), pour des fonctions de sécurité, s'est développée dans les années quatre-vingt. Les principales raisons de cette tendance étaient: 1) une meilleure fonctionnalité et des avantages économiques (compte tenu surtout de la durée de vie totale de l'appareil ou du système);

2) les avantages propres à certains concepts dont l'application a été rendue possible par la technologie informatique. Dans les premiers stades de l'introduction des systèmes informatisés, un certain nombre de constatations ont été faites:

- L'introduction du contrôle par ordinateur était mal conçue et insuffisamment planifiée.
- Les prescriptions de sécurité spécifiées étaient inadaptées.
- Les procédures mises au point pour la validation des logiciels étaient inadaptées.
- La mise en place de l'installation avait été mal exécutée.
- La documentation produite était inadaptée et insuffisamment validée par rapport au contenu effectif de l'installation.
- L'efficacité des procédures d'exploitation et de maintenance prévues était insuffisante.
- L'aptitude des personnes à exécuter les tâches qui leur étaient confiées était manifestement sujette à caution.

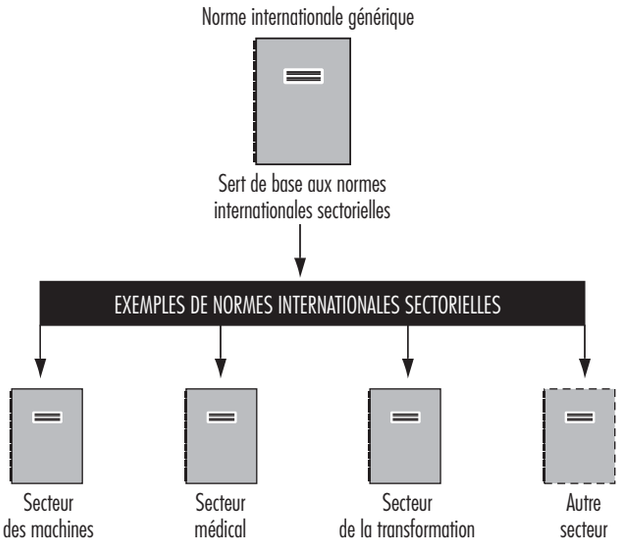
Pour remédier à cette situation, plusieurs organismes ont publié ou entrepris d'établir des guides pour une utilisation sûre de la technologie API. Au Royaume-Uni, la direction de la sécurité et de la santé (Health and Safety Executive (HSE)) a établi des guides sur les systèmes électroniques programmables employés dans les applications en rapport avec la sécurité et, en Allemagne, un projet de norme (DIN, 1990) a été publié. Au sein de la Communauté économique européenne, les prescriptions de la directive sur les machines ont constitué un premier jalon important des travaux d'harmonisation des normes européennes sur les systèmes de contrôle pour la sécurité (y compris ceux employant des API). Aux Etats-Unis, la Société américaine d'instrumentation (Instrument Society of America (ISA)) a établi une norme sur les API destinés aux industries de transformation, et le Centre pour la sécurité des processus chimiques (Center for Chemical Process Safety (CCPS)), organisme de l'Institut américain des ingénieurs chimistes (American Institute of Chemical Engineers (AIChe)), a établi des directives pour l'industrie chimique de transformation.

La CEI a entrepris un important travail de normalisation visant à élaborer une norme internationale générique pour les systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité (E/E/EP) susceptibles d'être utilisés dans des secteurs comme les industries de transformation, le secteur médical, les transports ou la construction des machines. Cette norme CEI comprend sept parties regroupées sous le titre général *CEI 1508. Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité* (CEI, 1998-2000). Ces parties sont les suivantes:

- Partie 1. Prescriptions générales.
- Partie 2. Prescriptions concernant les systèmes électriques, électroniques et électroniques programmables.
- Partie 3. Prescriptions concernant les logiciels.
- Partie 4. Définitions.
- Partie 5. Exemples de méthodes de détermination des niveaux d'intégrité de sécurité.
- Partie 6. Lignes directrices pour l'application des parties 2 et 3.
- Partie 7. Présentation des techniques et mesures.

Cette norme internationale générique est une publication CEI de référence pour la sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité, et elle aura des répercussions sur toutes les normes CEI dans tous les secteurs d'application du point de vue de la conception et de l'utilisation futures de ces systèmes. Un des principaux objectifs de ce texte est de favoriser l'élaboration de normes spécifiques pour les différents secteurs (voir figure 58.85).

Figure 58.85 • Normes génériques et normes d'application sectorielles



Les avantages et les problèmes des API

L'adoption des SEP pour les besoins de la sécurité présente de nombreux avantages potentiels, mais il a été reconnu qu'il ne serait possible de les obtenir que grâce à des méthodes de conception et d'évaluation appropriées, et cela pour plusieurs raisons: 1) un grand nombre de caractéristiques des API ne permettent pas de prédire l'intégrité de sécurité (c'est-à-dire les performances, en matière de sécurité, des systèmes assurant les fonctions de sécurité requises) avec le même niveau de confiance que celui qui a toujours caractérisé les systèmes moins complexes à base matérielle (câblés); 2) on a constaté que, bien que nécessaires, les tests effectués sur les systèmes complexes n'étaient pas suffisants à eux seuls, ce qui signifie que, même si le API assure des fonctions de sécurité relativement simples, le niveau de complexité de l'électronique programmable est nettement supérieur à celui des systèmes câblés qu'elle remplace; 3) cette complexité accrue impose de considérer avec beaucoup plus d'attention qu'auparavant les méthodes de conception et d'évaluation, de sorte que le niveau de compétences personnelles requis du personnel pour obtenir les performances voulues des systèmes liés à la sécurité est plus élevé.

Les avantages des API informatisés sont:

- possibilité d'effectuer en ligne un diagnostic beaucoup plus fréquent des composants critiques;
- possibilité de réaliser des verrouillages de sécurité perfectionnés;
- possibilité de fournir des fonctions de diagnostic et de surveillance d'état permettant d'analyser les performances de l'installation et des machines et d'en rendre compte en temps réel;
- possibilité de comparer l'état réel de l'installation avec celui d'un modèle «idéal»;
- possibilité de mieux informer les opérateurs et donc d'améliorer la prise de décisions concernant la sécurité;
- mise en œuvre de stratégies de contrôle évoluées permettant d'écarter les opérateurs des environnements dangereux ou hostiles;
- possibilité de diagnostics à distance du système de commande.

L'emploi de systèmes informatisés dans les applications de sécurité crée un certain nombre de problèmes qui doivent être traités de manière adéquate, tels que:

- les modes de défaillance sont complexes et pas toujours prévisibles;
- il est nécessaire de tester l'ordinateur, mais cette précaution ne suffit pas pour établir que les fonctions de sécurité seront exécutées avec le degré de certitude requis pour l'application;
- les microprocesseurs peuvent présenter de très faibles différences d'un lot à l'autre et avoir par conséquent un comportement distinct;
- les systèmes informatisés non protégés sont particulièrement sensibles aux interférences électriques (interférences rayonnées, crêtes de tension sur le réseau électrique, décharges électrostatiques, etc.);
- il est difficile et souvent impossible de quantifier la probabilité de défaillance des systèmes de sécurité complexes intégrant des logiciels. En l'absence d'une méthode de quantification bien établie, la vérification des logiciels repose sur des procédures et des normes décrivant les méthodes à appliquer pour la conception, la réalisation et la maintenance des logiciels.

Les systèmes de sécurité considérés

Les types de systèmes de sécurité considérés sont des systèmes électriques, électroniques et électroniques programmables (E/E/EP). Chaque système comporte un ensemble complet d'éléments, en particulier les signaux qui proviennent des détecteurs ou d'autres systèmes de saisie des données sur les équipements contrôlés et qui sont transmis par des bus de données ou d'autres voies de communication aux actionneurs ou aux autres organes de sortie (voir figure 58.86).

Le terme «dispositif électrique, électronique et électronique programmable» regroupe une grande diversité de dispositifs, répartis en trois grandes catégories:

1. Dispositifs électriques, tels que les relais électromécaniques.
2. Dispositifs électroniques, tels qu'instruments électroniques transistorisés et systèmes logiques.
3. Dispositifs électroniques programmables, qui comprennent des systèmes informatisés très divers, notamment:
   - des microprocesseurs;
   - des microcontrôleurs;
   - des contrôleurs programmables;
   - des circuits intégrés spécifiques à l'application;
   - des automates programmables;
   - d'autres dispositifs à base informatique (par exemple, détecteurs, transmetteurs et actionneurs «intelligents»).

Figure 58.86 • Système électrique, électronique et électronique programmable (E/E/EP)

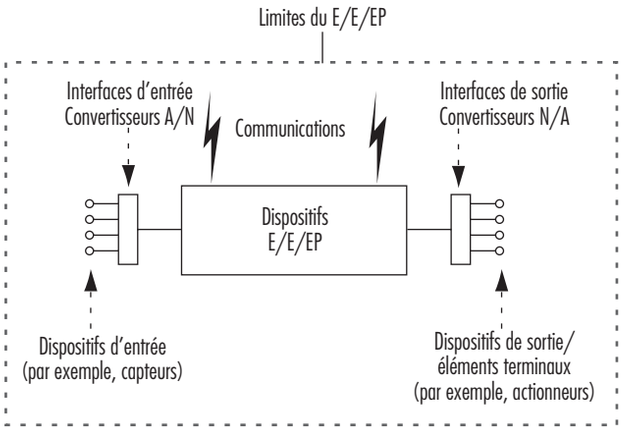
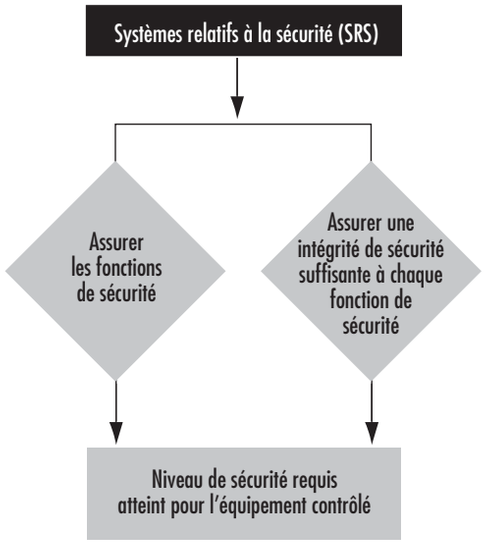


Figure 58.87 • Principales caractéristiques des systèmes relatifs à la sécurité



Par définition, un système de sécurité répond à deux objectifs:

1. Il exécute les fonctions de sécurité nécessaires pour assurer ou maintenir la sûreté des équipements contrôlés. Il doit assurer les fonctions de sécurité spécifiées pour le système. Ainsi, si la température atteint une certaine valeur *x*, la vanne *y* doit s'ouvrir pour introduire de l'eau dans une cuve.
2. Il assure, seul ou avec d'autres systèmes de sécurité, le niveau d'intégrité de sécurité nécessaire à l'exécution des fonctions de sécurité requises. Celles-ci doivent être exécutées par les systèmes de sécurité avec un niveau de confiance adapté à l'application, afin de conférer à l'équipement contrôlé le niveau de sécurité voulu.

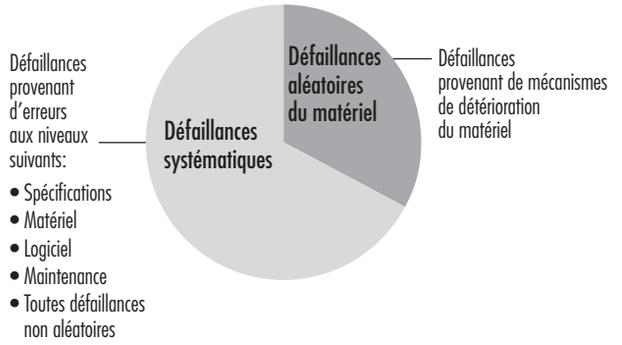
Ce concept est illustré à la figure 58.87.

Les défaillances du système

Pour obtenir un fonctionnement sûr des systèmes E/E/EP relatifs à la sécurité, il est nécessaire d'identifier les différentes causes possibles de leurs défaillances et de prendre dans chaque cas les mesures adéquates. On distingue deux catégories de défaillances, comme le montre la figure 58.88.

1. Les défaillances aléatoires du matériel sont celles qui proviennent des divers mécanismes de détérioration normale du matériel. Ces mécanismes sont nombreux et apparaissent plus ou moins rapidement selon les composants. Etant donné qu'en raison des tolérances de fabrication, les défaillances des différents composants dues à ces mécanismes apparaissent après des périodes de fonctionnement d'une durée variable, les défaillances d'un système comprenant de nombreux composants se produisent à des dates imprévisibles, c'est-à-dire de manière aléatoire. Certaines mesures de la fiabilité des systèmes, par exemple la moyenne des temps de bon fonctionnement (MTBF), sont utiles, mais elles ne concernent généralement que les défaillances aléatoires du matériel et ne tiennent pas compte des défaillances systématiques.
2. Les défaillances systématiques proviennent d'erreurs dans la conception, la réalisation ou l'utilisation d'un système qui provoquent une panne de celui-ci dans le cas d'une combinaison particulière des données qui sont entrées ou dans certains

Figure 58.88 • Catégories de défaillances



environnements. Si une défaillance du système se produit lorsqu'un ensemble de circonstances déterminé apparaît, elle se produira à nouveau chaque fois que ce même ensemble de circonstances sera réuni. Toute défaillance d'un système relatif à la sécurité n'ayant pas pour origine une défaillance aléatoire du matériel est, par définition, une défaillance systématique. Dans le cadre des systèmes E/E/EP relatifs à la sécurité, on rencontre les défaillances systématiques suivantes:

- défaillances systématiques dues à des erreurs ou à des omissions dans les caractéristiques requises des fonctions de sécurité;
- défaillances systématiques dues à des erreurs dans la conception, la fabrication, l'installation ou l'utilisation du matériel. Elles comprennent les défaillances provenant de causes environnementales et d'erreurs humaines, notamment de l'opérateur;
- défaillances systématiques dues à des défauts du logiciel;
- défaillances systématiques dues à des erreurs dans la maintenance et les modifications.

Figure 58.89 • Concepts de performances de sécurité

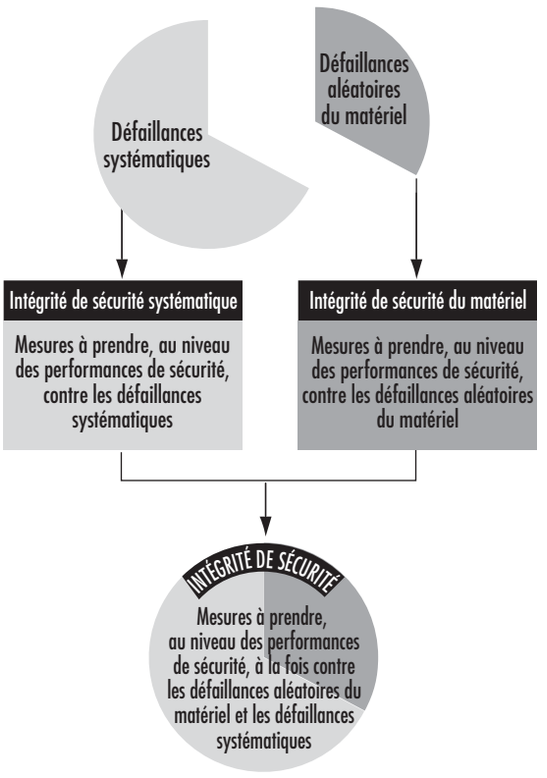
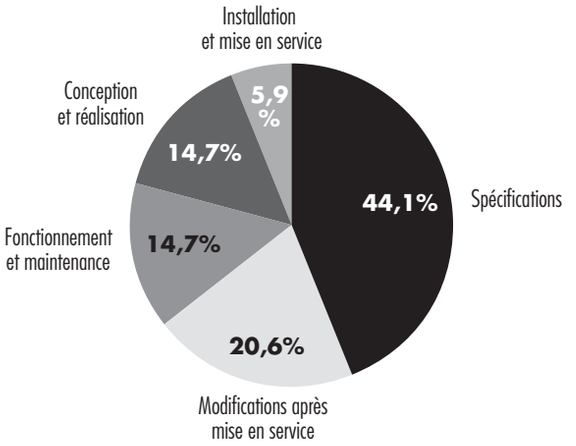


Figure 58.90 • Principales causes (étapes) des défaillances des systèmes de commande



La protection des systèmes relatifs à la sécurité

Les expressions employées pour désigner les précautions à prendre pour protéger les systèmes relatifs à la sécurité contre les défaillances aléatoires du matériel et les défaillances systématiques sont respectivement *mesures concernant l'intégrité de sécurité du matériel* et *mesures concernant l'intégrité de sécurité systématique*. Les mesures qu'un système de sécurité peut mettre en œuvre à la fois contre les défaillances aléatoires du matériel et contre les défaillances systématiques sont appelées *intégrité de sécurité*. Ces concepts sont illustrés à la figure 58.89.

Dans la norme internationale CEI 1508, on distingue quatre niveaux d'intégrité de sécurité, numérotés de 1 à 4, le niveau 1 étant le plus bas. Le niveau d'intégrité de sécurité d'un système relatif à la sécurité dépend du rôle qu'il joue pour assurer à l'équipement contrôlé le niveau de sécurité requis. Plusieurs systèmes relatifs à la sécurité peuvent être nécessaires, dont certains à base de technologie pneumatique ou hydraulique.

La conception des systèmes relatifs la sécurité

Une analyse de la direction britannique de la sécurité et de la santé (HSE) portant sur 34 incidents impliquant des systèmes de contrôle a révélé que dans près de 60% des cas la défaillance avait été «intégrée» avant la mise en service du système de sécurité (voir figure 58.90). Pour pouvoir disposer d'un système relatif à la sécurité adéquat, il est nécessaire de prendre en compte toutes les phases du cycle de vie de sécurité.

La sécurité fonctionnelle des systèmes relatifs à la sécurité ne dépend pas seulement d'une définition adéquate des caractéristiques techniques, mais aussi d'une mise en œuvre efficace de celles-ci et du maintien de l'intégrité initiale pendant toute la durée de vie de l'équipement. Pour cela, on doit disposer d'un système efficace de gestion de la sécurité et il faut que le personnel, dans tous les domaines d'activité, possède les compétences requises pour les tâches qui lui sont confiées. Il est particulièrement important de pouvoir compter sur un système de gestion de

Figure 58.91 • Rôle du cycle de vie de sécurité dans l'obtention de la sécurité fonctionnelle

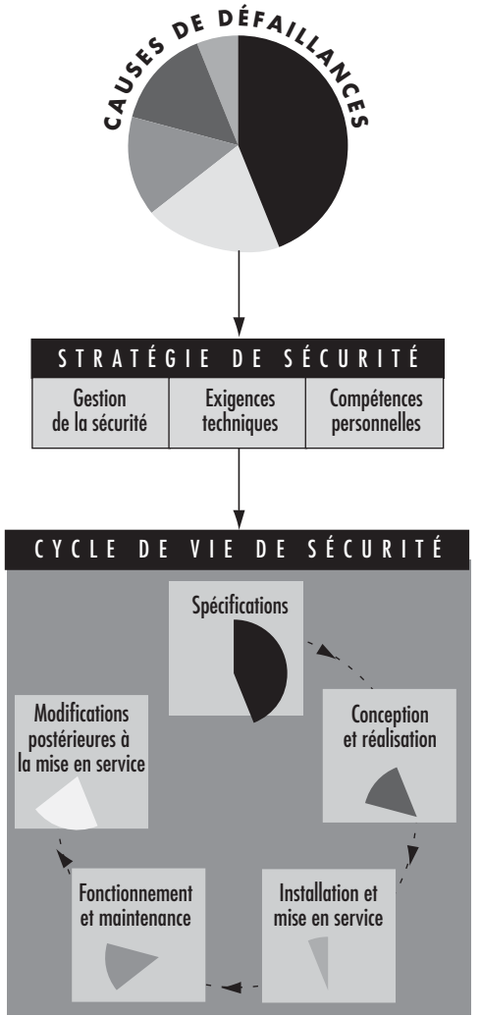
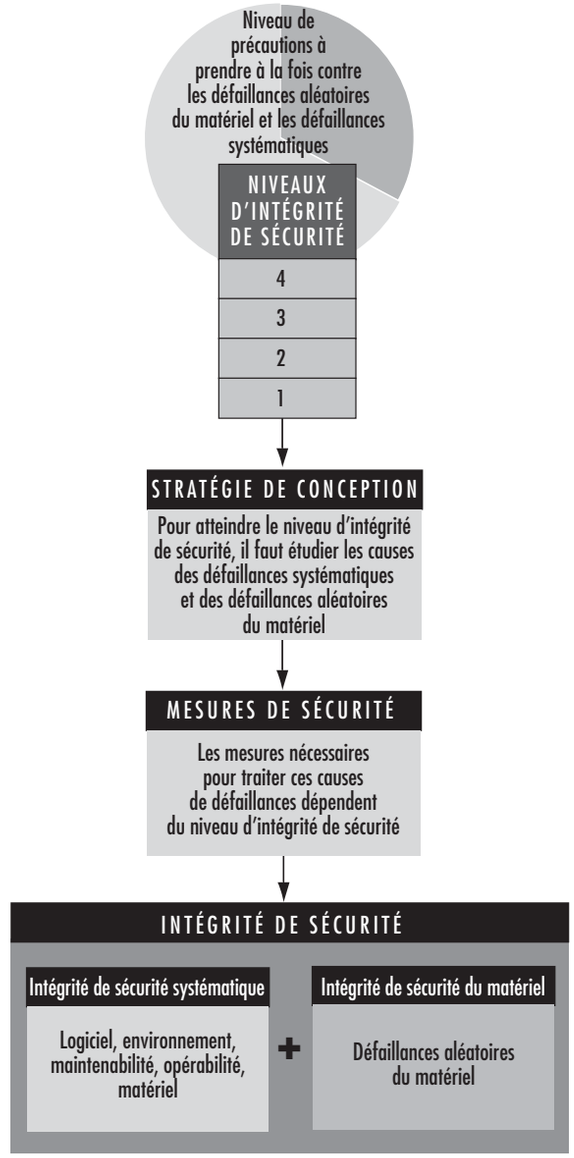


Figure 58.92 • Rôle des niveaux d'intégrité de sécurité dans le processus de conception



la sécurité adéquat dans le cas de systèmes de sécurité complexes. Cela conduit à une stratégie permettant de garantir:

- que l'on dispose d'un système de gestion de la sécurité efficace;
- que les caractéristiques techniques définies pour les systèmes E/E/EP relatifs à la sécurité suffisent pour traiter à la fois les causes des défaillances aléatoires du matériel et celles des défaillances systématiques;
- que les compétences des personnes concernées correspondent aux tâches à accomplir.

La nécessité d'une approche systématique de toutes les caractéristiques techniques de la sécurité fonctionnelle a conduit à créer la notion de cycle de vie de sécurité. Une version simplifiée de cette notion dans la norme CEI 1508 est représentée à la figure 58.91. Les grandes étapes du cycle de vie de sécurité sont:

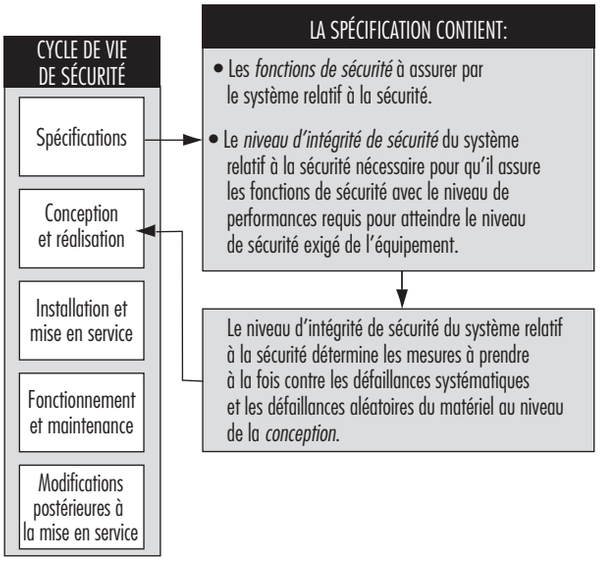
- les spécifications;
- la conception et la réalisation;
- l'installation et la mise en service;
- le fonctionnement et la maintenance;
- les modifications postérieures à la mise en service.

Le niveau de sécurité

La stratégie à adopter en matière de conception pour obtenir des niveaux adéquats d'intégrité de sécurité dans les systèmes relatifs à la sécurité (SRS) est illustrée par les figures 58.92 et 58.93. Le niveau d'intégrité de sécurité attribué dépend du rôle joué par le système dans l'obtention du niveau de sécurité global de l'équipement commandé. Le niveau d'intégrité de sécurité définit les précautions contre les défaillances matérielles aléatoires et les défaillances systématiques qui doivent être intégrées au stade de la conception.

Le concept et le niveau de sécurité s'appliquent à l'équipement commandé. Le concept de sécurité fonctionnelle s'applique au système de sécurité. Il est nécessaire que ce système présente une sécurité fonctionnelle pour que l'équipement à l'origine du risque atteigne un niveau de sécurité adéquat. Le niveau de sécurité prescrit pour une situation spécifique est un facteur essentiel des

Figure 58.93 • Rôle du cycle de vie de sécurité dans le processus de spécification et de conception



caractéristiques d'intégrité de sécurité requises des systèmes relatifs à la sécurité.

Le niveau de sécurité nécessaire dépend de nombreux facteurs, comme la gravité des lésions possibles, le nombre de personnes exposées ou la fréquence et la durée de l'exposition. La perception du danger par les personnes exposées et leurs opinions à ce sujet ont également une importance. Pour parvenir à ce qui représente un niveau de sécurité adapté à une application particulière, les principaux éléments à prendre en considération sont:

- les obligations légales visant l'application en cause;
- les directives des organismes de sécurité compétents;
- les discussions et accords avec les parties concernées par l'application;
- les normes industrielles;
- les normes nationales et internationales;
- les conseils des meilleurs experts industriels et scientifiques indépendants.

Résumé

Lors de la conception et de l'utilisation des systèmes relatifs à la sécurité, il convient de se rappeler que c'est l'équipement commandé qui crée le risque. Les systèmes relatifs à la sécurité sont conçus pour réduire la fréquence ou la probabilité de l'événement dangereux, ainsi que la gravité de ses conséquences éventuelles. Une fois défini le niveau de sécurité nécessaire à l'équipement, on peut déterminer le niveau d'intégrité de sécurité du système relatif à la sécurité; ce niveau permet au concepteur de définir les mesures qui doivent être intégrées au stade de la conception pour éviter les défaillances aléatoires du matériel et les défaillances systématiques.

LES CARACTÉRISTIQUES TECHNIQUES DES SYSTÈMES RELATIFS À LA SÉCURITÉ À BASE DE DISPOSITIFS ÉLECTRIQUES, ÉLECTRONIQUES ET ÉLECTRONIQUES PROGRAMMABLES

John Brazendale et Ron Bell

Les machines, les installations de production et les autres équipements peuvent, en cas de dysfonctionnement, présenter des risques d'incendie, d'explosion, de doses de rayonnements excessives ou de mouvements dangereux. Parmi les causes de ces risques figurent les défaillances des dispositifs électromécaniques, électroniques et électroniques programmables (E/E/EP) employés dans leurs systèmes de contrôle ou de sécurité. Ces défaillances peuvent provenir de défauts matériels du dispositif (comme les phénomènes d'usure se produisant de façon aléatoire dans le temps, appelés défaillances aléatoires du matériel), ou de défauts systématiques (comme les erreurs lors de la définition ou de la conception du système, qui conduisent à des défaillances dues: 1) à une combinaison particulière de signaux d'entrée; 2) à certaines conditions ambiantes; 3) à des signaux erronés ou incomplets émis par les détecteurs; 4) à une saisie erronée ou incomplète de données par les opérateurs; 5) à une mauvaise conception de l'interface).

Les défaillances des systèmes relatifs à la sécurité

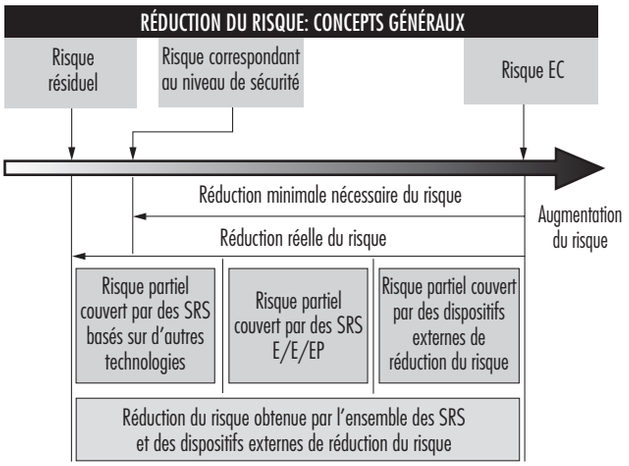
Le présent article a pour objet la sécurité fonctionnelle des systèmes de commande de sécurité, ainsi que les caractéristiques techniques requises des matériels et des logiciels pour obtenir l'intégrité de sécurité voulue. Son approche générale est conforme à la norme CEI 1508, parties 2 et 3, de la Commission électrotechnique internationale (CEI, 1998-2000). Sur un plan général, cette norme internationale vise à permettre une automatisation des installations et des équipements dans des conditions de sécurité. L'un de ses objectifs essentiels est de prévenir les événements ci-après ou d'en réduire le plus possible la fréquence:

- défaillances des systèmes de commande déclenchant d'autres événements susceptibles de conduire à leur tour à un danger (par exemple, défaillance du système de commande, perte de contrôle, processus échappant au contrôle et provoquant un incendie, émission de produits toxiques, etc.);
- défaillances des systèmes d'alarme et de surveillance, privant les opérateurs des informations immédiatement identifiables et compréhensibles qui leur sont nécessaires pour réagir en cas d'urgence;
- défaillances non décelées des systèmes de protection, les rendant indisponibles au moment où ils sont nécessaires pour l'action de sécurité (par exemple, panne d'une carte d'entrée dans un système d'arrêt d'urgence).

L'article «Les systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité», dans le présent chapitre, décrit l'approche générale de gestion de la sécurité exposée dans la partie 1 de la norme CEI 1508 pour assurer la sécurité des systèmes de commande et de protection importants pour la sécurité. Le présent article étudie les principes généraux de conception technique à appliquer pour ramener le risque d'accident à un niveau acceptable, notamment le rôle des systèmes de contrôle ou de protection à base de technologie E/E/EP.

Dans la figure 58.94, le risque inhérent aux équipements, installations de production ou machines (regroupés sous l'appellation *équipement commandé (EC)* sans dispositifs de protection) est indiqué

Figure 58.94 • Réduction du risque: concepts généraux



à une extrémité de l'échelle des risques EC, et le niveau de risque à ne pas dépasser pour assurer le niveau de sécurité voulu, à l'autre extrémité. Dans la zone intermédiaire, on a représenté la combinaison de systèmes relatifs à la sécurité et d'installations extérieures de réduction des risques permettant d'obtenir la limitation des risques requise. Ces dispositifs peuvent être mécaniques (par exemple, soupapes de sécurité), hydrauliques, pneumatiques, physiques ou constitués de systèmes E/E/EP. La figure 58.95 illustre le rôle de chaque couche de sécurité dans la protection de l'équipement à mesure que l'accident prend de l'extension.

Pour autant que l'équipement ait fait l'objet d'une analyse des phénomènes dangereux et des risques conformément à la partie 1 de la norme CEI 1508, le concept de sécurité global a été déterminé, et les fonctions et le niveau d'intégrité de sécurité (NIS) voulus pour un système de contrôle et de protection E/E/EP quelconque ont donc été définis. Le niveau d'intégrité de sécurité visé est défini par rapport à la probabilité des défaillances (voir tableau 58.6).

Les systèmes de protection

Cette section décrit les caractéristiques techniques qui devraient être envisagées par les concepteurs de systèmes E/E/EP relatifs à la sécurité pour que ces systèmes atteignent le niveau d'intégrité

Figure 58.95 • Modèle global: couches de protection

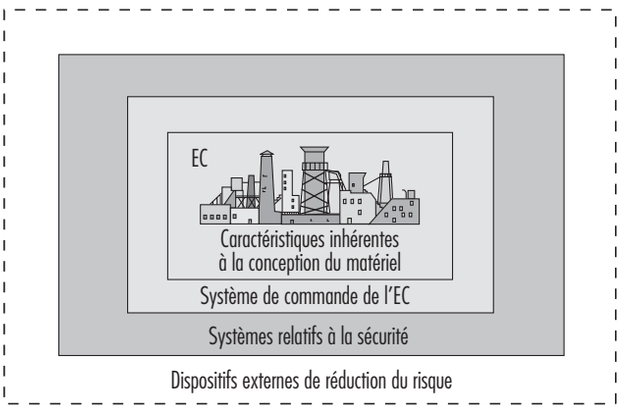
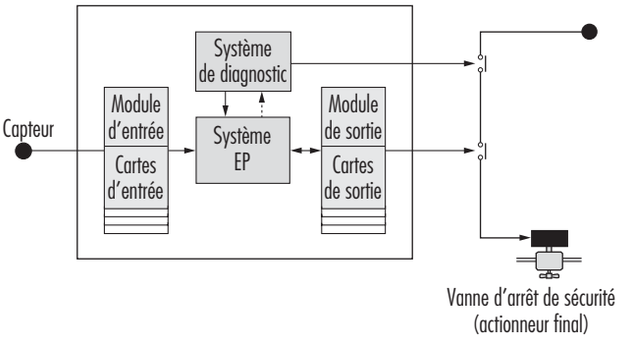


Figure 58.96 • Système type de protection



de sécurité voulu. On prend ici l'exemple d'un système de protection classique utilisant une électronique programmable, afin de commenter plus en détail certains points importants sans perdre de vue les principes généraux. La figure 58.96 illustre le schéma d'un système de protection type, comportant un dispositif de sécurité à voie unique, avec un système de coupure secondaire activé par un système de diagnostic. En fonctionnement normal, une insécurité de l'équipement contrôlé (par exemple, survitesse d'une machine, température excessive d'une installation chimique) sera détectée par le capteur et transmise à l'électronique programmable, qui donnera aux actionneurs, par l'intermédiaire des relais de sortie, l'ordre de mettre le système en sécurité (par exemple, en coupant l'alimentation d'un moteur électrique ou en ouvrant une soupape de sécurité pour faire chuter la pression).

Mais que se passera-t-il en cas de défaillance des composants du système de protection? C'est le rôle du dispositif de coupure secondaire, qui est commandé par la fonction d'autodiagnostic incorporée à cette configuration. Ce système n'est toutefois pas entièrement à sécurité intégrée, dans la mesure où cette configuration n'a qu'une certaine probabilité d'être disponible lorsqu'il lui sera demandé d'exécuter sa fonction de sécurité (donc une certaine probabilité de défaillance sur demande et, par conséquent, un niveau diminué d'intégrité de sécurité). Ce système peut, par exemple, être capable de détecter et de tolérer certains types de défaillances d'une carte de sortie, sans être capable de résister à une défaillance d'une carte d'entrée. Son niveau d'intégrité de sécurité sera donc nettement inférieur à celui d'une configuration comportant une carte d'entrée plus fiable ou un meilleur système de diagnostic, ou une combinaison de ces deux éléments.

Il existe d'autres causes possibles de défaillances des cartes, notamment les défauts physiques «traditionnels» du matériel, les défauts systématiques comme les erreurs dans la définition des

Tableau 58.6 • Niveau d'intégrité de sécurité des systèmes de protection: plages de probabilités des défaillances

Niveau d'intégrité de sécurité	Mode demande (probabilité de défaillance lors de l'exécution sur demande de la fonction spécifique)
4	$10^{-5} \leq x < 10^{-4}$
3	$10^{-4} \leq x < 10^{-3}$
2	$10^{-3} \leq x < 10^{-2}$
1	$10^{-2} \leq x < 10^{-1}$

caractéristiques requises, les défauts de mise en œuvre du logiciel ou une mauvaise protection contre les conditions ambiantes (humidité, par exemple). Dans cette configuration à une seule voie, le diagnostic n'assure pas nécessairement une couverture pour tous ces types de défauts, ce qui limitera le niveau d'intégrité de sécurité atteint en pratique (la couverture est le pourcentage de défaillances qu'un système peut détecter et gérer de façon sûre).

Les caractéristiques techniques

Les parties 2 et 3 de la norme CEI 1508 fournissent un cadre pour identifier les différentes causes possibles de défaillances du matériel et des logiciels et sélectionner les caractéristiques permettant d'y remédier selon le niveau d'intégrité de sécurité requis du système relatif à la sécurité. Par exemple, l'approche technique globale du système de protection de la figure 58.96 est représentée à la figure 58.97. On y indique les deux stratégies de base de protection contre les défaillances: 1) l'évitement des défaillances, qui vise à empêcher l'apparition des anomalies; 2) la tolérance aux défaillances, qui consiste à organiser spécialement le système pour qu'il tolère certaines défaillances spécifiées. Le système à une seule voie cité plus haut est un exemple de conception à tolérance (limitée) aux défaillances, dans laquelle la fonction de diagnostic sert à détecter certaines défaillances et à mettre le système à l'état de sécurité avant l'apparition d'une défaillance dangereuse.

L'évitement des défaillances

L'évitement des défaillances vise à prévenir leur introduction dans un système. La principale approche consiste à adopter une méthode systématique de gestion du projet, dans laquelle la sécurité est traitée comme une qualité définissable et gérable du système au stade de la conception et, par la suite, dans le cadre de l'exploitation et de la maintenance. Cette approche, semblable à l'assurance de la qualité, repose sur le concept du retour d'information et implique: 1) une planification (définition des objectifs de sécurité et identification des moyens d'y parvenir); 2) une mesure des objectifs atteints pendant la réalisation par rapport au plan conçu initialement; 3) l'application du retour d'information pour rectifier les éventuels écarts. Les études de conception sont un bon exemple de technique d'évitement des défaillances. Dans la norme CEI 1508, cette approche «qualitative» de l'évitement des défaillances est facilitée par la prescription faite d'utiliser un cycle de vie de sécurité et de respecter des procédures de gestion de la sécurité aussi bien pour le matériel que pour les logiciels. Pour ceux-ci, il s'agit souvent de procédures d'assurance de la qualité, comme celles décrites dans la norme ISO 9000-3 (ISO, 1997).

En outre, les parties 2 et 3 de la norme CEI 1508, qui concernent respectivement le matériel et les logiciels, établissent un classement de certaines techniques ou mesures considérées comme utiles pour l'évitement des défaillances au cours des différentes phases du cycle de vie de sécurité. Le tableau 58.7 donne un exemple, tiré de la partie 3, pour la phase de conception et de développement du logiciel. Le concepteur peut s'aider de ce tableau pour choisir les techniques appropriées d'évitement des défaillances en fonction du niveau d'intégrité de sécurité requis. Le tableau comporte, pour chaque technique ou mesure, une recommandation pour les différents niveaux d'intégrité de sécurité 1 à 4: fortement recommandé (FR), recommandé (R) et neutre (ni pour ni contre).

La tolérance aux défaillances

Selon la norme CEI 1508, il est nécessaire que le niveau de tolérance augmente en même temps que le niveau d'intégrité de sécurité recherché. La norme admet toutefois que cette tolérance a plus d'importance lorsque les systèmes (et les éléments qui les constituent) sont complexes (appelés de type B dans la norme CEI 1508). Pour les systèmes moins complexes et «éprouvés», on peut retenir un niveau de tolérance aux défaillances moins élevé.

La tolérance aux défaillances matérielles aléatoires

Le tableau 58.8 montre les exigences en matière de tolérance aux défaillances matérielles aléatoires des composants complexes (par exemple, microprocesseurs) utilisés dans un système de protection comme celui de la figure 58.96. Le concepteur devra, le cas échéant, envisager une combinaison appropriée de diagnostic, de tolérance aux défaillances et de vérifications manuelles pour apporter une solution à cette catégorie de défaillances, en fonction du niveau d'intégrité de sécurité acquis.

Figure 58.97 • Spécification de la conception et solution retenue

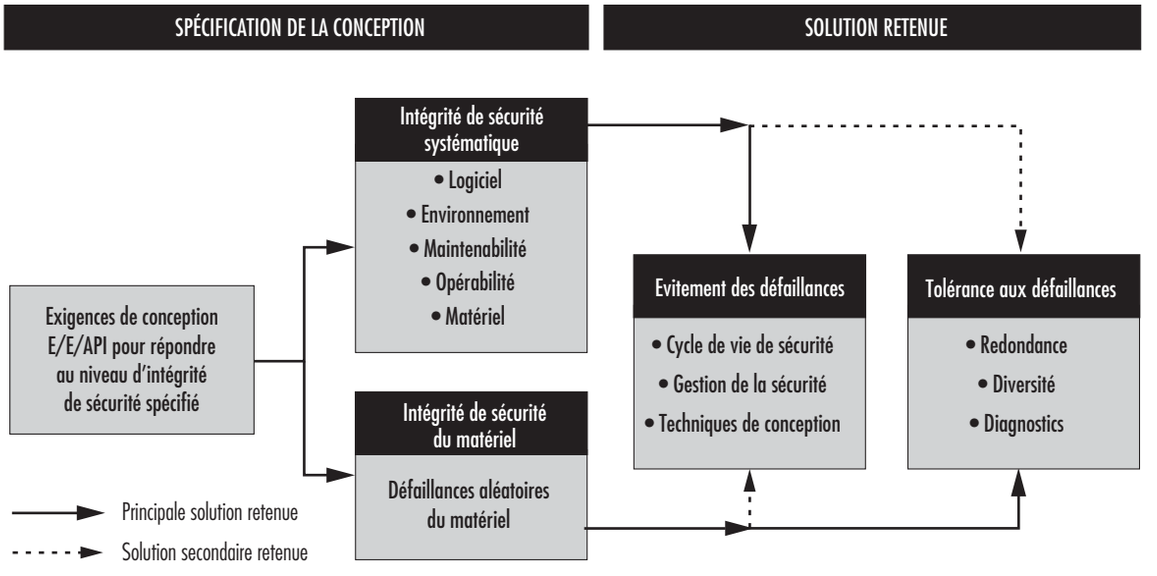


Tableau 58.7 • Conception et développement des logiciels

Technique/mesure	NIS 1	NIS 2	NIS 3	NIS 4
1. Méthodes formelles comprenant, par exemple, CCS, CSP, HOL, LOTOS	—	R	R	FR
2. Méthodes semi-formelles	R	FR	FR	FR
3. Méthodes structurées comprenant, par exemple, JSD, MASCOT, SADT, SSADM et YOURDON	FR	FR	FR	FR
4. Approche modulaire	FR	FR	FR	FR
5. Règles de conception et de codage	R	FR	FR	FR

FR = fortement recommandée; R = recommandée; — = neutre: la technique/mesure n'est ni recommandée, ni déconseillée au niveau d'intégrité de sécurité (NIS).
Note: la technique/mesure appropriée sera choisie en fonction du niveau d'intégrité de sécurité.

La norme CEI 1508 aide le concepteur en lui fournissant des tableaux de spécification (voir tableau 58.9), où les paramètres de conception sont rapportés au niveau d'intégrité de sécurité nécessaire pour un certain nombre d'architectures de système de protection couramment employées.

La première colonne du tableau représente des configurations avec différents degrés de tolérance aux défaillances. Les architectures figurant au bas du tableau ont généralement des degrés de tolérance aux défaillances supérieurs à celles du haut. Un système 1oo2 (un sur deux) est capable de supporter une défaillance unique quelconque, de même que 2oo3.

La deuxième colonne décrit le pourcentage de couverture des systèmes de diagnostic interne. Plus le niveau de diagnostic est élevé, plus les défauts interceptés seront nombreux. C'est là un élément important dans un système de protection, car si le composant défectueux (une carte d'entrée par exemple) est réparé dans un délai raisonnable (huit heures en général), la perte de sécurité fonctionnelle sera faible (on notera que ce ne serait pas le cas pour un système de contrôle en continu, sur lequel toute défaillance est susceptible de provoquer immédiatement une condition d'insécurité et un risque d'incident).

La troisième colonne indique l'intervalle entre les tests de vérification. Il s'agit de tests particuliers qui sont nécessaires pour éprouver de façon intensive le système de protection afin de vérifier l'absence de défauts latents. Ils sont généralement effectués par le fournisseur de l'équipement lors des périodes d'arrêt des installations.

La quatrième colonne indique le taux de faux déclenchements, c'est-à-dire des déclenchements qui provoquent l'arrêt des installations ou des équipements, alors qu'il n'existe pas de défaut dans le processus. La sécurité se paie souvent d'un taux de faux déclenchements supérieur. Un système de protection simple à redondance (1oo2) présente, tous les autres paramètres restant inchangés, un niveau d'intégrité de sécurité supérieur, mais également un taux de faux déclenchements plus élevé qu'un système à voie unique (1oo1).

Tableau 58.8 • Niveau d'intégrité de sécurité — Prescriptions relatives aux défauts sur les composants de type B[1]

1 Les défauts liés à la sécurité non détectés doivent être détectés par le contrôle périodique.

2 Pour les composants sans couverture moyenne du diagnostic en ligne, le système doit être capable d'exécuter la fonction de sécurité en présence d'un défaut unique. Les défauts liés à la sécurité non détectés doivent être détectés par le contrôle périodique.

3 Pour les composants avec une couverture élevée du diagnostic en ligne, le système doit être capable d'exécuter la fonction de sécurité en présence d'un défaut unique. Pour les composants sans couverture élevée du diagnostic en ligne, il doit être capable d'exécuter la fonction de sécurité en présence de deux défauts. Les défauts liés à la sécurité non détectés doivent être détectés par le contrôle périodique.

4 Les composants doivent pouvoir exécuter la fonction de sécurité en présence de deux défauts. Les défauts doivent être détectés avec une couverture élevée du diagnostic en ligne. Les défauts liés à la sécurité non détectés doivent être détectés par le contrôle périodique. L'analyse quantitative du matériel doit être fondée sur des scénarios de la pire éventualité.

[1] Composants dont les modes de défaillance sont mal définis ou difficiles à tester, ou pour lesquels on ne dispose que de peu de données sur leurs défaillances dans des conditions de fonctionnement réelles (par exemple, composants électroniques programmables).

Tableau 58.9 • Prescriptions pour le niveau d'intégrité de sécurité 2 — Architectures des systèmes électroniques programmables destinés aux systèmes de protection

Configuration du système EP	Couverture du diagnostic par voie	Intervalle entre tests périodiques	Temps moyen avant un faux déclenchement
EP simple, E/S simple, Ext. WD	Elevée	6 mois	1,6 an
EP double, E/S simple	Elevée	6 mois	10 an
EP double, E/S double, 2oo2	Elevée	3 mois	1281 ans
EP double, E/S double, 1oo2	Aucune	2 mois	1,4 an
EP double, E/S double, 1oo2	Faible	5 mois	1,0 an
EP double, E/S double, 1oo2	Moyenne	18 mois	0,8 an
EP double, E/S double, 1oo2	Elevée	36 mois	0,8 an
EP double, E/S double, 1oo2D	Aucune	2 mois	1,9 an
EP double, E/S double, 1oo2D	Faible	4 mois	4,7 ans
EP double, E/S double, 1oo2D	Moyenne	18 mois	18 ans
EP double, E/S double, 1oo2D	Elevée	48+ mois	168 ans
EP triple, E/S triple, IPC, 2oo3	Aucune	1 mois	20 ans
EP triple, E/S triple, IPC, 2oo3	Faible	3 mois	25 ans
EP triple, E/S triple, IPC, 2oo3	Moyenne	12 mois	30 ans
EP triple, E/S triple, IPC, 2oo3	Elevée	48+ mois	168 ans

E/S = entrée/sortie.

Si le concepteur ne désire pas utiliser l'une des architectures du tableau, ou s'il souhaite procéder à une analyse plus poussée, la norme CEI 1508 lui laisse cette possibilité. Les techniques d'optimisation de la fiabilité, comme la modélisation de Markov, peuvent alors être employées pour calculer l'élément matériel du niveau d'intégrité de sécurité (Johnson, 1989; Goble, 1992).

La tolérance aux défaillances systématiques et de cause commune

Cette catégorie de défaillances est très importante dans les systèmes de sécurité et elle fait obstacle à la recherche de l'intégrité de sécurité. Dans les systèmes à redondance, un composant, un sous-système, voire le système tout entier, sont doublés afin d'accroître la fiabilité des éléments les moins fiables. Il en résulte une amélioration de la fiabilité du fait que, statistiquement, la probabilité que deux systèmes présentent simultanément une défaillance à la suite de défauts aléatoires est égale au produit des probabilités de chacun, et donc nettement inférieure. En revanche, les défauts systématiques et de mode commun provoquent des défaillances simultanées des systèmes à redondance lorsque, par exemple, une erreur de spécification du logiciel conduit à une défaillance simultanée des parties dupliquées. Un autre exemple est celui de la panne d'une alimentation électrique commune aux deux parties d'un système à redondance.

La norme CEI 1508 comporte des tableaux dans lesquels les techniques sont classées en fonction du niveau d'intégrité de sécurité considéré comme efficace pour une protection contre les défaillances systématiques et de mode commun.

L'hétérogénéité et la redondance analytique sont des exemples de techniques de protection contre les défaillances systématiques. Le principe de l'hétérogénéité consiste à faire réaliser la deuxième voie d'un système à redondance au moyen d'une technologie ou d'un langage informatique différents; les voies redondantes peuvent alors être considérées comme indépendantes en matière de défauts, c'est-à-dire qu'elles présentent une faible probabilité de défaillance simultanée. Cependant, dans le cas notamment des systèmes à base logicielle, il semblerait que cette technique manque d'efficacité, étant donné que la plupart des erreurs se situent dans les spécifications. La redondance analytique tente d'exploiter les informations redondantes disponibles dans l'installation ou la machine pour déceler les défauts. Pour les autres causes de défaillances systématiques, comme les contraintes extérieures, la norme fournit des tableaux donnant des conseils sur les bonnes méthodes techniques à adopter (par exemple, séparation des câbles de signaux et d'alimentation), en fonction du niveau d'intégrité de sécurité.

Conclusion

Les systèmes à base informatique présentent de nombreux avantages, non seulement économiques, mais aussi du point de vue des possibilités d'amélioration de la sécurité. Toutefois, pour tirer parti de ce potentiel, il est nécessaire de porter une bien plus grande attention aux détails que lorsqu'il s'agit de composants classiques. Le présent article a exposé les principales exigences techniques que les concepteurs devraient prendre en compte pour exploiter avec succès cette technologie.

● LES RETOURNEMENTS

Bengt Springfeldt

Les tracteurs et les autres engins mobiles utilisés dans les travaux agricoles ou forestiers, sur les chantiers de construction ou dans les mines, ainsi que pour la manutention de matériaux, peuvent être à l'origine de graves dangers lorsque le véhicule se renverse sur le côté ou bascule vers l'avant ou l'arrière. Ces risques sont accrus lorsqu'il s'agit de tracteurs à roues à centre de gravité élevé. Les autres véhicules qui présentent des risques de retournement sont les tracteurs à chenilles, les chargeuses, les grues, les cueilleuses de fruits, les bouteurs, les tombereaux, les décapeuses et les niveleuses. Ces accidents se produisent en général trop rapidement pour que les conducteurs et les passagers puissent s'échapper; ils risquent alors d'être pris sous le véhicule. Ainsi, les tracteurs à centre de gravité élevé sont très sujets au retournement, et les tracteurs étroits sont encore plus instables que ceux qui sont larges. Un interrupteur à mercure servant à couper le moteur en cas de détection d'un mouvement latéral a été installé sur certains tracteurs, mais il s'est avéré trop lent par rapport aux efforts dynamiques produits par le mouvement de renversement (Springfeldt, 1993) et son utilisation a donc été abandonnée.

Les retournements s'expliquent en grande partie par le fait que ces matériels sont utilisés souvent sur un terrain incliné ou inégal, ou sur un sol meuble et, parfois, très près de fossés, de tranchées ou d'excavations. Lorsque des accessoires sont fixés sur un tracteur à un emplacement élevé, la probabilité de basculement vers l'arrière en montée (ou vers l'avant en descente) augmente. De plus, un tracteur peut se retourner en raison des efforts exercés par les équipements tractés (par exemple, dans une descente, lorsque cet équipement n'est pas freiné et qu'il descend plus rapidement que le tracteur). L'utilisation des tracteurs pour le remorquage occasionne des risques particuliers, notamment lorsque le crochet d'attelage est placé plus haut que l'essieu du tracteur.

Historique

On a commencé à prendre conscience du problème posé par les retournements dans certains pays où le nombre d'accidents mortels était élevé. En Suède et en Nouvelle-Zélande, des travaux de mise au point et d'essais de structures de protection en cas de retournement ROPS (Rollover Protective Structures (ROPS)) sur les tracteurs (voir figure 58.98) avaient déjà été entrepris dans les années cinquante, mais seules les autorités suédoises ont établi sur cette base une réglementation, qui est entrée en vigueur en 1959 (Springfeldt, 1993).

Les projets de réglementation imposant l'installation de structures ROPS sur les tracteurs se sont heurtés dans plusieurs pays à la résistance des milieux agricoles. Les tentatives visant à imposer aux employeurs l'installation de ROPS sur les tracteurs en service ont rencontré une vive opposition, qui s'est même étendue à la proposition que seuls les nouveaux engins soient équipés par les constructeurs. Mais de nombreux pays ont finalement réussi à imposer les ROPS sur les tracteurs neufs et, par la suite, certains sont parvenus également à exiger qu'ils soient montés sur les modèles anciens. Les normes internationales concernant les tracteurs et les engins de terrassement, y compris les normes d'essai des ROPS, ont contribué à améliorer la fiabilité de ces équipements. Par ailleurs, les tracteurs ont été conçus avec des centres de gravité et des crochets d'attelage plus bas. La propulsion à quatre roues motrices a contribué à réduire elle aussi le risque de retournement. La proportion des tracteurs équipés de ROPS reste toutefois assez faible dans les pays où le parc est ancien et où l'équipement a posteriori n'est pas obligatoire.

Les recherches

Les accidents par retournement, en particulier ceux impliquant des tracteurs, ont fait l'objet de recherches dans de nombreux pays. Il n'existe cependant pas de statistiques internationales centralisées sur le nombre d'accidents causés par les types de machines mobiles considérés dans le présent article. Les statistiques dont on dispose au niveau national montrent néanmoins que ce nombre est élevé, surtout dans l'agriculture. Selon un rapport écossais sur les accidents par retournement de tracteurs dans la période

allant de 1968 à 1976, 85% des engins impliqués comportaient des équipements auxiliaires, avec une égale proportion d'équipements tractés et montés. Il était précisé dans le rapport écossais que les deux tiers des accidents de retournement s'étaient produits sur des terrains en pente (Springfeldt, 1993). On a pu démontrer par la suite qu'il serait possible de réduire le nombre de ces accidents en dispensant une formation sur la conduite en terrain incliné, ainsi qu'en installant des instruments de mesure de la déclivité, associés à un indicateur des limites de sécurité correspondantes.

Dans d'autres études, des chercheurs néo-zélandais ont observé que la moitié des accidents mortels par retournement étudiés se produisaient sur sol horizontal ou en pente douce, et seulement un dixième sur des pentes raides. Il se peut que, sur sol plat ou peu incliné, les conducteurs soient moins attentifs aux risques de retournement et sous-estiment les risques présentés par les inégalités de terrain. Sur l'ensemble des décès par retournement de tracteurs survenus en Nouvelle-Zélande de 1949 à 1980, 80% concernaient des tracteurs à roues et 20% des engins à chenilles (Springfeldt, 1993). Des études suédoises et néo-zélandaises ont révélé qu'environ 80% des retournements de tracteurs entraînant un décès étaient des renversements latéraux. La moitié des tracteurs impliqués dans les cas mortels en Nouvelle-Zélande s'étaient retournés de 180°.

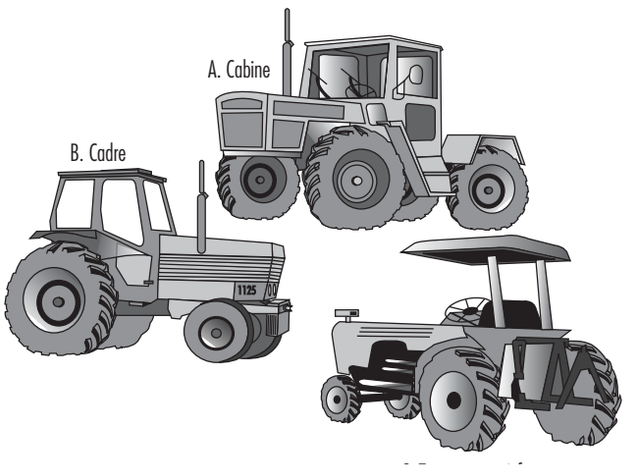
Une étude des cas mortels de retournement en Allemagne de l'Ouest (Springfeldt, 1993) a montré que la proportion de tracteurs anciens non protégés, construits avant 1957 et impliqués dans un retournement mortel était de 1 pour 10 000. Pour les tracteurs équipés de ROPS et construits à partir de 1970, cette proportion était de 1 pour 25 000. Les statistiques sur les retournements ayant entraîné un décès en Allemagne de l'Ouest au cours de la période allant de 1980 à 1985 montrent que les deux tiers des victimes avaient été éjectées de leur zone de protection, puis écrasées ou heurtées par l'engin (Springfeldt, 1993). Dans le cas de retournements non mortels, un quart des conducteurs avaient été éjectés de leur siège, mais non écrasés. Il est évident que le risque d'accident mortel augmente lorsque le conducteur est éjecté de la zone protégée (comme dans les accidents d'automobile). La plupart des tracteurs concernés avaient un toit en porte-à-faux (voir figure 58.98, C) qui n'empêche pas l'éjection du conducteur. Dans quelques cas, le ROPS avait été brisé ou très déformé.

Les fréquences relatives des accidents pour 100 000 tracteurs sur différentes périodes et dans certains pays, ainsi que la réduction des taux d'accidents mortels, ont été calculées par Springfeldt (1993). L'efficacité des ROPS pour la diminution de la gravité des lésions consécutives aux accidents de retournement de tracteurs a été démontrée en Suède, où le nombre de décès pour 100 000 engins a été ramené de 17 environ à 0,3 sur une période de 30 ans (1960-1990) (voir figure 58.99). On estime qu'à la fin de cette période environ 98% des tracteurs étaient équipés de ROPS, principalement sous la forme d'une cabine intégrale (voir figure 58.98, A). En Norvège, les décès ont été ramenés de 24 à 4 pour 100 000 tracteurs environ sur une période analogue. Les résultats ont été moins bons en Finlande et en Nouvelle-Zélande.

La prévention des accidents par retournement

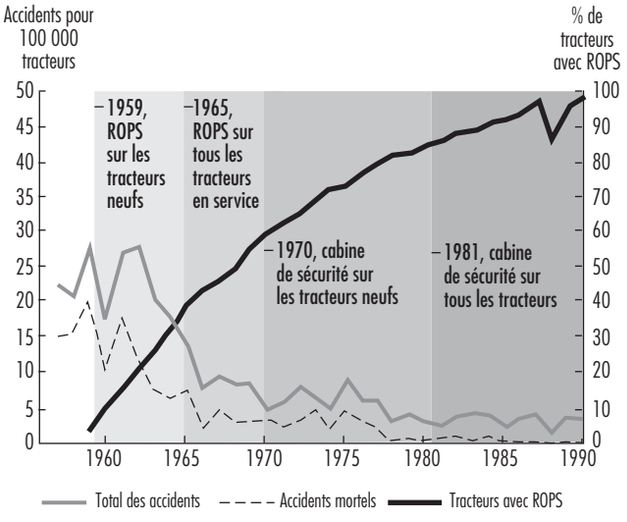
Les tracteurs sont les engins qui présentent le risque de retournement le plus élevé. Malheureusement, les moyens dont on dispose pour empêcher ce type d'accident, dans le cas des travaux agricoles et forestiers, sont peu nombreux. L'installation de ROPS sur les tracteurs et les types de machines de terrassement les plus exposés aux risques de retournement permet de réduire le risque de lésions corporelles, à condition que le conducteur reste sur son siège pendant l'accident (Springfeldt, 1993). La fréquence des décès dépend largement de la proportion de machines protégées

Figure 58.98 • Modèles courants de structures ROPS pour tracteurs



en service et du type de ROPS employé. Un toit en porte-à-faux (voir figure 58.98, C) protège nettement moins qu'une cabine ou un cadre (Springfeldt, 1993). La structure la plus efficace est une cabine intégrale qui permet au conducteur de rester protégé à l'intérieur lorsque l'engin se retourne (la protection contre les intempéries est une raison supplémentaire de choisir une cabine). Le moyen le plus efficace pour que le conducteur reste protégé par le ROPS est la ceinture de sécurité, pour autant qu'il la porte. Dans certains pays, des inscriptions sont apposées sur le siège du conducteur pour lui conseiller de s'accrocher au volant en cas de retournement. On peut également, à titre de mesure de sécurité supplémentaire, concevoir la cabine ou l'environnement intérieur et le ROPS de manière à éviter les risques de blessure par les arêtes vives et les parties saillantes.

Figure 58.99 • Accidents par retournement pour 100 000 tracteurs en Suède entre 1960 et 1990



Dans tous les pays, les retournements de machines mobiles, principalement de tracteurs, sont à l'origine d'accidents graves. Il existe toutefois des différences considérables entre les pays, tant en ce qui concerne les caractéristiques techniques pour la conception de ces machines que les procédures administratives de vérification, d'essai, d'inspection et de mise sur le marché. La diversité qui caractérise, à l'échelle internationale, les efforts de sécurité dans ce domaine peut s'expliquer notamment par les considérations suivantes:

- le fait que l'installation de ROPS soit obligatoire ou qu'il s'agisse de simples recommandations, ou encore l'absence de réglementation;
- la nécessité de règles distinctes pour les machines neuves et pour les matériels anciens;
- l'existence d'inspections effectuées par les autorités et la présence d'une pression sociale et d'une culture favorables au respect des règles de sécurité; dans de nombreux pays, le respect des consignes de sécurité ne fait pas l'objet d'inspections dans les travaux agricoles;
- la pression des syndicats; il convient toutefois de noter que les organisations de travailleurs ont moins d'influence sur les conditions de travail dans l'agriculture que dans d'autres secteurs, compte tenu du grand nombre d'exploitations familiales;
- le type de ROPS utilisé dans le pays;
- l'information et la compréhension des risques auxquels sont exposés les conducteurs de tracteurs; on rencontre souvent des difficultés pratiques à atteindre les agriculteurs et les forestiers pour les faire bénéficier d'une information et d'une formation;
- la géographie du pays, notamment pour les travaux agricoles, forestiers et routiers.

Les réglementations de sécurité

La nature des règles en matière de ROPS et le degré d'application de ces règles au niveau national ont une influence déterminante sur les accidents de retournement, en particulier les accidents mortels. La mise au point de machines plus sûres a été favorisée par les directives, codes et normes publiés par les organismes nationaux et internationaux. En outre, de nombreux pays ont adopté des prescriptions rigoureuses en matière de ROPS, ce qui a permis de réduire sensiblement l'importance de ces accidents.

La Communauté économique européenne

La Communauté économique européenne (CEE) a publié, à partir de 1974, des directives relatives aux approbations de type des tracteurs agricoles et forestiers à roues et, en 1977, des directives spéciales concernant les ROPS, y compris leur fixation au tracteur (Springfeldt, 1993; CEE, 1979, 1982, 1985, 1987, 1988, 1994, 1999). Ces directives imposent aux constructeurs de tracteurs une procédure d'approbation et d'homologation pour chaque type, et les ROPS doivent subir un examen CEE. Ces directives ont été adoptées par tous les pays membres.

Certaines directives de la CEE concernant les ROPS montés sur les tracteurs ont été abrogées le 31 décembre 1995 et remplacées par la directive générale sur les machines, qui s'applique aux types de machines présentant des dangers en raison de leur mobilité (CEE, 1979, 1982, 1985, 1987, 1988, 1994, 1999). Les tracteurs à roues, ainsi que certains engins de terrassement d'une puissance supérieure à 15 kW (à savoir les chargeuses à chenilles et à roues, les chargeuses pelleteuses, les tracteurs à chenilles, les décapeuses, les niveleuses et les tombereaux articulés) doivent être équipés d'un ROPS. En cas de retournement, cet équipement doit offrir au conducteur et aux opérateurs un espace laissant une possibilité de mouvement aux occupants avant qu'ils n'entrent en contact avec des éléments intérieurs lors d'un accident). Il appartient aux constructeurs ou à leurs représentants autorisés d'effectuer les essais requis.

L'Organisation de coopération et de développement économiques

En 1973 et 1987, l'Organisation de coopération et de développement économiques (OCDE) a approuvé des codes standards sur les essais de tracteurs (Springfeldt, 1993; OCDE, 1988). Ces codes donnent les résultats d'essais et décrivent le matériel et les conditions d'essai. Ils prescrivent des essais de nombreuses parties et fonctions des machines, par exemple la résistance des ROPS. Ils décrivent les méthodes d'essais statiques et dynamiques de ces équipements sur certains types de tracteurs. Un ROPS peut être conçu seulement pour protéger le conducteur en cas de retournement. Il doit être testé à nouveau pour chaque modèle de tracteur sur lequel il sera monté. Les codes demandent également qu'il soit possible d'installer sur la structure une protection contre les intempéries. Les codes sur les tracteurs ont été adoptés par tous les Etats membres de l'OCDE à partir de 1988; les Etats-Unis et le Japon admettent aussi des ROPS non conformes à ces codes si les engins sont équipés de ceintures de sécurité (Springfeldt, 1993).

L'Organisation internationale du Travail

En 1981, le Bureau international du Travail (BIT) a publié en français un manuel, *Sécurité et hygiène dans les travaux agricoles,* dans lequel il était prescrit qu'une cabine ou un cadre d'une résistance suffisante soient fixés de manière adéquate sur les tracteurs pour protéger correctement le conducteur et les passagers en cas de retournement (Springfeldt, 1993; BIT, 1981). Selon les recueils de directives pratiques du BIT, les tracteurs agricoles et forestiers devraient être équipés de ROPS protégeant le conducteur et les éventuels passagers en cas de renversement, de chutes d'objets ou de déplacements des charges (BIT, 1976).

L'installation de ROPS ne devrait pas entraver:

- l'accès au poste de conduite depuis le sol;
- l'accès aux commandes principales du tracteur;
- la manœuvrabilité du tracteur dans les espaces limités;
- la fixation ou l'utilisation des équipements devant être rattachés au tracteur;
- le contrôle et le réglage des accessoires.

Les normes internationales et nationales

En 1981, l'Organisation internationale de normalisation (ISO) a publié une norme sur les tracteurs et les matériels agricoles et forestiers (ISO, 1989). Cette norme décrit une méthode d'essai statique des ROPS et définit les conditions de leur homologation. Elle a été approuvée par les organisations membres de 22 pays. Le Canada et les Etats-Unis ont toutefois exprimé leur désapprobation pour des raisons techniques. Une norme avec un recueil de directives pratiques, publiée en 1974 par la Société des ingénieurs automobiles (Society of Automotive Engineers (SAE)) en Amérique du Nord, définit les caractéristiques requises des ROPS installés sur les tracteurs à roues agricoles et de chantier, les décapeuses à roues, les chargeuses frontales, les bouteurs, les chargeuses à chenilles et les niveleuses (SAE, 1974, 1975). Les dispositions de cette norme ont été reprises dans la réglementation des Etats-Unis et dans celle des provinces canadiennes de l'Alberta et de la Colombie-Britannique.

Les réglementations et la conformité à celles-ci

Les codes de l'OCDE et les normes internationales concernent la conception et la construction des ROPS de même que le contrôle de leur résistance, mais ces textes n'ont pas le pouvoir de rendre obligatoire le recours à ce type de protection (OCDE, 1988; ISO, 1989). La Communauté économique européenne a également proposé que les tracteurs et les engins de terrassement soient équipés d'une protection (CEE, 1979, 1982, 1985, 1987, 1988, 1994, 1999). Le but des directives européennes est d'uniformiser les réglementations nationales en ce qui concerne la sécurité des

nouvelles machines au stade de leur fabrication. Les Etats membres sont tenus de respecter ces directives et d'édicter des règlements correspondants. En 1996, les Etats membres de la CEE ont prévu d'élaborer des réglementations exigeant que les tracteurs et engins de terrassement neufs soient équipés de ROPS.

En 1959, la Suède est devenue le premier pays à imposer les ROPS sur les tracteurs neufs (Springfeldt, 1993). La même réglementation afférente est entrée en vigueur au Danemark et en Finlande dix ans plus tard. Par la suite, dans les années soixante-dix et quatre-vingt, des règlements imposant les ROPS sur les tracteurs neufs sont entrés en vigueur au Royaume-Uni, en Allemagne de l'Ouest, en Nouvelle-Zélande, aux Etats-Unis, en Espagne, en Norvège, en Suisse et dans d'autres pays. Dans tous ces pays, à l'exception des Etats-Unis, ces règles ont été étendues aux tracteurs anciens quelques années plus tard, sans avoir toujours un caractère obligatoire. En Suède, tous les tracteurs doivent être équipés d'une cabine protectrice, règle dont l'application au Royaume-Uni est limitée aux tracteurs employés par les ouvriers agricoles (Springfeldt, 1993). Au Danemark, en Finlande et en Norvège, tous les tracteurs doivent être équipés au moins d'un cadre, tandis qu'aux Etats-Unis et en Australie les toits en porte-à-faux sont acceptés. Aux Etats-Unis, les tracteurs doivent être équipés de ceintures de sécurité.

Aux Etats-Unis, les machines de terrassement construites avant 1972 et employées sur les chantiers de construction doivent être équipées de ROPS répondant à des critères de performances minimaux (US Bureau of National Affairs, 1975). Parmi ces machines, on peut citer les décapeuses, les chargeuses frontales, les bouteurs, les tracteurs à chenilles, les chargeuses et les niveleuses.

Résumé

Dans les pays où il est obligatoire d'équiper les tracteurs neufs de ROPS et d'en poser sur les anciens modèles, on a constaté une diminution des lésions par retournement, notamment des accidents mortels. La cabine intégrale est à l'évidence le type de dispositif le plus sûr. Les toits en porte-à-faux n'offrent pas une protection satisfaisante en cas de retournement. De nombreux pays ont imposé des ROPS efficaces au moins sur les tracteurs neufs et, depuis 1996, sur les machines de terrassement. Certaines autorités semblent néanmoins accepter des types de ROPS non conformes aux normes de l'OCDE ou de l'ISO. On s'attend à une harmonisation croissante de la réglementation sur ces protections dans le monde entier, y compris dans les pays en développement.

● LES CHUTES DE HAUTEUR

Jean Arteau

Les chutes de hauteur sont des accidents graves qui se produisent dans de nombreux secteurs d'activité. Les lésions causées résultent du contact entre la personne qui tombe et l'objet ou la surface rencontrés (souvent appelés «agent causal») et peuvent survenir dans les circonstances suivantes:

- La chute de la personne et la force de son impact sont causés par la pesanteur.
- Le point d'impact est situé plus bas que le niveau auquel se trouvait la personne au début de la chute.

Cette définition laisse présumer que les chutes sont inévitables, puisque la pesanteur est omniprésente. Les chutes sont des accidents, souvent très graves, qui peuvent néanmoins être évités dans la plupart des cas. Nous nous proposons d'étudier ci-après les stratégies propres à réduire le nombre des chutes, ou du moins à diminuer leur gravité lorsqu'elles surviennent.

La hauteur de chute

La gravité des lésions occasionnées par les chutes de hauteur est essentiellement fonction de la différence de niveau entre le point de départ et le point d'impact. Toutefois, il convient de nuancer cette assertion: l'énergie en cas de chute libre est le produit de la masse qui tombe par la hauteur de chute, et la gravité des lésions est directement proportionnelle à l'énergie transmise durant l'impact. Les statistiques sur les accidents par chute confirment cette étroite relation, mais montrent également que des chutes d'une hauteur de moins de 3 m peuvent être mortelles. Une étude détaillée des chutes mortelles dans le secteur du bâtiment montre que 10% des décès résultent de chutes d'une hauteur inférieure à 3 m (voir figure 58.100). Deux questions sont à considérer: la limite légale de 3 m, ainsi que le lieu où la chute s'arrête et la manière dont elle est arrêtée.

Dans de nombreux pays, la réglementation impose de prévoir une protection lorsque les travailleurs sont exposés à une chute de plus de 3 m. Une interprétation simpliste de cette règle consisterait à dire que les chutes de moins de 3 m ne sont pas dangereuses. Cette limite de 3 m résulte en fait d'un consensus social, politique et pratique selon lequel il n'est pas obligatoire d'être protégé contre les chutes si l'on travaille à la hauteur d'un seul étage. Même si, sur le plan légal, une protection contre les chutes n'est obligatoire qu'à partir d'une hauteur de 3 m, cette protection devrait toujours être envisagée. La hauteur de la chute n'est pas le seul facteur déterminant pour la gravité de ce type d'accident et le nombre de morts qu'il entraîne. On doit considérer aussi où et comment les chutes surviennent, ce qui conduit à analyser les secteurs d'activité dans lesquels les chutes de hauteur sont les plus fréquentes.

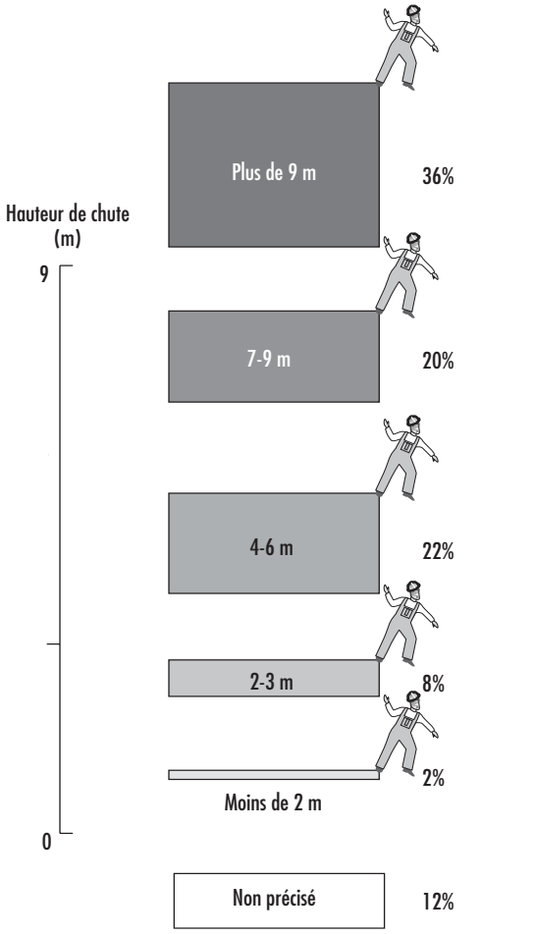
Les lieux des chutes

Les chutes de hauteur sont fréquemment associées au secteur du bâtiment parce qu'elles représentent un fort pourcentage de tous les accidents mortels qui y surviennent. Aux Etats-Unis, par exemple, les chutes de hauteur sont à l'origine de 33% de tous les accidents mortels dans cette branche; au Royaume-Uni, ce pourcentage atteint 52%. Les chutes de hauteur se produisent aussi dans d'autres secteurs d'activité. Leur fréquence est élevée également dans l'exploitation minière et la construction de matériels de transport. Au Québec, qui compte beaucoup de mines souterraines, avec des veines étroites et très inclinées, 20% de tous les accidents sont des chutes de hauteur. La construction, l'utilisation et la maintenance d'engins de transport comme les avions, les camions et les wagons ferroviaires sont des activités où les chutes sont fréquentes (voir tableau 58.10). La proportion varie d'un pays à l'autre en fonction du niveau d'industrialisation, du climat, etc., mais les chutes de hauteur se produisent dans tous les secteurs avec des conséquences similaires. En plus de la hauteur de chute libre, il faut considérer ce sur quoi la chute est arrêtée et quelle partie du corps subit l'impact. Tomber dans un liquide chaud, sur des rails électrifiés ou dans un broyeur peut causer la mort même si la hauteur de chute est inférieure à 3 m.

Les causes des chutes

Jusqu'à maintenant, il a été montré que les chutes surviennent dans tous les secteurs économiques et qu'elles peuvent être mortelles même si la hauteur est inférieure à 3 m. Pour quelles raisons une personne tombe-t-elle? De nombreux facteurs humains peuvent être à l'origine d'une chute. Par souci de simplicité et de commodité, nous regrouperons ces facteurs dans les grandes catégories ci-après:

Figure 58.100 • Décès par chute et hauteur de chute dans le secteur du bâtiment aux Etats-Unis, de 1985 à 1993



Nombre total de décès par chute: 1 954
Nombre total d'accidents mortels (toutes causes confondues): 5 964

Source: Culver et Connolly, 1994.

Les *occasions* de chute sont déterminées par des facteurs liés à l'environnement et sont à l'origine du type de chute le plus fréquent, à savoir le fait de trébucher ou de glisser, et de tomber au même niveau. D'autres occasions de chute sont associées à des activités se déroulant au-dessus du niveau du sol.

Une *propension* à tomber peut être provoquée par une ou plusieurs maladies aiguës et chroniques. Les maladies spécifiquement liées aux chutes sont généralement celles qui affectent le système nerveux, le système circulatoire, le système musculo-squelettique ou une combinaison de ces systèmes.

Une *tendance* à tomber résulte des détériorations intrinsèques universelles qui caractérisent le processus normal de vieillissement. Lors d'une chute, l'aptitude à maintenir une position verticale, ou stabilité posturale, est perdue du fait d'une combinaison de tendances, de propensions et d'occasions.

La stabilité posturale

Les chutes sont provoquées par une défaillance momentanée de la stabilité posturale qui maintient normalement une personne en position debout. Elle est le fait d'un système constitué d'un grand nombre d'adaptations rapides à des perturbations extérieures, en particulier la pesanteur. Ces adaptations sont en majeure partie des actions réflexes, favorisées par de nombreux arcs réflexes possédant chacun une entrée sensorielle, des liaisons intégratives internes et une sortie motrice. Les entrées sensorielles sont la vision, les mécanismes de l'oreille interne qui détectent la position dans l'espace, l'appareil somato-sensoriel qui détecte les stimuli de pression sur la peau, et la position des articulations portantes. Il apparaît que la perception visuelle joue un rôle particulièrement important. On sait très peu de choses des structures intégratives normales et des fonctions de la moelle épinière ou du cerveau. La sortie motrice de l'arc réflexe est la réaction musculaire.

Tableau 58.10 • Chutes de hauteur: Québec 1982-1987

	Chutes de hauteur par 1 000 travailleurs	Chutes de hauteur par rapport à l'ensemble des accidents
Construction	14,9	10,1%
Industrie lourde	7,1	3,6%

La vision

La principale entrée sensorielle est la vision. Deux fonctions visuelles sont liées à la stabilité posturale et au contrôle de la démarche:

- la perception de ce qui est vertical et de ce qui est horizontal, qui est à la base de l'orientation spatiale;
- la capacité de détecter et de distinguer des objets dans des espaces encombrés.

Deux autres fonctions visuelles sont importantes:

- la capacité de stabiliser la direction du regard afin d'immobiliser l'environnement et un point de référence visuelle pendant qu'on se déplace;
- la capacité de fixer et de suivre du regard des objets bien définis au sein d'un large champ de vision. Cette fonction exige une attention considérable et entraîne une détérioration des performances dans les autres tâches demandant simultanément de l'attention.

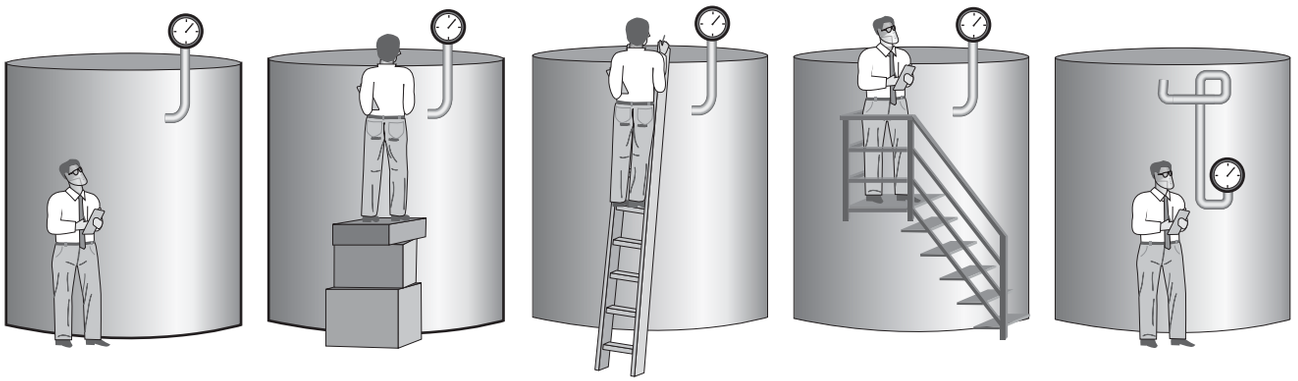
Les causes de l'instabilité posturale

Les trois entrées sensorielles sont interactives et liées entre elles. L'absence de l'une d'elles, ou la présence d'entrées faussées, conduisent à une instabilité posturale, voire à la chute. Quelles sont les causes de cette instabilité?

La vision

- l'absence de références verticales et horizontales, comme dans le cas d'un monteur de charpentes métalliques travaillant sur le toit d'un bâtiment;
- l'absence de références visuelles stables; ainsi, l'eau qui coule sous un pont ou des nuages en mouvement ne sont pas des références stables;
- le fait de fixer un objet précis dans le cadre du travail, ce qui diminue d'autres fonctions visuelles comme la capacité de détecter et de distinguer des objets qui pourraient faire trébucher dans un espace encombré;
- un objet en mouvement sur un arrière-plan ou une référence mobile, par exemple un élément de structure métallique déplacé par une grue, avec des nuages en mouvement comme arrière-plan et référence visuelle.

Figure 58.101 • Installations pour la lecture d'une jauge



L'oreille interne
- avoir la tête en bas, alors que le système d'équilibration a des performances optimales à l'horizontale;
- voyager dans un avion pressurisé;
- un mouvement très rapide, par exemple sur des montagnes russes;
- les maladies.

L'appareil somato-sensoriel (stimuli de pression sur la peau et position des articulations portantes)
- se tenir sur une seule jambe;
- engourdissement des membres en raison d'un maintien prolongé dans une position immobile, par exemple à genoux;
- port de bottes rigides;
- membres très froids.

La sortie motrice
- membres engourdis;
- fatigue musculaire;
- maladies, lésions;
- vieillissement, incapacité permanente ou temporaire;
- vêtements volumineux ou pesants.

La stabilité posturale et le contrôle de la démarche sont des réflexes très complexes chez l'être humain. Toute perturbation des entrées sensorielles peut provoquer une chute. Les perturbations décrites dans cette section sont fréquentes sur les lieux de travail où les chutes sont considérées comme une sorte de phénomène naturel qu'il convient de prévenir.

La stratégie de protection contre les chutes

Comme nous l'avons déjà mentionné, les risques de chute sont identifiables. Il est donc possible de prévenir ce type d'accidents. Sur la figure 58.101, on peut voir une situation très répandue dans laquelle un opérateur doit lire les indications d'un cadran. La première illustration montre une situation classique: un manomètre est installé au sommet d'un réservoir sans moyen d'y accéder. Sur la deuxième, le travailleur improvise un moyen d'accès en montant sur plusieurs caisses, solution qui est dangereuse. Sur la troisième, il utilise une échelle, ce qui est une amélioration. Mais comme cette échelle n'est pas fixée à demeure sur le réservoir, il est probable qu'elle sert à effectuer ailleurs d'autres contrôles lorsqu'une lecture est requise. Une telle situation est envisageable si l'on ajoute à l'échelle ou au réservoir un dispositif d'arrêt des chutes ou si le travailleur porte un harnais complet avec une sangle accrochée à un point d'ancrage. Le risque de chutes de hauteur subsiste néanmoins.

Dans la quatrième illustration, il existe un moyen d'accès amélioré, constitué d'un escalier, d'une plate-forme et d'un garde-corps. Les avantages sont une réduction des risques de chute et une plus grande facilité de lecture (confort) qui réduit la durée de chaque mesurage et assure une posture de travail stable qui améliore la précision de la mesure.

La solution correcte est celle de la cinquième illustration. Au stade de la conception de l'installation, les activités de maintenance et d'exploitation ont été prises en compte. Le manomètre a été installé de manière à pouvoir être lu au niveau du sol. Aucune chute de hauteur n'est possible et tout danger est donc écarté.

La stratégie exposée met l'accent sur la prévention des chutes par l'emploi de moyens d'accès appropriés, comme des échafaudages, des échelles ou des escaliers (Bouchard, 1991). S'il n'est pas

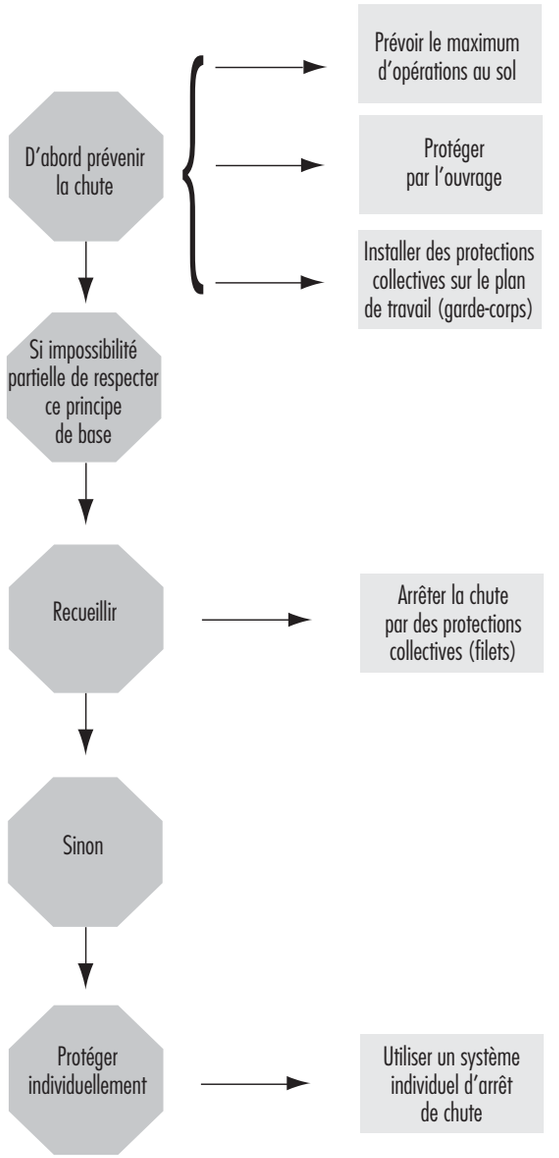
Tableau 58.11 • Dispositifs types de prévention et d'arrêt des chutes

	Dispositifs de prévention des chutes	Dispositifs d'arrêt des chutes
Protection collective	Garde-corps, mains courantes	Filet de sécurité
Protection individuelle	Dispositif de limitation des déplacements	Harnais, longe, absorbeur d'énergie, ancrage, etc.

Tableau 58.12 • Différences entre prévention et arrêt des chutes

	Prévention	Arrêt
Chute	Non	Oui
Equipement type	Garde-corps	Harnais, longe, absorbeur d'énergie et ancrage (dispositif d'arrêt des chutes)
Force nominale	1 à 1,5 kN appliqué horizontalement et 0,45 kN appliqué verticalement — en un point quelconque de la lisse supérieure	Force minimale de rupture du point d'ancrage: 18 à 22 kN
Type d'effort	Statique	Dynamique

Figure 58.102 • Stratégie de prévention des chutes



Source: OPPBTP, 1984.

possible de prévenir les chutes, des dispositifs d'arrêt des chutes doivent être employés (voir figure 58.102). Pour que ces dispositifs soient efficaces, il est nécessaire que leur mise en place soit planifiée. Le point d'ancrage en est un élément essentiel, qui devrait être prévu au stade de la conception. Les dispositifs employés doivent être efficaces, fiables et confortables. Deux exemples sont donnés par Arteau, Lan et Corbeil (1994) et Lan, Arteau et Corbeil (1994). Des exemples de dispositifs types de prévention des chutes et d'arrêt des chutes sont donnés dans le tableau 58.11. Les systèmes d'arrêt des chutes et leurs éléments sont exposés en détail par Sulowski (1991).

L'accent mis sur la prévention n'est pas un choix idéologique, mais pratique. Le tableau 58.12 relève les différences entre la prévention et l'arrêt des chutes avec, dans ce dernier cas, la solution traditionnelle de l'équipement de protection individuelle.

Il faut privilégier les mesures de prévention, qui sont caractérisées par des sollicitations mécaniques dix à vingt fois inférieures à celles des dispositifs d'arrêt des chutes. Ainsi, la lisse d'un garde-corps doit pouvoir accepter une charge de service de l'ordre de 1 kN — le poids d'un homme corpulent — alors que la longe accrochée à un point d'ancrage doit pouvoir résister à une force de l'ordre de 20 kN, soit le poids de deux petites voitures ou d'un bloc de béton de 1 m^3. Avec un dispositif de prévention, la chute est évitée et le risque de lésion est inexistant; avec un dispositif d'arrêt de chute, elle se produit et, même si elle est arrêtée, il peut y avoir un risque de lésions, selon les circonstances.

LES ESPACES CONFINÉS

Neil McManus

Toutes les branches d'activité peuvent comporter des espaces confinés qui sont à l'origine d'accidents, mortels ou non. Le terme «espace confiné» est habituellement employé pour désigner des structures comme les réservoirs, les cuves, les fosses, les égouts ou les trémies. Une telle définition basée sur une description est cependant trop restrictive et permet difficilement une extrapolation à toutes les structures où des accidents se sont effectivement produits. En soi, toute structure dans laquelle des personnes travaillent peut être ou peut devenir un espace confiné. Les espaces de cette nature peuvent être soit très grands soit très petits. Ce terme désigne en fait un environnement dans lequel une grande diversité de situations dangereuses peuvent se présenter: confinement de personnes, risques liés aux structures, aux processus, aux éléments mécaniques, aux produits liquides ou en vrac, risques atmosphériques, physiques, chimiques ou biologiques, risques ergonomiques, etc. Un grand nombre de situations créées par ces risques ne sont pas propres aux espaces confinés, mais elles sont aggravées par l'existence d'un confinement.

Les espaces confinés sont considérablement plus dangereux que les espaces de travail normaux. A la suite de modifications apparemment mineures, ces lieux jusqu'alors sans danger peuvent présenter subitement des risques mortels. Ces modifications peuvent être transitoires et discrètes, ce qui les rend difficiles à identifier et à traiter. Les travaux nécessitant de pénétrer dans des espaces confinés correspondent généralement à des activités d'inspection, de maintenance ou de transformation. Ces interventions ne font pas partie du travail courant et sont de courte durée, non répétitives et imprévisibles (elles se déroulent souvent en dehors des heures de travail normales ou pendant l'arrêt des installations).

Les accidents dans les espaces confinés

Les accidents qui se produisent dans les espaces confinés diffèrent de ceux qui surviennent dans les espaces de travail courants. Une erreur ou une omission apparemment anodines dans la préparation de l'espace, dans le choix ou la maintenance des matériels ou dans les travaux eux-mêmes peut précipiter un accident du fait même que, dans ces situations, la tolérance aux erreurs est plus faible que dans les environnements habituels.

Les victimes d'accidents dans des espaces confinés appartiennent à toutes les catégories professionnelles. Ce sont pour la plupart des ouvriers, ce qui n'est pas surprenant, mais on trouve également des ingénieurs, des techniciens, des cadres et des dirigeants, ainsi que des membres des équipes de secours. Le personnel de sécurité et d'hygiène du travail n'est pas épargné lui non

plus. Les seules données disponibles sur les accidents dans des espaces confinés proviennent des Etats-Unis et elles ne concernent que les accidents mortels (NIOSH, 1994). A l'échelle mondiale, ces accidents coûteraient la vie à environ 200 personnes par an (Reese et Mills, 1986). Il s'agit là au mieux d'une estimation reposant sur des données incomplètes, mais à laquelle on semble pouvoir se fier. Les deux tiers environ des accidents étaient dus à la présence d'une atmosphère dangereuse dans l'espace confiné et, dans environ 70% de ces cas, cette situation existait avant l'entrée dans cet espace et le début des travaux. Ces accidents provoquent parfois des décès multiples, dont certains résultent de l'incident initial et de la tentative de sauvetage qui a suivi. Les conditions extrêmement stressantes dans lesquelles se déroulent les secours exposent souvent les sauveteurs improvisés à un danger nettement supérieur à celui subi par la victime initiale.

Les causes et les conséquences des accidents survenus lors de travaux à l'extérieur de structures contenant des atmosphères dangereuses sont semblables à celles des accidents se produisant à l'intérieur des espaces confinés. Les explosions ou les incendies impliquant une atmosphère confinée sont à l'origine d'environ la moitié des accidents mortels de soudage et de découpage aux Etats-Unis. Environ 16% de ces accidents concernaient des fûts ou des réservoirs prétendument vides (OSHA, 1988).

L'identification des espaces confinés

Une étude sur les accidents mortels dans les espaces confinés montre que les meilleures précautions sont l'information et la formation des travailleurs et la mise en place d'un programme d'identification et de gestion des risques. Un programme de développement des compétences est également essentiel pour permettre au personnel d'encadrement et aux travailleurs de reconnaître les situations potentiellement dangereuses. L'un des éléments utiles de ce programme est un inventaire précis et mis à jour des espaces confinés, indiquant le type d'espace, son emplacement, ses caractéristiques, son contenu, ses conditions dangereuses, etc. Il est souvent très difficile de dresser cet inventaire, dans la mesure où le nombre et le type des espaces changent constamment. En revanche, les espaces confinés des industries de transformation sont faciles à identifier; d'ailleurs ils restent fermés et inaccessibles la plupart du temps. Dans certains cas, un espace peut être considéré comme confiné un jour et ne plus l'être le lendemain.

Un avantage de l'identification des espaces confinés est la possibilité qui est ainsi donnée de les signaler. Cette signalisation peut toutefois présenter des inconvénients: 1) elle peut devenir impossible à repérer lorsqu'il existe déjà un grand nombre d'autres panneaux de mise en garde; 2) les entreprises possédant de nombreux espaces confinés peuvent avoir de grandes difficultés à les signaler; 3) la signalisation apporterait peu d'avantages lorsque les personnes appelées à pénétrer dans les espaces confinés changent fréquemment; 4) le fait de s'en remettre à des signalisations engendre une dépendance. Certains espaces confinés peuvent être oubliés.

L'évaluation des risques

L'aspect le plus complexe et le plus difficile des espaces confinés demeure l'évaluation des risques. Cette évaluation vise à identifier les situations dangereuses ou potentiellement dangereuses, ainsi que le niveau et l'acceptabilité du risque. L'évaluation du risque est délicate, car un grand nombre de situations dangereuses peuvent entraîner des lésions ou des traumatismes. Elles sont difficiles à reconnaître et changent fréquemment. L'élimination ou l'atténuation des dangers pendant la préparation d'un espace confiné avant une entrée sont donc indispensables pour réduire le plus possible les risques au cours du travail.

L'évaluation des risques peut fournir une estimation qualitative du niveau de gravité d'une situation particulière à un moment donné (voir tableau 58.13). Des niveaux allant d'un minimum à un maximum sont définis dans chaque catégorie. Les différentes catégories ne sont pas comparables, puisque leurs niveaux maximaux peuvent être très différents.

Il est possible de développer chacune des entrées du tableau 58.13 de manière à donner des précisions sur les risques lorsque la situation est préoccupante. On peut aussi éliminer de l'étude les rubriques qui ne sont pas pertinentes.

Les qualifications de l'évaluateur sont un élément essentiel du succès du processus d'identification et d'évaluation des risques. La personne ainsi désignée est réputée capable, de par son expérience, ses connaissances ou sa formation spécialisée, de prévoir, de reconnaître et d'évaluer les expositions à des substances dangereuses ou à d'autres situations à risques, et d'indiquer les mesures de contrôle et de protection appropriées. On attend donc de cette personne qu'elle sache ce qu'il faut faire dans une situation particulière impliquant des travaux en espace confiné.

Tableau 58.13 • Formulaire type d'évaluation de conditions dangereuses

Conditions dangereuses	Conséquence réelle ou possible		
	Faible	Modérée	Elevée
Travail à la chaleur			
Risques atmosphériques			
manque d'oxygène			
excès d'oxygène			
risques chimiques			
risques biologiques			
incendie/explosion			
Ingestion/contact avec la peau			
Agents physiques			
bruit/vibrations			
contrainte thermique (chaud/froid)			
rayonnements non ionisants/ionisants			
laser			
Confinement des personnes			
Risques mécaniques			
Risques liés au processus			
Risques pour la sécurité			
risques structurels			
engloutissement/immersion			
enchevêtrement			
risques électriques			
chute			
glissade/perte d'équilibre			
visibilité/niveau d'éclairage			
explosion/implosion			
surfaces chaudes/froides			

Certains termes comme *substance toxique, manque d'oxygène, excès d'oxygène, risques mécaniques,* etc., appellent une définition plus précise en fonction des normes existantes.

Tableau 58.14 • Exemple de permis d'entrée

SOCIÉTÉ ABC **ESPACE CONFINÉ — PERMIS D'ENTRÉE**			
1. DESCRIPTION			
Service:			
Site:			
Bâtiment/atelier:			
Equipement/espace:			
Partie:			
Date:	Evaluateur:		
Durée:	Qualifications:		
2. ESPACES ADJACENTS			
Espace:			
Description:			
Contenu:			
Processus:			
3. CONDITIONS RÉGNANT AVANT LES TRAVAUX			
Risques atmosphériques			
Manque d'oxygène Concentration	❑ Oui (Minimum acceptable:	❑ Non	❑ Sous contrôle %)
Excès d'oxygène Concentration	❑ Oui (Maximum acceptable:	❑ Non	❑ Sous contrôle %)
Risques chimiques Concentration des substances	❑ Oui (Norme acceptable:	❑ Non	❑ Sous contrôle)
Risques biologiques Concentration des substances	❑ Oui (Norme acceptable:	❑ Non	❑ Sous contrôle)
Incendie/explosion Concentration des substances	❑ Oui (Maximum acceptable:	❑ Non	❑ Sous contrôle % LIE*)
Ingestion /contact avec la peau	❑ Oui	❑ Non	❑ Sous contrôle
Agents physiques			
Bruit/vibrations Niveau:	❑ Oui (Maximum acceptable:	❑ Non	❑ Sous contrôle dBA)
Contrainte thermique (chaud/froid) Température:	❑ Oui (Plage acceptable:	❑ Non	❑ Sous contrôle)
Rayonnements non ionisants/ionisants Type: Niveau:	❑ Oui (Maximum acceptable:	❑ Non	❑ Sous contrôle)
Laser Type: Niveau:	❑ Oui (Maximum acceptable:	❑ Non	❑ Sous contrôle)
Confinement des personnes (voir les mesures de protection)	❑ Oui	❑ Non	❑ Sous contrôle
Risques mécaniques (voir la procédure)	❑ Oui	❑ Non	❑ Sous contrôle

* LIE: limite inférieure d'explosibilité.

Tableau 58.14 • Exemple de permis d'entrée

SOCIÉTÉ ABC **ESPACE CONFINÉ — PERMIS D'ENTRÉE**			
Risques liés au processus (voir la procédure)	❑ Oui	❑ Non	❑ Sous contrôle
Risques pour la sécurité			
Risques structurels (voir les mesures de protection)	❑ Oui	❑ Non	❑ Sous contrôle
Engloutissement/immersion (voir les mesures de protection)	❑ Oui	❑ Non	❑ Sous contrôle
Enchevêtrement (voir les mesures de protection)	❑ Oui	❑ Non	❑ Sous contrôle
Risques électriques (voir la procédure)	❑ Oui	❑ Non	❑ Sous contrôle
Chute (voir les mesures de protection)	❑ Oui	❑ Non	❑ Sous contrôle
Glissade/perte d'équilibre (voir les mesures de protection)	❑ Oui	❑ Non	❑ Sous contrôle
Visibilité/niveau d'éclairage	❑ Oui	❑ Non	❑ Sous contrôle
Niveau:	(Plage acceptable:		lux)
Explosion/implosion (voir les mesures de protection)	❑ Oui	❑ Non	❑ Sous contrôle
Surfaces chaudes/froides (voir les mesures de protection)	❑ Oui	❑ Non	❑ Sous contrôle
Si vous cochez les cases «Oui» ou «Sous contrôle», prière de fournir des précisions complémentaires et de vous reporter aux mesures de protection. Pour les risques pouvant être évalués par voie de tests, se reporter aux tests requis. Indiquer la date de l'étalonnage le plus récent. Les maxima, minima, plages ou valeurs normales sont fonction de la réglementation.			
4. Procédure de travail			
Description:			
Travail à la chaleur (voir les mesures de protection)	❑ Oui	❑ Non	❑ Possible
Risques atmosphériques			
Manque d'oxygène (voir les tests complémentaires requis. Noter les résultats. Voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Concentration:	(Minimum acceptable:		%)
Excès d'oxygène (voir les tests complémentaires requis. Noter les résultats. Voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Concentration:	(Maximum acceptable:		%)
Risques chimiques (voir les tests complémentaires requis. Noter les résultats. Voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Concentration:	(Valeur normale acceptable:		)
Risques biologiques (voir les tests complémentaires requis. Noter les résultats. Voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Concentration:	(Valeur normale acceptable:		)
Incendie/explosion (voir les tests complémentaires requis. Noter les résultats. Voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Concentration:	(Valeur normale acceptable:		)
Ingestion/contact avec la peau (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Agents physiques			
Bruit/vibrations (voir les mesures de protection requises. Voir les tests complémentaires requis. Noter les résultats)	❑ Oui	❑ Non	❑ Possible
Niveau:	(Maximum acceptable:		dBA)
Contrainte thermique (chaleur/froid) (voir les mesures de protection requises. Voir les tests complémentaires requis. Noter les résultats)	❑ Oui	❑ Non	❑ Possible
Température:	(Plage acceptable:		)
Suite au verso			

Tableau 58.14 • Exemple de permis d'entrée

SOCIÉTÉ ABC **ESPACE CONFINÉ — PERMIS D'ENTRÉE**			
Rayonnements non ionisants/ionisants (voir les mesures de protection requises. Voir les tests complémentaires requis. Noter les résultats) Type: Niveau:	❑ Oui (Maximum acceptable:	❑ Non	❑ Possible)
Laser (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Risques mécaniques (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Risques liés au processus (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Risques pour la sécurité *Risques structurels* (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Engloutissement/immersion (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Enchevêtrement (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Risques électriques (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Chute (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Glissade/perte d'équilibre (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Visibilité/niveau d'éclairage (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Explosion/implosion (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Surfaces chaudes/froides (voir les mesures de protection requises)	❑ Oui	❑ Non	❑ Possible
Si vous cochez les cases «Oui» ou «Possible», prière de fournir des précisions complémentaires et de vous reporter aux mesures de protection. Pour les risques pouvant être évalués par voie de tests, se reporter aux tests requis. Indiquer la date de l'étalonnage le plus récent.			
Mesures de protection Equipement de protection individuelle (préciser)			
Equipement et procédure de communications (préciser)			
Systèmes d'alarme (préciser)			
Equipements de secours (préciser)			
Ventilation (préciser)			
Eclairage (préciser)			
Autres (préciser)			
Tests requis Préciser les tests à effectuer et leur fréquence			
Personnel Supérieur responsable pour l'entrée			
Supérieur du service d'origine			
Personnes autorisées à entrer			
Personnel chargé des tests			
Veilleurs			

Une évaluation des risques devrait être effectuée pour chacun des stades suivants du cycle d'intervention dans un espace confiné: l'espace non modifié, la préparation de l'entrée, l'inspection préalable aux travaux, les travaux eux-mêmes (McManus, non daté, manuscrit) et les mesures à prendre en cas d'urgence. Des accidents mortels se sont produits à chacun de ces stades. L'espace non modifié se réfère à la situation qui existe entre la fermeture de l'espace à la fin d'une intervention et le début de la préparation de la suivante. La préparation de l'entrée englobe toutes les mesures prises pour sécuriser l'espace de manière qu'on puisse y entrer et y travailler en toute sécurité. L'inspection préalable consiste à pénétrer une première fois dans l'espace et à l'examiner pour s'assurer qu'on peut commencer le travail sans danger (cette pratique est imposée par certaines réglementations). Les travaux sont les tâches à exécuter par les personnes pénétrant dans l'espace. Les mesures d'urgence correspondent aux opérations de sauvetage ou à d'autres situations d'urgence. Les risques qui subsistent au début des travaux ou qui sont créés par eux déterminent la nature des accidents auxquels on doit se préparer.

Une évaluation des risques est indispensable pour chacun de ces éléments, car les points à surveiller changent constamment. Ainsi, une situation particulière correspondant à un certain niveau de préoccupation peut disparaître à la suite de la préparation de l'entrée, mais elle peut réapparaître, ou une situation nouvelle peut se manifester à l'issue de travaux à l'intérieur ou à l'extérieur de l'espace confiné. C'est la raison pour laquelle il ne se justifierait pas d'affecter définitivement un niveau de préoccupation à une situation dangereuse en se fondant uniquement sur une évaluation des conditions régnant avant l'ouverture de l'espace ou même à l'ouverture.

Différents instruments et méthodes sont employés pour déterminer l'état de certains agents physiques, chimiques ou biologiques présents à l'intérieur et autour des espaces confinés. Ce contrôle peut être nécessaire avant l'entrée, pendant l'entrée ou au cours des travaux. Les sources d'énergie sont désactivées par verrouillage, par la pose de panneaux d'interdiction ou par d'autres procédés. Une isolation à l'aide de plaques de fermeture, d'obturateurs et de bouchons, ou par des vannes doubles d'arrêt et de purge ou d'autres types de vannes, empêche la pénétration des substances dans les tuyauteries. Une aération au moyen de ventilateurs et de conduits d'aspiration est souvent nécessaire pour assurer un environnement de travail sûr, éventuellement complétée par une protection respiratoire homologuée. L'évaluation et le contrôle des autres conditions reposent sur les capacités de jugement de l'évaluateur.

La dernière partie du processus est la plus critique. L'évaluateur doit décider si les risques liés à l'entrée et aux travaux sont acceptables. La prévention est la meilleure façon d'assurer la sécurité. S'il est possible de maîtriser les conditions dangereuses ou risquant de le devenir, la décision est simple. Plus cette maîtrise semble difficile, plus il faut prendre de précautions, la seule autre solution étant d'interdire l'entrée.

Le contrôle de l'entrée

Les solutions habituelles aux problèmes posés par les activités en espace confiné sont l'établissement d'un permis d'entrée et la présence sur les lieux d'une personne qualifiée. Tous deux nécessitent une définition claire de la ligne hiérarchique et des responsabilités de la personne qualifiée, des personnes qui pénètrent dans l'espace confiné et de celles qui restent à l'extérieur, des équipes de secours et de la direction.

La fonction d'un document d'entrée est d'informer et de justifier. Le tableau 58.14 fournit une base formelle pour évaluer les risques et justifier les résultats de cette évaluation. Lorsqu'il est préparé pour comporter uniquement les informations correspondant à une situation particulière, il constitue la base d'un permis ou d'un certificat d'entrée. En vue d'une efficacité maximale, le permis d'entrée devrait prendre la forme d'un récapitulatif renseignant sur les actions entreprises et mentionnant les mesures de sécurité supplémentaires à adopter le cas échéant. Il devrait être délivré par une personne qualifiée et qui soit également habilitée à le retirer si les circonstances l'exigent. La personne qui le délivre devrait être indépendante de la hiérarchie, afin d'éviter toute pression en vue d'accélérer l'exécution des travaux. Le permis spécifiera les procédures à respecter ainsi que les conditions dans lesquelles on pourra pénétrer et exécuter le travail, et il permettra de consigner les résultats des tests ainsi que d'autres informations. Le permis signé sera apposé à l'entrée ou au point d'accès à l'espace, ou à tout autre emplacement fixé par l'entreprise ou par une autorité compétente. Il restera affiché jusqu'à la fin des travaux ou jusqu'à ce qu'il soit annulé ou remplacé. Une fois ceux-ci terminés, le permis devient un document qui doit être conservé conformément aux dispositions réglementaires.

Le système du permis fonctionne de façon optimale lorsque les conditions dangereuses sont connues et que des essais ont démontré l'efficacité des mesures de sécurité correspondantes. Il permet une répartition efficace des compétences. Le permis trouve ses limites en présence de risques inconnus jusque-là. Si la personne qualifiée n'est pas disponible, on risque de ne pas pouvoir parer à ces dangers.

Le certificat d'entrée est un autre mécanisme de contrôle des entrées. Il nécessite la présence d'une personne qualifiée qui apportera son savoir-faire pour l'identification, l'évaluation et la maîtrise des risques. La possibilité de réagir rapidement aux cas préoccupants et de traiter les risques imprévus est un avantage supplémentaire. Certaines réglementations imposent que la personne qualifiée procède à une inspection visuelle de l'espace avant le début des travaux. A la suite de l'évaluation des conditions régnant dans l'espace et de la mise en place des mesures de prévention, la personne qualifiée délivrera un certificat décrivant l'état de l'espace et les conditions dans lesquelles les travaux peuvent être entrepris (NFPA, 1993). Cette manière de procéder convient parfaitement aux opérations portant sur un grand nombre d'espaces confinés ou sur des espaces dont les conditions ou la configuration sont susceptibles de changer rapidement.

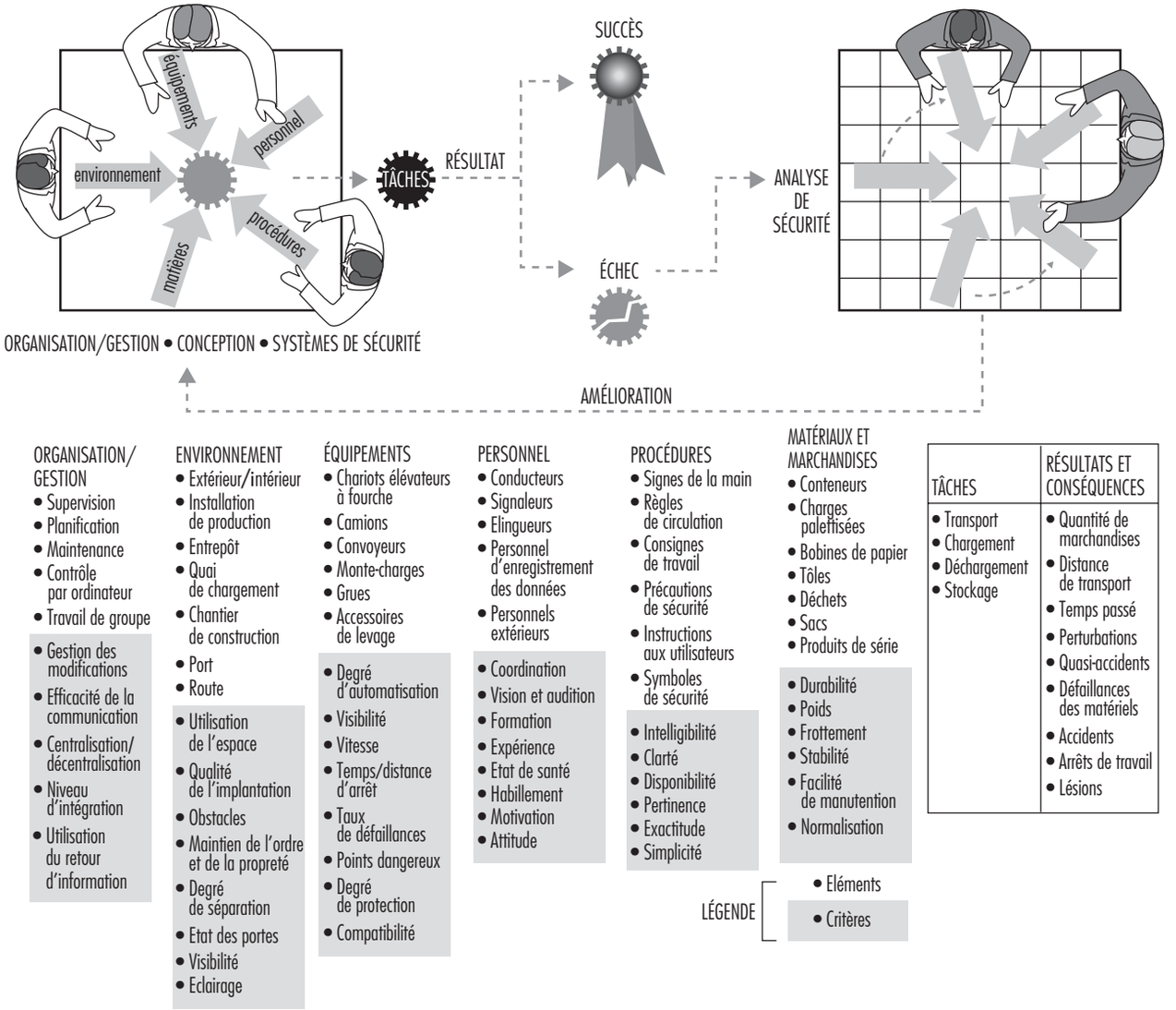
LA MANUTENTION ET LA CIRCULATION INTERNE: PRINCIPES DE PRÉVENTION

Kari K. Häkkinen

La manutention des matériaux et la circulation interne sont des facteurs qui contribuent à une grande partie des accidents dans de nombreux secteurs d'activité. Selon le secteur considéré, la proportion d'accidents du travail attribuables à la manutention des matériaux varie de 20 à 50%. La maîtrise des risques liés à la manutention des matériaux est le principal problème de sécurité dans les activités portuaires, le bâtiment, les entrepôts, les scieries, les chantiers navals et d'autres industries lourdes similaires. Dans un grand nombre d'industries de transformation, comme la chimie, l'industrie du papier, les aciéries ou les fonderies, de nombreux accidents continuent de se produire au cours de la manutention des produits finis, manuellement ou à l'aide de chariots élévateurs ou de grues.

Ce fort potentiel d'accidents de manutention s'explique par trois caractéristiques fondamentales au moins:

Figure 58.103 • Système de manutention de matériaux



- Le transport et la manutention mettent en œuvre des niveaux d'énergie potentielle et cinétique élevés qui peuvent facilement occasionner des lésions et des dommages matériels.
- Le transport et la manutention continuent de nécessiter un personnel relativement nombreux qui est fréquemment exposé aux risques liés à ces activités.
- Dans toutes les circonstances où plusieurs opérations de manutention doivent être effectuées simultanément et nécessitent une coopération dans des environnements de nature variée, il est impératif de pouvoir disposer en temps voulu d'informations claires. Si ce n'est pas le cas, la probabilité d'erreurs ou d'omissions humaines de toutes sortes est élevée et peut alors créer des situations dangereuses.

Les accidents de manutention de matériaux

Un risque d'accident est présent chaque fois que des personnes ou des machines déplacent des charges. L'ampleur du risque dépend des caractéristiques technologiques et organisationnelles du processus de travail, de l'environnement et des mesures de prévention mises en œuvre. Pour les besoins de la sécurité, il est utile de représenter la manutention de matériaux sous la forme d'un système dont les différents éléments sont liés (voir figure 58.103). Chaque fois que des changements sont apportés à un élément quelconque de ce système (matériaux, équipements, marchandises, procédures, environnement, personnel, gestion ou organisation), le risque d'accident est susceptible de changer lui aussi.

Les accidents de manutention de matériaux et de circulation interne les plus fréquents sont associés à la manutention manuelle, aux transports et aux déplacements faisant intervenir l'énergie humaine (chariots, bicyclettes, etc.) ou effectués au moyen de camions, de chariots élévateurs, de grues, de palans, de convoyeurs ou de véhicules sur rails.

Plusieurs types d'accidents se produisent couramment dans le transport et la manutention de charges sur les lieux de travail. Voici les plus fréquents:

- foulures à l'occasion de manutentions manuelles;
- chutes de charges sur des personnes;

- personnes prises entre des objets;
- collisions entre des équipements;
- chutes de personnes;
- blessures par coups, chocs et coupures causés par les équipements ou les charges;
- efforts excessifs lors du soulèvement de charges pesantes.

Les éléments des systèmes de manutention

Chacun des éléments d'un système de manutention de matériaux peut être conçu de différentes manières; chacune d'elles entraîne des risques différents. Plusieurs critères de sécurité sont à prendre en compte pour chaque élément. Il est important d'adopter une approche orientée vers le système dans son ensemble pendant toute la durée de vie utile de celui-ci, c'est-à-dire lors de sa conception, de son utilisation normale et du suivi des accidents et perturbations antérieurs, si l'on veut pouvoir y apporter des améliorations.

Les principes généraux de prévention

Certains principes généraux de prévention sont considérés comme applicables à la sécurité dans la manutention de matériaux. Ils s'appliquent à la fois aux systèmes manuels et mécaniques de manutention, aussi bien dans le cadre d'une usine que dans celui d'un entrepôt ou d'un chantier. De nombreux principes doivent être mis en œuvre au sein d'un même projet pour obtenir une sécurité optimale, une seule mesure ne suffisant en principe pas à prévenir entièrement les accidents. A l'inverse, ces principes généraux ne sont pas tous nécessaires, et certains peuvent ne pas convenir à une situation spécifique. Les professionnels de la sécurité et les spécialistes de la manutention des matériaux devraient considérer les éléments les plus pertinents dans chaque cas particulier pour orienter leurs études. Le plus important est d'exploiter au mieux ces principes afin de créer des systèmes de manutention des matériaux sûrs et commodes, plutôt que de se décider pour une seule technique à l'exclusion de toute autre.

Les 22 principes mentionnés ci-après peuvent être appliqués à la mise au point et à l'évaluation des systèmes de manutention des matériaux à des fins de sécurité au stade de la planification ou dans leur état présent ou passé. Tous sont applicables aux actions de sécurité décidées a priori ou a posteriori. La liste qui suit ne suppose aucun ordre de priorité rigoureux, mais il est possible de distinguer sommairement les premiers principes — qui concernent davantage la conception initiale des nouvelles installations et des nouveaux procédés de manutention des matériaux — des derniers, qui sont orientés plutôt vers les méthodes existantes de manutention des matériaux.

Vingt-deux principes de prévention des accidents de manutention

1. *Eliminer toutes les opérations de transport et de manutention qui ne sont pas indispensables.* Etant donné le danger inhérent à de nombreuses opérations de transport et de manutention, il est utile d'examiner si certaines d'entre elles ne pourraient pas être supprimées ou modifées. Un grand nombre de procédés de fabrication modernes peuvent être organisés en flux continu, sans séparation entre les phases de manutention et de transport. De nombreuses opérations d'assemblage et de construction peuvent être planifiées et conçues de façon à supprimer des mouvements pénibles et difficiles. On peut également trouver des solutions plus efficaces et plus rationnelles en analysant la logistique et les flux de matières dans les processus de fabrication et de transport.
2. *Tenir les personnes à l'écart des zones de transport et de manutention.* Lorsque les travailleurs ne se trouvent pas sous les charges à déplacer ou à proximité, les conditions de sécurité sont ipso facto améliorées du fait d'une moindre exposition au danger. Dans les aciéries, il est interdit au personnel de pénétrer dans la zone de manutention de ferraille, parce que les électroaimants employés pour ce type de transport présentent un risque permanent de chute des charges transportées. Il est souvent possible d'automatiser la manutention de matériaux dans des environnements agressifs grâce à des robots et des chariots automatiques, et de réduire ainsi l'exposition des travailleurs aux risques d'accidents liés aux charges en mouvement. En outre, en interdisant au personnel de traverser sans nécessité les aires de chargement et de déchargement, on supprime pratiquement plusieurs autres risques liés à la manutention des matériaux.
3. *Séparer au maximum les opérations de transport pour limiter les collisions.* Plus il y a de possibilités de rencontres entre véhicules, ou entre des véhicules et des équipements ou des personnes, plus la probabilité de collision augmente. La séparation des opérations de transport est un élément important des activités de planification en vue d'assurer des transports intérieurs sûrs. De nombreuses séparations peuvent être envisagées — entre piétons et véhicules, véhicules lourds et véhicules légers, circulation interne et circulation en direction ou à partir de l'extérieur, transport entre différents lieux de travail et manutention des matériaux dans un même lieu de travail, transport et stockage, transport et ligne de production, réception et expédition, transport des matières dangereuses et transports courants, etc.

   Lorsqu'une séparation spatiale n'est pas possible, on peut affecter aux engins de transport et aux piétons des horaires d'accès différents à une zone de travail (par exemple, dans un entrepôt ouvert au public). S'il n'est pas possible d'aménager des passages séparés pour les piétons, leurs itinéraires pourront être signalés par des panneaux ou des marquages. A l'entrée des bâtiments d'usine, des portes piétonnes séparées devraient être prévues pour le personnel. Si la circulation des piétons se mélange à celle des chariots élévateurs au droit des portes, elles auront aussi tendance à se mélanger au-delà, ce qui crée un risque. Lors des travaux de transformation, il est souvent nécessaire de limiter les déplacements des engins et des personnes dans les zones intéressées. Dans le cas des transports par ponts roulants, on évitera les collisions en aménageant des cheminements sans chevauchement et en installant des contacteurs de fin de course et des barrières mécaniques.
4. *Affecter un espace suffisant à la manutention des matériaux et au transport.* L'exiguïté des espaces de manutention des matériaux est souvent une cause d'accidents. Les mains peuvent par exemple se trouver prises entre une charge et un mur dans les opérations de manutention manuelle, ou une personne peut être coincée entre le poinçon d'une grue mobile et une pile de marchandises si la distance de sécurité minimale de 0,5 m n'a pas été respectée. L'espace nécessaire aux opérations de transport et de manutention devrait être soigneusement pris en compte dans la conception des installations et la planification des modifications. Il est recommandé de réserver une certaine marge de sécurité pour pouvoir tenir compte des modifications futures dans les dimensions des charges ou les types de matériels. Il arrive fréquemment que le volume des produits fabriqués ait tendance à augmenter avec le temps, alors que l'espace affecté à leur manutention diminue constamment. Bien que la recherche d'une rentabilisation de l'espace consacré à la production soit l'une des raisons qui incitent à le réduire, il ne faut pas oublier que l'espace nécessaire à certains chariots élévateurs pour tourner et repartir en sens opposé est plus important qu'il n'apparaît au premier abord.

5. *Rechercher la continuité des opérations de transport et éviter les solutions de continuité dans la manutention des matériaux*. La continuité des flux de matières réduit les risques d'accidents; l'agencement de base d'une installation est déterminant pour l'application de ce principe de sécurité. Les accidents ont tendance à se produire plus volontiers là où la circulation des matières est interrompue en raison d'un changement d'équipement ou pour des raisons propres à la production. L'intervention humaine est souvent nécessaire, notamment pour charger, décharger, attacher, emballer, soulever ou tirer des charges. La nature des matières manutentionnées joue un rôle, mais on peut dire, d'une manière générale, que les convoyeurs assurent des flux plus continus que les ponts roulants ou les chariots élévateurs. Une bonne planification consiste à organiser les opérations de transport de telle sorte que les véhicules motorisés circulent dans les locaux de l'usine selon un itinéraire circulaire à sens unique, sans déplacement en zigzag ou marche arrière. Etant donné que des solutions de continuité tendent à apparaître aux limites séparant deux services ou deux cellules de fabrication, la production et le transport devraient être organisés de manière à éviter ces «no man's lands».
6. *Utiliser des éléments standards dans les systèmes de manutention des matériaux*. Il est généralement préférable pour la sécurité d'employer des charges, des équipements et des outils standards dans la manutention des matériaux. La notion d'unité de charge est bien connue des professionnels du transport. Les matériaux regroupés en conteneurs ou sur palettes sont plus faciles à arrimer et à déplacer lorsque les autres éléments de la chaîne de transport (rayons de stockage, chariots élévateurs, véhicules à moteur et dispositifs d'accrochage sur les grues) sont conçus pour ces unités de charge. L'utilisation de chariots élévateurs de modèles standards, avec des commandes semblables, réduit la probabilité d'erreurs des conducteurs; il est arrivé en effet que des accidents se produisent lorsqu'un conducteur passe d'un engin à un autre ayant des commandes différentes.
7. *Connaître les matériaux à manutentionner*. La connaissance des caractéristiques des matériaux à transporter est une condition préalable à la sécurité des manutentions. Pour choisir des dispositifs de levage ou de préhension appropriés, on doit tenir compte du poids, de la position du centre de gravité et des dimensions des charges à soulever ou transporter. Pour la manutention des matières dangereuses, il est nécessaire de disposer d'informations sur leur réactivité, leur inflammabilité et leur toxicité. Les produits fragiles, tranchants, pulvérulents, visqueux ou mal assujettis présentent des risques particuliers, de même que les substances explosives ou les animaux vivants, par exemple. Les emballages fournissent souvent des indications importantes sur les méthodes de manutention correctes, mais il arrive que des étiquettes disparaissent, ou que des emballages protecteurs masquent des informations essentielles. Il n'est pas non plus toujours possible de voir comment est réparti le contenu d'un emballage et donc de situer correctement l'emplacement de son centre de gravité.
8. *Maintenir une marge de sécurité*. Les surcharges sont une cause fréquente d'accidents dans les systèmes de manutention des matériaux. Les charges maximales admissibles des élingues et autres dispositifs de levage devraient être clairement marquées et on prendra soin de choisir ceux qui conviennent. Les erreurs d'appréciation (poids, centre de gravité) des charges peuvent conduire à des surcharges et à des arrimages et des manœuvres inappropriés. Dans le cas d'une manutention à l'aide d'élingues, l'opérateur doit avoir conscience que, lorsque l'engin se déplace sur une surface inclinée, les forces qui s'exercent peuvent suffire à libérer la charge ou à déséquilibrer l'engin. La limite de charge devrait être indiquée sur les chariots élévateurs. Elle varie en fonction de la hauteur de levage et des dimensions de la charge. Une rupture par fatigue peut se produire dans le cas d'opérations répétées avec des charges très inférieures à la charge de rupture nominale si le matériel en cause n'est pas conçu pour résister à ce type de défaillance.
9. *Fixer des limites de vitesse suffisamment basses pour préserver la sécurité des déplacements*. Les limites de vitesse des véhicules se déplaçant sur les lieux de travail varient de 10 à 40 km/h. Ces vitesses devraient être encore réduites dans les couloirs intérieurs, au passage des portes, aux intersections et dans les allées étroites. Un bon conducteur sait adapter la vitesse de son véhicule à chaque situation, mais il est recommandé de prévoir des panneaux de limitation de vitesse aux endroits critiques. La vitesse maximale d'une grue mobile commandée à distance, par exemple, devrait être déterminée en fixant une vitesse comparable à celle d'un homme marchant au pas et en tenant compte également du temps nécessaire à la surveillance simultanée des charges, de manière à ne pas dépasser le temps de réaction de l'opérateur.
10. *Eviter les opérations de levage lorsque des personnes risquent de se trouver sous la charge*. Le levage de matériaux s'accompagne toujours d'un risque de chute des charges. Il est normalement interdit de travailler sous des charges suspendues, mais il arrive couramment que des charges soient transportées au-dessus du personnel dans les opérations de production, ce qui présente un danger. Le transport par chariots élévateurs jusqu'à des rayonnages élevés et le levage entre étages sont d'autres exemples de levage à grande hauteur. Les convoyeurs aériens transportant des roches, du coke ou des pièces de coulée peuvent également présenter des risques de chutes de charges pour les personnes travaillant au-dessous s'ils ne sont pas équipés de carters de protection. Lorsqu'on envisage l'installation d'un système de transport surélevé, on devrait tenir compte du fait qu'il présente des risques potentiels supérieurs à ceux d'un système au niveau du sol.
11. *Eviter les méthodes de manutention des matériaux qui imposent de grimper et de travailler en hauteur*. Il existe un risque de chute chaque fois que le personnel doit grimper, par exemple pour détacher des élingues, bâcher un véhicule ou porter des inscriptions sur des charges. Une meilleure organisation, une modification du déroulement des opérations, l'emploi d'accessoires de levage différents et d'outils commandés à distance ou le recours à la mécanisation et à l'automatisation permettent souvent d'éviter ces risques.
12. *Fixer des protections aux emplacements dangereux*. Des protections devraient être installées aux points dangereux des équipements de manutention, comme les chaînes des chariots élévateurs, les mécanismes d'entraînement des câbles des grues et les angles rentrants des tambours de convoyeurs. Dans de nombreux cas, il ne suffit pas de placer ces points dangereux hors de portée, étant donné qu'il reste possible de les atteindre avec une échelle ou par d'autres moyens. Les protections offrent également une sécurité contre les défaillances techniques pouvant occasionner un accident (par exemple, les retenues de câble sur les poulies des grues, les clavettes de sûreté sur les crochets de levage ou les gaines entourant les élingues en textile pour les protéger contre les parties coupantes). Les garde-corps et les plinthes installés au bord des plates-formes de chargement et des rayons de stockage en hauteur et autour des ouvertures dans les sols empêchent les chutes d'objets ou de personnes. Ce genre de protection est souvent nécessaire dans le cas du levage, par grues ou chariots élévateurs, entre différents étages. Dans les opérations de manutention des matériaux, le personnel peut être protégé contre les chutes d'objets par des filets de sécurité, par des grillages ou par des carters métalliques.

13. *N'utiliser pour le levage et le transport des personnes que les équipements prévus à cet effet.* Les grues, les chariots élévateurs, les pelles mécaniques et les convoyeurs sont destinés à déplacer des matériaux et non des personnes. Il existe des plates-formes spéciales pour soulever les personnes, par exemple lorsqu'on doit réparer un éclairage au plafond. On peut également se servir, sans risque excessif d'accident grave, d'un engin élévateur équipé d'une cage spéciale répondant aux critères de sécurité requis.
14. *Veiller à la stabilité des engins et des charges.* Des accidents se produisent lorsque des engins (en particulier des chariots élévateurs ou des grues mobiles), des marchandises ou des rayonnages deviennent instables. Le choix d'équipements à stabilisation active est une première étape dans la réduction des risques. Il est en outre recommandé d'employer des équipements qui émettent un signal sonore avant que la charge utile admissible ne soit dépassée. De bonnes pratiques de travail et des opérateurs qualifiés font également partie de la prévention. Un personnel suffisamment expérimenté et formé est capable d'évaluer la position des centres de gravité, de reconnaître les empilements instables et de prendre les mesures adéquates.
15. *Assurer une bonne visibilité.* La manutention au moyen de chariots élévateurs a toujours pour effet de limiter la visibilité. Lors de l'achat d'un nouveau véhicule, il importe de vérifier le champ de vision dont dispose l'opérateur à travers les structures du mât (et pour les chariots à grande levée, à travers le cadre supérieur). Quoi qu'il en soit, les matériaux soulevés entraînent une certaine perte de visibilité, et cela doit être pris en compte. On devrait, autant que possible, assurer un champ de vision dégagé, par exemple en ménageant des ouvertures ou des espaces libres à certains endroits critiques des rayonnages et entre les piles de marchandises. Des miroirs peuvent être installés sur les engins ainsi qu'à des emplacements appropriés pour rendre les angles morts moins dangereux. Les miroirs ne sont toutefois qu'un moyen de prévention secondaire par rapport à l'élimination effective des angles morts pour permettre une vision directe. Pour les déplacements par grue, il est souvent nécessaire de charger quelqu'un de s'assurer que personne ne se trouve dans la zone où la charge doit être déposée. Une bonne pratique de sécurité consiste à peindre ou à signaler par d'autres moyens les points dangereux et les obstacles présents dans l'environnement de travail, comme les piliers, les encadrements de portes et les bords des quais de déchargement, les éléments saillants des machines ou les parties mobiles des engins de manutention. Un bon éclairage apporte souvent une amélioration considérable de la visibilité, par exemple dans les escaliers et les couloirs ou aux portes.
16. *Remplacer le soulèvement et le transport manuels des charges par des systèmes mécaniques automatisés.* Près de 15% de tous les accidents du travail sont associés au soulèvement ou au transport manuels de charges. La plupart sont dus à un effort excessif, le reste étant constitué de glissades et de chutes ou de lésions des mains par des arêtes vives. Les troubles consécutifs aux traumas cumulatifs et les dorsalgies sont des problèmes de santé typiques de la manutention manuelle. Bien que la mécanisation et l'automatisation aient supprimé un grand nombre de tâches de manutention manuelle dans l'industrie, il existe encore des lieux de travail où les personnes doivent effectuer des efforts physiques excessifs en soulevant et en transportant de lourdes charges. On devrait envisager de mettre à disposition des équipements de manutention appropriés tels que palans, plates-formes de levage, monte-charges, chariots élévateurs, ponts roulants, convoyeurs, palettiseurs, robots ou manipulateurs mécaniques.
17. *Instaurer et entretenir une communication efficace.* Un grand nombre d'accidents graves ont pour origine un manque de communication. Le grutier doit pouvoir communiquer avec l'élingueur qui attache la charge; si leurs signaux sont ambigus ou erronés ou si les liaisons radio sont mauvaises, il peut en résulter des erreurs lourdes de conséquences. Les communications sont un élément important entre le personnel de manutention, le personnel de production, les chargeurs, les dockers, les conducteurs d'équipements et le personnel de maintenance. Ainsi, lors du changement d'équipe, le conducteur d'un chariot élévateur doit informer celui qui le remplace quant aux problèmes qu'il a pu rencontrer, comme les angles morts dus à des empilements de marchandises dans les allées. Les conducteurs de véhicules à moteur ou de grues mobiles qui ne font pas partie du personnel d'entreprise ont souvent une connaissance insuffisante des risques particuliers qu'ils peuvent rencontrer; ils devraient par conséquent recevoir des conseils et une formation spéciale. On pourrait, par exemple, leur remettre à l'entrée un plan des lieux accompagné des principales consignes de sécurité. Les panneaux de signalisation sont moins fréquents sur les lieux de travail que sur les voies publiques, bien qu'une large part des risques rencontrés dans la circulation routière soient également présents dans les installations industrielles. Il est donc important de prévoir des panneaux pour la circulation interne afin de mieux signaler les dangers et d'informer les conducteurs des précautions à prendre.
18. *Organiser les interfaces humaines et la manutention manuelle selon les principes de l'ergonomie.* Les travaux de manutention de matériaux devraient être adaptés aux capacités et aux qualifications des personnes appelées à les exécuter, afin d'éviter les erreurs et les efforts inutiles. Les commandes et les tableaux de bord des grues et des chariots élévateurs devraient être compatibles avec les attentes normales et les habitudes des utilisateurs. En manutention manuelle, on devrait veiller à ce qu'il existe un espace suffisant pour permettre les mouvements nécessaires à l'exécution des tâches. On devrait éviter les postures de travail excessivement pénibles, par exemple le levage manuel au-dessus du niveau de la tête, et les charges ne devraient pas dépasser le maximum autorisé. Les différences interindividuelles (âge, force, mensurations, état de santé, expérience) peuvent imposer une modification correspondante des espaces de travail et des tâches. La desserte manuelle des installations de magasinage est un exemple de tâche où l'ergonomie revêt une extrême importance pour la sécurité et la productivité.
19. *Fournir une formation et des conseils appropriés.* Les tâches de manutention sont souvent considérées comme étant d'un niveau trop inférieur pour justifier une formation spéciale du personnel. Les effectifs de grutiers et de caristes spécialisés sont en diminution dans les entreprises et il existe une tendance croissante à considérer la conduite de ces engins comme une tâche pratiquement à la portée de tout le monde. Bien que des mesures techniques et ergonomiques permettent de réduire les dangers, c'est le savoir-faire de l'opérateur qui s'avère en fin de compte décisif pour éviter les situations dangereuses dans un environnement de travail aussi dynamique. Les enquêtes sur les accidents ont révélé qu'un grand nombre des victimes d'accidents de manutention n'étaient pas elles-mêmes impliquées dans ces tâches. Il faudrait donc que les autres personnes présentes dans les zones de manutention bénéficient également d'une certaine formation.
20. *Fournir au personnel affecté au transport et à la manutention des équipements individuels appropriés.* Plusieurs types de lésions peuvent être prévenus grâce à des équipements de protection individuelle adaptés. Les chaussures de sécurité antidérapantes et à

embout d'acier, les gants épais, les lunettes et les casques de protection sont des équipements habituels pour les tâches de manutention. Lorsque des risques particuliers l'exigent, des protections contre les chutes, des appareils de protection respiratoire et des vêtements spéciaux sont également utilisés. Un équipement individuel approprié pour les tâches de manutention devrait assurer une bonne visibilité et ne pas comporter d'éléments qui pourraient facilement s'accrocher au matériel ou se prendre dans les parties mobiles des engins.

21. *Assurer une maintenance et des vérifications adéquates.* Lorsque des accidents se produisent en raison de défaillances du matériel, on découvre souvent que celles-ci sont dues à des procédures de maintenance et de vérification insuffisantes. Les instructions concernant la maintenance et les inspections figurent dans les normes de sécurité et dans les manuels des constructeurs. Le non-respect des procédures indiquées peut conduire à des situations dangereuses. Les utilisateurs des engins de manutention sont responsables de la maintenance et des vérifications courantes, comme le contrôle des batteries, des entraînements de câbles et de chaînes, des dispositifs de levage, des freins et des commandes, le nettoyage des vitres et les apports d'huile, si nécessaire. Des vérifications plus approfondies et moins fréquentes sont effectuées à des intervalles réguliers d'une semaine, d'un mois, d'un semestre ou d'un an, selon les conditions d'utilisation. L'ordre et la propreté, y compris un nettoyage adéquat des sols et des lieux de travail, sont également importants pour la sécurité de la manutention. Les sols gras ou mouillés provoquent des chutes de personnes et des dérapages d'engins. Les palettes et les rayonnages brisés devraient être immédiatement mis au rebut. Dans les opérations impliquant un transport de matières en vrac sur des convoyeurs, il est important d'éliminer les dépôts de poussières pour éviter les explosions et les feux de poussière.
22. *Inclure les changements de conditions ambiantes dans la planification.* Les équipements, comme les personnes, n'ont qu'une capacité d'adaptation limitée aux variations de l'environnement. Les caristes ont besoin de plusieurs secondes pour s'adapter lorsqu'ils passent de l'intérieur d'un bâtiment obscur à une cour ensoleillée ou inversement. Pour assurer une meilleure sécurité, il est possible d'installer un éclairage spécial à proximité des portes. En plein air, les grues sont souvent exposées à des vents forts dont il faut tenir compte lors des opérations de levage. Par vent trop violent, le levage par grue devrait être totalement interrompu. La glace et la neige peuvent occasionner un surcroît de travail considérable pour le personnel, qui doit nettoyer la surface des charges. Cela conduit parfois à prendre des risques supplémentaires, par exemple lorsque ce travail est fait en se plaçant sur la charge ou au-dessous d'une charge soulevée. La planification devrait concerner également les méthodes de sécurité relatives à ces tâches. Une charge recouverte de glace peut glisser à l'extérieur de la fourche lors de son transport par chariot élévateur. Enfin, les atmosphères corrosives, la chaleur, le gel et l'eau de mer peuvent détériorer les matériels et occasionner par la suite des pannes si ces matériels n'ont pas été prévus pour résister à ces conditions.

Références bibliographiques

Arteau, J., Lan, A. et Corbeil, J.F., 1994: *Use of Horizontal Lifelines in Structural Steel Erection*. Proceedings of the International Fall Protection Symposium, San Diego, California (October 27–28, 1994) (Toronto, International Society for Fall Protection).

Backström, T., 1996: «Accident risk and safety protection in automated production», thèse de doctorat, *Arbete och Hälsa*, vol. 7 (Solna, National Institute for Working Life).

Backström, T. et Döös, M., 1994: «Technical defects behind accidents in automated production», dans P.T. Kidd et W. Karwowski (directeurs de publication): *Advances in Agile Manufacturing: Integrating Technology, Organization and People* (Amsterdam, IOS Press).

—. 1995: «A comparison of occupational accidents in industries with of advanced manufacturing technology», *International Journal of Human Factors in Manufacturing*, vol. 5, nº 3, pp. 267-282.

—. 1997a: «The technical genesis of machine failures leading to occupational accidents», *International Journal of Industrial Ergonomics*, vol. 19, pp. 361-376.

—. 1997b: «Absolute and relative frequencies of automation accidents at different kinds of equipment and for different occupational groups», *Journal of Safety Research*, vol. 28, nº 3, pp. 147-158.

Backström, T. et Harms-Ringdahl, L., 1984: «A statistical study of control systems and accidents at work», *Journal of Occupational Accidents*, vol. 6, pp. 201-210.

Bainbridge, L., 1983: «Ironies of automation», *Automatica*, vol. 19, pp. 775-779.

Bell, R. et Reinert, D., 1992: «Risk and system integrity concepts for safety related control systems», *Safety Science*, vol. 15, pp. 283-308.

Bouchard, P., 1991: *Echafaudages.* Guide série 4 (Montréal, Commission de la santé et de la sécurité du travail (CSST)).

Bureau international du Travail (BIT), 1976: *Sécurité dans la construction et l'utilisation des tracteurs. Recueil de directives pratiques* (BIT, Genève).

—. 1981: *Sécurité et hygiène dans les travaux agricoles. Recueil de directives pratiques*, 2e édition (BIT, Genève).

Commission électrotechnique internationale (CEI), 1992: *122 Draft Standard: Software for Computers in the Application of Industrial Safety-related Systems*, CEI 65 (Sec) (Genève).

—. 1998-2000: *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité. Parties 1 à 7*, CEI 1508 (Genève).

Communauté économique européenne (CEE), 1979, 1982, 1985, 1987, 1988, 1994, 1999: *Directive 79/622/CEE du Conseil, du 25 juin 1979, concernant le rapprochement des législations des Etats membres relatives aux dispositifs de protection en cas de renversement des tracteurs agricoles ou forestiers à roues (essais statiques)* (Bruxelles).

—. 1989: *Directive 89/392/CEE du Conseil, du 14 juin 1989, concernant le rapprochement des législations des Etats membres relatives aux machines, modifiée par la directive 93/44/CEE, du 14 juin 1993, et par la directive 98/37/CE, du 22 juin 1998* (Luxembourg).

Corbett, J.M., 1988: «Ergonomics in the development of human-centred AMT», *Applied Ergonomics*, vol. 19, nº 1, pp. 35-39.

Culver, C. et Connolly, C., 1994: «Prevent fatal falls in construction», *Safety and Health*, sept., pp. 72-75.

Deutsche Industrie Normen (DIN), 1990: *Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben*, DIN V VDE 0801 (Berlin, Beuth Verlag GmbH).

—. 1994: *Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben; Änderung A1*, DIN V VDE 0801/A1 (Berlin, Beuth Verlag GmbH).

—. 1995: *Nutzkraftwagen und Anhängefahrzeuge — Rangier-Warneinrichtungen — Anforderungen und Prüfung*, DIN 75031 (Berlin, Beuth Verlag GmbH).

—. 1997: *Sicherheit von Maschinen — Druckempfindliche Schutzeinrichtungen — Teil 1: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schaltmatten und Schaltplatten*, DIN EN 1760-1 (Berlin, Beuth Verlag GmbH).

Döös, M. et Backström, T., 1993: «Description of accidents in automated materials handling», dans W.S. Marras, W. Karwowski, J.L. Smith et L. Pacholski (directeurs de publication): *Ergonomics of Materials Handling and Information Processing at Work* (Varsovie, Taylor and Francis).

—. 1994: «Production disturbances as an accident risk», dans *Advances in Agile Manufacturing: Integrating Technology, Organization and People, op. cit.*

Etherton, J.R. et Myers, M.L., 1990: «Machine safety research at NIOSH and future directions», *International Journal of Industrial Ergonomics*, vol. 6, pp. 163-174.

Freund, E., Dierks, F. et Rossmann, J., 1993: *Untersuchungen zum Arbeitsschutz bei Mobilen Robotern und Mehrrobotersystemen* (Dortmund, Schriftenreihe der Bundesanstalt für Arbeitsschutz).

Goble, W., 1992: *Evaluating Control System Reliability* (New York, Instrument Society of America).

Goodstein, L.P., Anderson, H.B. et Olsen, S.E. (directeurs de publication), 1988: *Tasks, Errors and Mental Models* (Londres, Taylor and Francis).

Health and Safety Executive (HSE), 1989: «Health and safety statistics 1986-87», *Employment Gazette* (Londres), vol. 97, nº 2.

Hollnagel, E. et Woods, D., 1983: «Cognitive systems engineering: New wine in new bottles», *International Journal of Man-Machine Studies*, vol. 18, pp. 583-600.

Hölscher, H. et Rader, J., 1984: *Mikrocomputer in der Sicherheitstechnik* (Cologne, Verlag TÜV Rheinland).

Hörte, S.Å. et Lindberg, P., 1989: *Diffusion and Implementation of Advanced Manufacturing Technologies in Sweden*. IMIT Working Paper No. 16, Institute for Management of Innovation and Technology (IMIT), Göteborg.

Johnson, B., 1989: *Design and Analysis of Fault Tolerant Digital Systems* (New York, Addison Wesley).

Kidd, P.T., 1994: «Skill-based automated manufacturing», dans W. Karwowski et G. Salvendy (directeurs de publication): *Organization and Management of Advanced Manufacturing Systems* (New York, Wiley).

Knowlton, R.E., 1986: *An Introduction to Hazard and Operability Studies: The Guide Word Approach* (Vancouver, Colombie-Britannique, Chemetics).

Kuivanen, R., 1990: «The impact on safety of disturbances in flexible manufacturing systems», dans W. Karwowski et M. Rahimi (directeurs de publication): *Ergonomics of Hybrid Automated Systems II* (Amsterdam, Elsevier).

Laeser, R.P., McLaughlin, W.I. et Wolff, D.M., 1987: «Fernsteuerung und Fehlerkontrolle von Voyager 2», *Spektrum der Wissenschaft*, nº 1, pp. S 60-70.

Lan, A., Arteau, J. et Corbeil, J.F., 1994: *Protection Against Falls from Above-ground Billboards*. Proceedings of the International Fall Protection Symposium, San Diego, Californie (October 27-28, 1994) (Toronto, International Society for Fall Protection).

Langer, H.J. et Kurfürst, W., 1985: *Einsatz von Sensoren zur Absicherung des Rückraumes von Grossfahrzeugen*, FB 605 (Dortmund, Schriftenreihe der Bundesanstalt für Arbeitsschutz).

Levenson, N.G., 1986: «Software safety: Why, what, and how», *ACM Computer Surveys*, nº 2, pp. S 129-163.

McManus, T.N., non daté, *Confined Spaces*, manuscrit.

Mester, U., Herwig, T., Dönges, G., Brodbeck, B., Bredow, H.D., Behrens, M. et Ahrens, U., 1980: *Gefahrenschutz durch passive Infrarot-Sensoren (II)* FB 243 (Dortmund, Schriftenreihe der Bundesanstalt für Arbeitsschutz).

Mohan, D. et Patel, R., 1992: «Design of safer agricultural equipment: Application of ergonomics and epidemiology», *International Journal of Industrial Ergonomics*, vol. 10, nº 4, pp. 301-310.

National Fire Protection Association (NFPA), 1993: *NFPA 306: Control of Gas Hazards on Vessels* (Quincy, Massachusetts).

National Institute for Occupational Safety and Health (NIOSH), 1994: *Worker Deaths in Confined Spaces. A Summary of NIOSH Surveillance and Investigative Findings*, DHHS (NIOSH) Publication No. 94-103 (Cincinnati, Ohio).

Neumann, P.G, 1994: «Illustrative risks to the public in the use of computer systems and related technologys», *Software Engineering Notes* (ACM Press/SIGSOFT, New York).

—. 1995: *Computer-related Risks*, Association for Computing Machinery (ACM) (ACM Press/Addison Wesley, New York).

Occupational Safety and Health Administration (OSHA), 1988: *Selected Occupational Fatalities Related to Welding and Cutting as Found in Reports of OSHA Fatality/Catastrophe Investigations* (Washington, DC).

Organisation de coopération et de développement économiques (OCDE), 1988: *Codes normalisés de l'OCDE pour les essais officiels de tracteurs agricoles* (Paris).

Organisation internationale de normalisation (ISO), 1989: *Tracteurs agricoles et forestiers à roues. Structures de protection: méthodes d'essais statiques et conditions d'acceptation*, ISO 5700 (Genève).

—. 1994a: *Véhicules utilitaires. Dispositifs de détection d'obstacles pendant la marche arrière. Exigences et essais*, ISO/TR 12155 (Genève).

—. 1994b: *Systèmes d'automatisation industrielle. Sécurité des systèmes de fabrication intégrés. Prescriptions fondamentales*, ISO 11161 (Genève).

—. 1997: *Normes pour le management de la qualité et l'assurance de la qualité. Partie 3: Lignes directrices pour l'application de l'ISO 9001:1994 au développement, à la mise à disposition, à l'installation et à la maintenance du logiciel*, ISO 9000-3 (Genève).

Organisme professionnel de prévention du bâtiment et des travaux publics (OPPBTP), 1984: *Les équipements individuels de protection contre les chutes de hauteur* (Boulogne-Billancourt).

Rasmussen, J., 1983: «Skills, rules and knowledge: Agenda, signs and symbols, and other distinctions in human performance models», *IEEE Transactions on Systems, Man and Cybernetics*, vol. 13, nº 3, pp. 257-266.

Reason, J., 1990: *Human Error* (New York, Cambridge University Press).

Reese, C.D. et Mills, G.R., 1986: «Trauma epidemiology of confined space fatalities and its application to intervention/prevention now», dans *The Changing Nature of Work and Workforce* (Cincinnati, Ohio, NIOSH).

Reinert, D. et Reuss, G., 1991: «Sicherheitstechnische Beurteilung und Prüfung mikroprozessorgesteuerter Sicherheitseinrichtungen», *BIA-Handbuch*, Sicherheitstechnisches Informations- und Arbeitsblatt 310222 (Bielefeld, Erich Schmidt Verlag).

Schreiber, P., 1990: «Entwicklungsstand bei Rückraumwarneinrichtungen», *Technische Überwachung*, nº 4, avril, S, p. 161.

Schreiber, P. et Kuhn, K., 1995: *Informationstechnologie in der Fertigungstechnik*, FB 717 (Dortmund, Schriftenreihe der Bundesanstalt für Arbeitsschutz).

Sheridan, T., 1987: «Supervisory control», dans G. Salvendy (directeur de publication): *Handbook of Human Factors* (New York, Wiley).

Society of Automotive Engineers (SAE), 1974: *Operator Protection for Industrial Equipment*, SAE Standard j1042 (Warrendale, E.-U.).

—. 1975: *Performance Criteria for Rollover Protection. SAE Recommended Practice*, SAE Standard j1040a (Warrendale, E.-U.).

Springfeldt, B., 1993: *Effects of Occupational Safety Rules and Measures with Special Regard to Injuries. Advantages of Automatically Working Solutions* (Stockholm, The Royal Institute of Technology, Department of Work Science).

Sugimoto, N., 1987: «Subjects and problems of robot safety technology», dans K. Noto (directeur de publication): *Occupational Safety and Health in Automation and Robotics* (Londres, Taylor and Francis).

Sulowski, A.C. (directeur de publication), 1991: *Fundamentals of Fall Protection* (Toronto, International Society for Fall Protection).

US Bureau of National Affairs, 1975: *Occupational Safety and Health Standards. Roll-over Protective Structures for Material Handling Equipment and Tractors, Sections 1926, 1928* (Washington, DC).

Zimolong, B. et Duda, L., 1992: «Human error reduction strategies in advanced manufacturing systems», dans M. Rahimi et W. Karwowski (directeurs de publication): *Human-robot Interaction* (Londres, Taylor and Francis).

Références complémentaires

Börner, F. et Kreutzkampf, F., 1994: «Unfälle und Störfälle, verursacht durch das Versagen von Steuerungen», *BIA-Handbuch*, Sicherheitstechnisches Informations- und Arbeitsblatt 330250 (Bielefeld, Erich Schmidt Verlag).

Bureau international du Travail (BIT), 1969: *Sécurité et hygiène dans les travaux forestiers. Recueil de directives pratiques* (BIT, Genève).

Emery, F.E., 1969: *Systems Thinking* (Harmondsworth, Royaume-Uni, Penguin).

Grams, T., 1990: *Denkfallen und Programmierfehler* (Berlin, Springer).

Gryfe, C.I., 1988: *Causes and prevention of falling*, International Fall Protection Symposium, Orlando (Toronto, International Society for Fall Protection).

Heinrich, H.W., Peterson, D. et Roos, N., 1980: *Industrial Accident Prevention*, 5e édition (New York, McGraw-Hill).

Meffert, K. et Germer, J., 1985: «Einsatz von Rechnern für Sicherheitsaufgaben — Standortbestimmung», *Die BG*, vol. 5, S, pp. 246-253.

Schreibwer, P., Becker, G. et Dicke, W., 1985: *Gefahrenschutz durch Kontaktmatten und- böden*, FB 414 (Dortmund, Schriftenreihe der Bundesanstalt für Arbeitsschutz).

System Safety Society, 1993: *System Safety Analysis Handbook* (Albuquerque, Nouveau-Mexique, New Mexico Chapter).

Thomas, M., 1988: «Should we trust computers?», dans *SHARE* (Nijwegen, Pays-Bas, Europe Association).

United States Nuclear Regulatory Commission, 1975: *Reactor Safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. Wash 1400 (NUREG-75/014)* (Washington, DC). Publié également en français (1975) sous le titre: *Projet Rasmussen. Etude de la sûreté des réacteurs*, ministère de l'Industrie et de la Recherche (Paris, La Documentation française).

Villemeur, A., 1988: *Sûreté de fonctionnement des systèmes industriels. Fiabilité. Facteurs humains. Informatisation* (Paris, Editions Eyrolles).

Wehner, T., 1992: *Sicherheit als Fehlerfreundlichkeit* (Opladen, Westdeutscher Verlag).

Yoshinobu, S., 1985: *Safety Assessment of Automated Production Systems using Microelectronics. The Comprehensive Logic Models for the Analysis of Accidents Caused by Robots*. (Research reports of the Research Institute of Industrial Safety, March 1985 (21–31), en japonais, avec un résumé et des illustrations en anglais) (Tokyo, Research Institute of Industrial Safety).