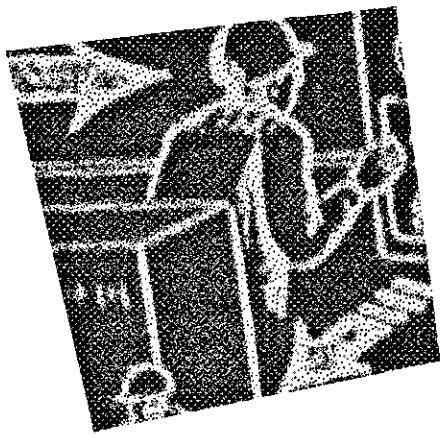
Règles sommaires de sécurité pour l'utilisation des automates programmables industriels (API)

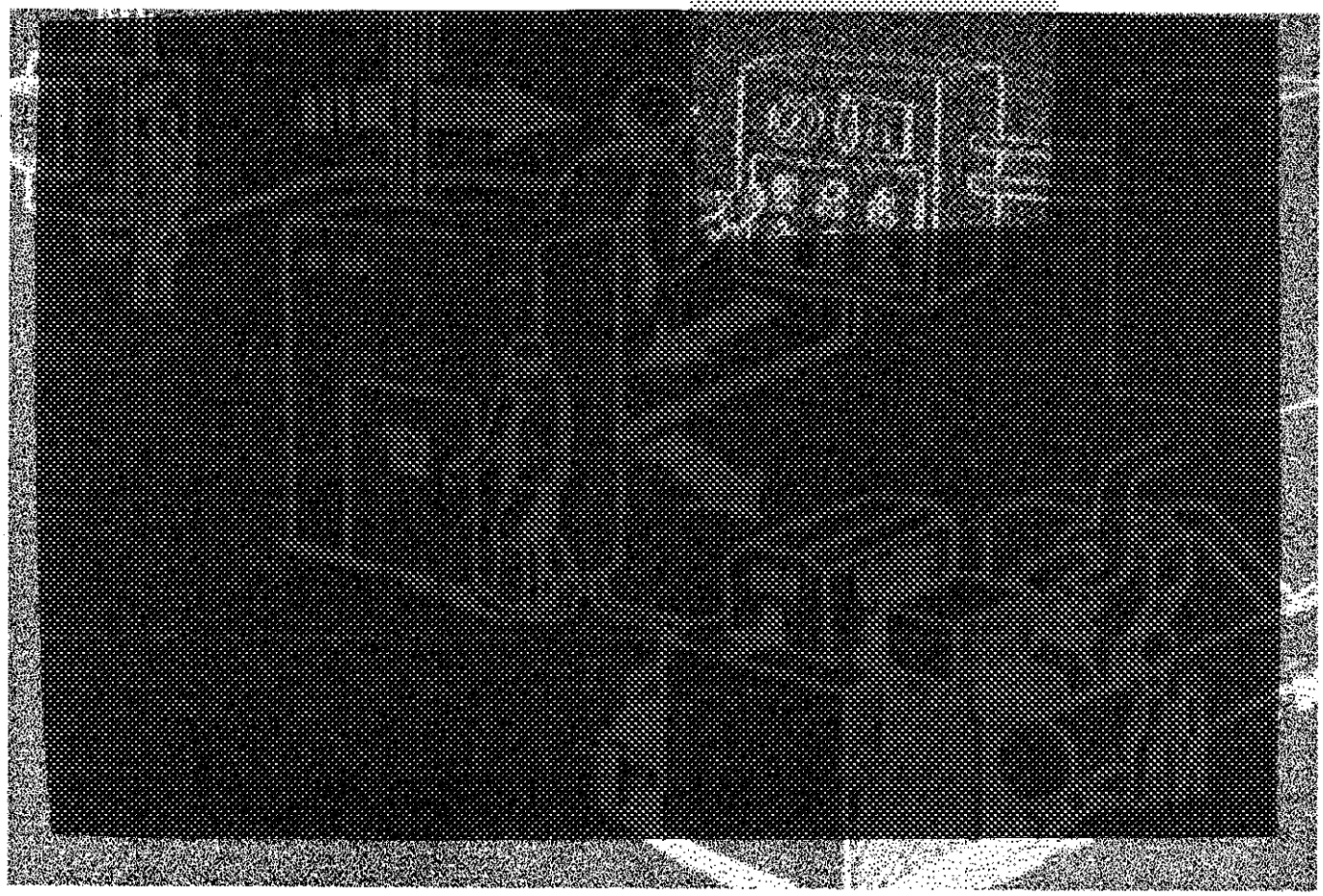


BILANS DE CONNAISSANCES

Joseph-Jean Paques

Janvier 1991 B-028

RAPPORT



IRSST
Institut de recherche en santé et en sécurité du travail du Québec

La recherche, pour mieux comprendre

L'Institut de recherche en santé et en sécurité du travail du Québec (IRSST) est un organisme de recherche scientifique voué à l'identification et à l'élimination à la source des dangers professionnels, et à la réadaptation des travailleurs qui en sont victimes. Financé par la CSST, l'Institut réalise et finance, par subvention ou contrats, des recherches qui visent à réduire les coûts humains et financiers occasionnés par les accidents de travail et les maladies professionnelles.

Pour tout connaître de l'actualité de la recherche menée ou financée par l'IRSST, abonnez-vous gratuitement au magazine *Prévention au travail,* publié conjointement par la CSST et l'Institut.

Les résultats des travaux de l'Institut sont présentés dans une série de publications, disponibles sur demande à la Direction des communications.

Il est possible de se procurer le catalogue des publications de l'Institut et de s'abonner à *Prévention au travail* en écrivant à l'adresse au bas de cette page.

ATTENTION

Cette version numérique vous est offerte à titre d'information seulement. Bien que tout ait été mis en œuvre pour préserver la qualité des documents lors du transfert numérique, il se peut que certains caractères aient été omis, altérés ou effacés. Les données contenues dans les tableaux et graphiques doivent être vérifiées à l'aide de la version papier avant utilisation.

Dépôt légal
Bibliothèque nationale du Québec

IRSST - Direction des communications
505, boul. de Maisonneuve Ouest
Montréal (Québec)
H3A 3C2
Téléphone : (514) 288-l 551
Télécopieur: (514) 288-7636
Site intemet : www.irsst.qc.ca

Règles sommaires de sécurité pour l'utilisation des automates programmables industriels (API)

Joseph-Jean Paques

Programme sécurité-ingénierie
Direction des laboratoires
IRSST

Cette étude a été financée par l'IRSST. Les conclusions et recommandations sont celles de l'auteur.

1er trimestre 1991.

TABLE DES MATIÈRES

PAGE

RÉSUMÉ 1

1.0 L'AUTOMATISATION : LA MEILLEURE OU LA PIRE DES CHOSES? 2

2.0 DÉTAIL DES RISQUES ASSOCIÉS AUX API 2

2.1 Fiabilité des API 2
2.2 Identification des risques du système machine et API 2
2.3 Risques spécifiques des API 3

2.3.1 Influence de l'environnement 3
2.3.2 Modes de défaillance aléatoires 4
2.3.3 Facilité de la modification des programmes 4

3.0 MOYENS DE PRÉVENTION 5

3.1 Conditions d'application 5
3.2 Cadre légal québécois et normes 5
3.3 Mesures minimum à appliquer 6

3.3.1 Utilisation d'un relais de sécurité 6
3.3.2 Fonction de chien de garde externe 7
3.3.3 Cablage des fonctions de sécurité 7
3.3.4 Surveillance des défauts internes 7
3.3.5 Cablage sécuritaire 8
3.3.6 Conditions environnementales 8
3.3.7 Procédures d'arrêt d'urgence 8
3.3.8 Conditions initiales sécuritaires 8

TABLE DES MATIÈRES

PAGE

3.4 Mesures fortement recommandées 9

3.4.1 Surveillance des défauts internes et affichage 9
3.4.2 Surveillance des défauts de sorties 9
3.4.3 Surveillance des alimentations auxiliaires 9
3.4.4 Contrôle strict des programmes 10
3.4.5 Tenue à jour de la documentation 10
3.4.6 Développement modulaire des programmes 10
3.4.7 Commandes impulsionnelles 11

3.5 Autres Mesures de prévention possibles dans d'autres conditions . . . 11

3.5.1 Duplication 11
3.5.2 Triplication 11

4.0 CONCLUSION 12

5.0 RÉFÉRENCES BIBLIOGRAPHIQUES 13

RÉSUMÉ

Avec l'automatisation de plus en plus poussée au Québec, le nombre d'automates programmables industriels (API) qui commandent les machines de production augmente aussi.

Comme pour toute nouvelle technologie, les conditions de travail des utilisateurs de machines sont modifiées et des mesures particulières de sécurité doivent être prises pour éviter les nouveaux risques succeptibles d'être introduits par ces nouvelles technologies d'automatisation.

Ce rapport, à l'usage des concepteurs de sytèmes de commande programmés, présente de façon structurée les principales techniques qui doivent être appliquées dans l'utilisation des automates programmables industriels pour améliorer la sécurité d'opération des machines qu'ils commandent. Ce rapport met aussi en évidence les limites actuelles de la sécurité que l'on peut attendre d'un automate programmable industriel.

En particulier, dans l'état actuel de la technique courante, la sécurité directe des travailleurs qui oeuvrent à proximité de certaines machines dangereuses commandées par API, doit être assurée par des moyens plus conventionnels et éprouvés que les automates programmables industriels (API).

1.0 L'AUTOMATISATION: LA MEILLEURE OU LA PIRE DES CHOSES?

Les automates programmables industriels (ou API) sont directement associés avec l'automatisation des procédés ou machines de production.

A ce titre, il est parfois facile de porter un jugement rapide sur les problèmes de sécurité en considérant que l'automatisation des machines, parce qu'elle éloigne les travailleurs des zones dangereuses, va résoudre tous les problèmes de sécurité au travail.

A l'inverse, on peut aussi prendre une attitude de suspicion vis à vis des API car il y a eu bien des expériences malheureuses à l'occasion de l'introduction d'API sur des machines ou en remplacement de machines existantes; en particulier, dans certains cas, on a pu observer des incidents et des pannes directement associées à ces nouvelles technologies utilisées de façon inappropriée.

La réalité se situe entre ces deux extrêmes et le concepteur d'un système commandé par API devra prendre une attitude lucide et objective; il devra connaître le type des risques associés à cette technologie et choisir les moyens de préventions appropriés en fonction des risques pour les travailleurs et la machinerie.

2.0 DÉTAIL DES RISQUES ASSOCIÉS AUX API

2.1 Fiabilité des API

Le premier élément du problème est la fiabilité propre des API. On rappelle que "La fiabilité caractérise un système suivant sa capacité à fonctionner sans panne et sans erreur". En général, les experts et les recherches faites à ce sujet s'entendent pour dire que globalement les systèmes de commande utilisant des API sont aussi fiables que les systèmes de commande à relais. Il est même des cas où la fiabilité des systèmes utilisant des API est supérieure à celle utilisant des relais.

Certaines études ont même montré que les éléments les plus susceptibles de faire défaut, dans ces systèmes API, sont les éléments utilisés comme interface (modules d'entrée/sortie ou liens de communication).

2.2 Identification des risques du système machine et API

La première démarche à effectuer, vis à vis de la sécurité d'une machine commandée par API, est d'identifier, de façon précise et détaillée, les composantes de la machine qui présentent un danger potentiel pour le travailleur qui opère cette machine.

Cette démarche s'appelle l'analyse des risques et doit porter sur toutes les sortes d'interventions que le travailleur est susceptible de faire sur la machine:

- chargement ou déchargement de matériaux ou de pièces;
- changement ou réglage d'outil;
- ajustement en cours de production;
- production normale;
- déblocage des matériaux;
- entretien en cours de production;
- entretien à l'arrêt;
- réparation;
- etc.

A la suite de cette démarche, chaque composant dangereux pour l'opérateur, aura été identifié.

Au cours de cette démarche, un moyen de protection adapté à chacun des risques identifiés sera prévu. Ce moyen sera souvent obtenu par un verrouillage de marche du composant potentiellement dangereux avec un détecteur de condition dangereuse. Par exemple, un détecteur de fermeture de capot de protection empêchera la mise en marche d'un moteur tant que le capot de protection n'est pas entièrement fermé.

Dans cette démarche, il faudra évaluer aussi la conséquence de commandes erronées, issues de l'API, sur la sécurité du travailleur.

2.3 Risques spécifiques des API

Sans entrer dans le détail complet des risques spécifiques associés aux API, le concepteur de système commandé par API doit être conscient de trois aspects originaux des API:

2.3.1 Influence de l'environnement

De façon plus marquée que les relais électromagnétiques, les API sont plus susceptibles de faire défaut si on ne prend pas garde aux conditions d'installation. Comme les API sont constitués principalement d'éléments électroniques, les conditions de température de bon fonctionnement sont limitées, souvent entre 0°C et 40°C. Ces éléments électroniques peuvent aussi être affectés par les poussières, l'humidité, les vibrations comme tout équipement électronique.

De plus, les API sont sensibles à un environnement électromagnétique ou électrostatique agressif. Du fait que les niveaux énergétiques des signaux qui actionnent l'API sont faibles, ils peuvent dans certains cas être perturbés par des inductions de parasites causés par un environnement électrique industriel. Par exemple, il est bien connu que des commandes à thyristor de gros moteurs peuvent générer des parasites sous forme de rayonnement électromagnétique de "pics" de fort niveau énergétique.

2.3.2 Mode de défaillance aléatoire

Alors que pour des composants de type électromécanique, on peut prévoir un mode de défaut relativement connu à l'avance, il est très difficile de prévoir le mode de défaut a priori d'un composant électronique.

Par exemple, on sait que le bris d'un ressort entraîne en général le non retour de l'armature d'un relais à sa position de repos; mais on ne peut pas dire a priori si un thyristor fait défaut en court circuit ou en circuit ouvert.

De façon générale, on a pu observer également que l'effet des parasites électromagnétiques ou électrostatiques est également imprévisible; par exemple, le contenu d'une mémoire volatile (RAM) peut aussi bien passer de l'état 0 à l'état 1 que l'inverse, sous l'effet d'une induction parasite.

Tout ceci implique que l'on doit considérer, par exemple, la possibilité aussi bien qu'un moteur ne démarre pas alors qu'il le devrait ou au contraire reste en marche alors qu'il devrait s'arrêter.

Par exemple aussi, le mouvement d'un cylindre à air, commandé par API peut ne pas correspondre à la commande effectuée par l'API.

En résumé, il faut considérer que les entrées et les sorties peuvent faire défaut en circuit ouvert ou en court circuit. On doit considérer aussi la possibilité d'un arrêt de résolution de la logique, c'est à dire que le déroulement du programme est arrêté ou bloqué dans une boucle.

Enfin, pour des API comportant des modules de communication à distance, il faut considérer que ces modules peuvent faire défaut, en général par interruption du lien de communication, car ces modules sont souvent munis de dispositifs de surveillance assez élaborés.

2.3.3 Facilité de modification des programmes

Un des avantages majeurs des API peut mettre en cause la sécurité d'une machine, si on ne prend pas un minimum de précautions.

Il est très facile de modifier un programme qui fait fonctionner un API; il est même souvent tentant de faire ces modifications "sur le tas", sans établir de documentation et sans tester toutes les conditions d'opération de la machine, incluant les cas un peu spéciaux de mode de fonctionnement rarement utilisés.

Il s'ensuit qu'on peut se retrouver avec un programme dont des sections sont inconnues (pas de documentation) et partiellement vérifiées (pas de test complet). Parfois même, si plusieurs versions du programme ont été produites, on ne sait plus laquelle est opérationnelle ni laquelle est effectivement chargée dans l'API.

3.0 MOYENS DE PRÉVENTION

3.1 Conditions d'application

Les mesures recommandées dans ce rapport auront leur pleine efficacité si et seulement si les trois conditions suivantes sont remplies:

- **L'analyse des risques de la machine** a été faite, de sorte que les éléments dangereux ont été identifiés de même que les sorties de l'API qui les actionnent.

- **Les éléments de sécurité requis**, tels que interrupteurs de position, manostats, détecteurs de présence, contacts auxiliaires, etc. ont été **définis et associés à des risques précis.**

- La machine est commandée par **un seul automate programmable** industriel (API). Des cas plus complexes sont abordés au chapitre 3.4.

3.2 Cadre légal québécois et normes

Au Québec, la référence légale qui sert de base à la plupart des analyses de sécurité de machine est le Règlement du Québec sur les établissement industriels et commerciaux, principalement au paragraphe 6.3.3 qui dit: "Les dispositifs ou interrupteurs de commande des machines et appareils doivent être conçus, installés et entretenus de façon à éviter la mise en marche accidentelle". Il faut remarquer qu'il n'y est fait référence à aucune technologie en particulier, programmable ou non.

La norme canadienne sur les fonctions de sécurité utilisant des techniques électroniques (CSA C22.2 No 0.8) donne quelques indications supplémentaires mais n'est également ni très détaillée ni très spécifique. Cette norme n'a pas de caractère obligatoire pour aucun équipement, à notre connaissance, au Québec.

A notre connaissance la seule norme à teneur légale au Canada qui va faire référence, lors de sa prochaine révision, aux automatismes programmables est la norme CAN/CSA-Z142, sur les presses mécaniques. Dans la version de travail

produite en avril 1990, qui fait d'ailleurs référence à la norme CSA C22.2 No. 0.8, des directives précises sont données sur les mesures de sécurité à prendre vis à vis de dispositifs de commande programmable qui seraient utilisées sur une presse mécanique. Ces directives sont en concordance avec les recommandations préconisées dans ce rapport. Si la législation québécoise est amendée plus tard pour prendre cette nouvelle version en préparation de la norme Z142 comme référence, ses recommandations devront donc s'appliquer.

Aux Etats-Unis, les normes de certains types de machines donnent des critères de performance de sécurité à rencontrer par les commandes de ces machines. En particulier, les normes en production ou en révision, attachées aux nouvelles technologies de production, indiquent des critères de performance qui doivent être rencontrés par les dispositifs de commande et de sécurité pour les robots, les véhicules filo-guidés, les entrepôts automatisés, les cellules de fabrication flexible etc.

Enfin c'est en Europe, au niveau national ou internationnal que l'on peut retrouver le plus grand nombre de normes et directives sur les mesures de sécurité à prendre lorsque des automates programmbles sont appelés à commander des machines potentiellement dangereuses.

3.3 Mesures minimum à appliquer

Voici les éléments minimum qu'il faut prévoir pour un système de commande à API.

3.3.1 Utilisation d'un relais de sécurité

Un relais de sécurité ("Master safety relay") sera prévu dont, la désalimentation aura pour effet de couper l'alimentation de puissance sur les modules de sortie qui actionnent tous les ensembles ou sous ensembles de la machine.

Ce relais sera du type à auto maintien de façon à se désamorcer en cas de coupure d'alimentation électrique.

Éventuellement ce relais pourra être sans effet sur les entrées de l'API et sur les sorties qui actionnent seulement des dispositifs de signalisation ou d'alarme afin que le système ne devienne pas aveugle en cas de condition d'arrêt par relais de sécurité.

L'amorçage du relais, à la mise en service de la machine, se fait par un bouton poussoir seulement. Le désamorçage du relais se fait à partir de différents signaux, issus d'autres dispositifs, décrit ci-après.

3.3.2 Fonction de chien de garde externe

Afin de s'assurer que le programme se déroule normalement, on doit insérer, dans le tronc du programme, une fonction qui actionne une sortie à chaque balayage du programme. Cette sortie sera raccordée à une minuterie, extérieure à l'API, qui se trouvera ainsi réarmée régulièrement.

L'ajustement de cette minuterie sera tel que si elle n'est pas réarmée après le temps moyen correspondant à deux ou trois balayages de programme, un jeu de contacts s'ouvre et désamorce le relais de sécurité.

De cette façon, on s'assure que le programme ne se trouve pas bloqué, soit à cause de changement causé par un parasite ou une mauvaise transcription magnétique, soit à cause de bouclage de séquence, non détectée lors des essais.

Dans certain cas de procédé très rapide, l'utilisation d'un chien de garde à tous les cyles peut poser des problèmes de temps de réponse.

3.3.3 Cablage des fonctions de sécurité

Parmi les dispositifs de sécurité qui ont été définis initialement par analyse, certaines fonctions, comme le bouton d'arrêt d'urgence, ont une action globale sur toute la machine. Ces dispositifs seront donc **DIRECTEMENT** cablées au relais de sécurité, de façon à le désamorcer lorsqu'ils seront actionnés. Ce mode de cablage est appelé "logique cablée".

D'autres dispositifs de sécurité (manostats, interrupteurs de position, etc) ne sont associés qu'à certains actionneurs ou moteurs; ils seront cablés **DIRECTEMENT** sur le circuit de commande de l'actionneur, à la sortie de l'API. Si un dispositif est raccordé aussi à un module d'entrées de l'API, cela ne pourra être fait qu'en utilisant d'autres jeux de contacts que ceux déjà raccordés aux actionneurs pour action directe.

3.3.4 Surveillance des défauts internes

Souvent les manufacturiers prévoient un certain nombre de dispositifs de surveillance du bon fonctionnement des parties internes de l'API (modules d'entrées-sortie non-compris).

Ces dispositions internes peuvent être du type vérification de parité ("parity check"), dépassement de registre ("overflow"), division par zéro, valideur ("check sum") ou même parfois chien de garde interne ("watch dog") ou autre.

La sortie, prévue par le fabricant, doit être raccordée au relais de sécurité, de façon à le désamorcer en cas de défaut interne.

3.3.5 Câblage sécuritaire

Pour les éléments raccordés à l'entrée ou à la sortie de l'API et qui ont un impact direct sur la sécurité, il faut respecter les règles de l'art pour le type de câblage à utiliser.

En particulier, il faut choisir le mode de défaut sécuritaire (défaut ouvert ou défaut fermé) de façon à ce que par exemple la coupure d'un câble, le démontage intempestif d'un détecteur de position, l'ouverture d'un fusible, amène la machine à un état sécuritaire.

Dans la plupart des cas, la perte de tension électrique correspond à une condition sécuritaire, mais l'usage de freinage à contre courant par exemple peut être nécessaire.

3.3.6 Conditions environnementales

Bien que les API fabriqués aujourd'hui présentent une meilleure résistance aux éléments extérieurs physiques ou électriques, il convient toujours de s'assurer que les conditions d'installation sont acceptables et correspondent aux recommandations des fabricants.

3.3.7 Procédures d'arrêt d'urgence

Toute machine, présentant un minimum de risques pour les travailleurs, doit disposer d'un dispositif d'arrêt d'urgence, facilement accessible, bien identifié et à action complète sur tous les éléments de la machine.

Au delà de l'action immédiate de l'arrêt d'urgence, il faut évaluer aussi l'impact de l'actionnement de l'arrêt d'urgence sur le déroulement du programme et par contre coup sur le comportement général de la machine.

En particulier, un arrêt brutal peut entraîner des pertes de matériaux, des bris mécaniques ou même des conditions potentiellement dangereuses pour les travailleurs (exemple d'un four de coulée de métal en cours de vidage).

3.3.8 Conditions initiales sécuritaires

Du fait de la volatilité potentielle des informations contenues dans l'API, il est souhaitable de prévoir un module du programme qui force l'état des sorties de façon connue et sécuritaire, avant que le programme de commande ne commence à se dérouler. Ce module sera utilisé chaque fois que l'API sera réinitié et que le déroulement du programme sera lancé, après un arrêt de l'API à des fins d'entretien, par exemple.

Éventuellement un module analogue pourra être prévu après l'arrêt de la machine et avant sa mise en marche.

3.4 Mesures fortement recommandées

Afin d'améliorer le fonctionnement d'une machine commandée par API, de réduire les risques d'accident et aussi d'améliorer sa maintenabilité (facilité de réparations), il est fortement recommandé de compléter les mesures de protection minimum, par les moyens suivants.

3.4.1 Surveillance de défauts internes et affichage

Certains fabricants de API fournissent des dispositifs de surveillance des défauts internes et par un affichage approprié qui améliore la facilité de diagnostique donc de réparation de l'API.

3.4.2 Surveillance des défauts des sorties

A l'aide de câblage supplémentaire et en utilisant d'autres entreés, il est possible de s'assurer que les sorties critiques réagissent de façon appropriée aux commandes effectuées.

On peut alors actionner soit des alarmes soit le relais de sécurité si des sorties critiques vis à vis de la sécurité sont par exemple en défaut en court circuit. Il existe même certaines techniques sophistiquées de surveillance dynamique des sorties.

3.4.3 Surveillance des alimentations auxiliaires

De façon générale, il faut évaluer les conséquences de coupure d'alimentation électrique en général ou parfois de défaut du type surtension s'il s'agit d'alimentation régulée.

Si des dispositifs de protection contre les surtensions du type "crowbar" sont utilisés sur les tensions régulées, leur déclenchement entraine une perte d'alimentation électrique par rupture de fusible.

Comme dans certains cas les circuits d'entrée ou de sortie, en tout ou en partie, sont polarisés à partir de source électrique différente de celle de l'API, il est recommandé de surveiller ces sources et de définir de façon précise les conséquences de leur perte pour la machine.

3.4.4 Contrôle strict des programmes

Afin de limiter les risques de modifications intempestives des programmes, il est fortement recommandé de limiter par des dispositifs à clé, à cadenas ou même par plombage, l'accès aux moyens de chargement de programmes dans les API.

Il faut considérer que des panneaux électriques ou des interrupteurs à clé, dont la clé sert sur plusieurs machines dans une usine ou est mise à la portée de tous, ne constitue pas une protection valable.

Par exemple dans certaines grosses usines, on a été amené à "plomber" l'accès aux sélecteurs de mode de fonctionnement des API, sur la position de marche normale ("RUN").

En général aussi, les consoles de programmation disposent d'un interrupteur à clé de mise en marche. En autant que la console est unique et que sa clé est unique aussi et est attribuée nominalement à une personne qualifiée et responsable pour effectuer les changements, cette procédure constitue une certaine forme de contrôle.

3.4.5 Tenue à jour de la documentation

Plus encore que pour les systèmes à relais, il est impératif de conserver, sous une forme facile à accéder et simple à comprendre, une image du programme qui fonctionne dans l'API. Il faut aussi effectuer des copies de relève de la ou des disquettes qui contiennent les programmes, entreposées dans un lieu différent.

Après chaque modification implantée et fonctionnelle, on aura donc soin de remettre à jour la liste imprimée du programme pour le dossier d'entretien, la disquette qui contient le programme implanté et la ou les copies de relève des disquettes.

Les modifications devraient faire l'objet d'une description écrite afin de pouvoir retracer l'évolution du programme depuis sa première implantation sur l'API, au moment de la mise en service de la machine.

3.4.6 Développement modulaire des programmes

Pour simplifier le développement et réduire les coûts d'entretien du programme, il est recommandé de suivre les règles de l'art en matière de programmation informatique.

En particulier une approche modulaire et intégrée des programmes conduira à fractionner le déroulement du programme en modules de commode des différents éléments de la machine.

Il existe de nombreuses régles de développement de logiciel informatique qui peuvent être avantageusement appliquées au développement de logiciel de commande de machine ou de procédé.

3.4.7 Commandes impulsionnelles

Une philosophie de commande, qui facilite l'élaboration des programmes de commande pour le déroulement normal des séquences de la machine et aussi dans les conditions d'urgence, consiste à utiliser des boutons poussoirs pour envoyer des commandes à l'API.

Cette technique de commande impulsionnelle est préférée à la technique des contacts maintenus. Cela n'empêche pas d'effectuer des sélections de mode de fonctionnement à l'aide de commutateurs à contacts maintenus, si cela est jugé nécessaire.

3.5 Autres mesures de prévention possibles dans d'autres conditions

3.5.1 Duplication

Lorsque les fonctions de sécurité sont trop complexes pour être réalisées en logique cablée, on est parfois conduit à utiliser deux ensembles de commande en parallèle, dont les éléments sont dupliqués totalement ou partiellement.

Pour conserver les critères de sécurité, parfois le câblage des éléments de sécurité doublés peut être tel que si l'un d'entre eux fait défaut, la machine est amenée dans un état sécuritaire.

On conçoit que si une telle disposition améliore la sécurité de la machine (capacité de fonctionner sans accident), elle réduit toutefois sa fiabilité (capacité de fonctionner sans panne et sans erreur).

3.5.2 Triplication

Dans certains cas, l'arrêt d'une machine ou d'un ensemble de machine, lorsque seulement un composant fait défaut, peut avoir des conséquences innacceptables financièrement (par exemple: arrêt de contrôle nucléaire). On peut alors faire appel à la technique de triplication des chaînes.

Cette technique consiste à installer trois chaînes de commande, incluant les capteurs et les actionneurs en triple, et à agencer les commandes de façon à ne pas déclencher d'arrêt de sécurité si seulement une chaîne de commande donne l'ordre d'arrêter. On considère alors que si une seule chaîne donne l'ordre d'arrêter et non les autres, c'est que cette chaine présente un ou plusieurs éléments en défaut.

Le déclenchement d'arrêt de sécurité est dit avec "vote 2 dans 3", c'est dire que l'arrêt de sécurité est déclenché si au moins deux des trois canaux en donnent l'ordre.

Naturellement chaque chaine de commande dispose de dispositifs de surveillance appropriés qui permettent d'identifier le défaut et d'aider la réparation d'une chaîne en défaut le plus tôt possible après que le défaut ait été détecté.

Comme cette technique de triplicationelle est très coûteuse, elle est réservée lorsque les conséquences économiques, écologiques ou de sécurité le justifient. Elle est utilisée par exemple dans l'industrie nucléaire, pétrochimique, aérospatiale ou militaire.

4.0 CONCLUSION

En utilisant les techniques décritent dans ce rapport, il est possible d'améliorer la sécurité et la fiabilité de commande de machine par automate programmable.

Leur application entrainera une meilleure sécurité de fonctionnement, une surveillance accrue des défauts et un entretien plus facile.

Toutefois, la protection directe des travailleurs, vis à vis des risques d'accidents rencontrés autours des machines, ne peut pas dépendre uniquement de la fiabilité d'un seul automate programmable.

La redondance des dispositifs de sécurité doit assurer que leur bon fonctionnement n'est pas entravé en cas de défaut et que, de plus, tout défaut unique doit être signalé et ne peut permettre ultérieurement le fonctionnement de la machine sans protection.

Habituellement, une redondance active des dispositifs de sécurité en logique cablée permet d'assurer un niveau de sécurité satisfaisant.

Si aucun document légal à l'heure actuel au Québec n'impose de contrainte spécifique pour des machines commandées par automate programmable industriel, il faut s'attendre à ce que certaines normes soit remises à jour pour tenir compte de ces nouvelles technologies. Il est possible de trouver dans d'autres pays, principalement en Europe, des normes et directives très précises dans ce domaine.

5.0 RÉFÉRENCES BIBLIOGRAPHIQUES

1. B.K. DANIELS. Safety and Reliability of Programmable Electronic Systems. National Centre of Systems Reliability, U.K. 1986

2. Programmable Electronic Systems in Safety Related Applications, Introductory guide and general technical guidelines. Health and safety executive, U.K. 1987

3. H. HÖLSCHER, J. RODER. Les microprocesseurs dans les techniques de sécurité, traduction de l'Institut national de recherche et de sécurité. Avril 1986

4. Technical committee N° 65: Industrial process measurement and control, Subcommitee 65A: System considerations on Programmable Controllers, Report of Working group 9 : Safe software. International Electrotechnical commission. August 1989.

5. Technical committee N° 65: Industrial process measurement and control, Subcommitee 65A: System considerations. Draft - Fonctional safety of programmable electronic systems: Generic aspects (Working Group 10). International Electrotechnical commission. October 1989.

6. D.DEI-SVALDI, J.P. VAUTRIN. Les automates programmables, nouvelles technologies, nouveaux risques, principes de sécurité à appliquer. Institut national de recherche et de sécurité. 1984

7. D. DEI-SVALDI, J.P. VAUTRIN. Automates programmables, comportement en ambiance industrielle. Electronique industrielle, février 1984

8. D.DEI-SVALDI. Les automates programmables: vers un meilleur comportement en ambiance industrielle. Institut de recherche et de sécurité. Juin 1986

9. J.P. GÉRARDIN. Aide à la conception de systèmes fiables et sûrs: l'appareil DEFI. Electronique industrielle. Novembre 1986

10. KEVIN L. WADE. Method of improving programmable controller failure mode predictability. 14th Annual international programmable controllers conference, Engineering Society of Detroit. April 1985

11. W.O. MINISH. Safety and security considerations in the application of programmable controllers. Institute of Electrical and Electonical Engineers, PCIC-84-7. 1985

12. P. ITICSOHN. Sécurité et automates programmables. Revue de la sécurité. Octobre 1987

13. C. ADAMS. I/O Systems, Recent advances. Europe first Conference on Programmable Controllers, 1985.

14. W.A. NEAL. Keeping tabs via programmable control. Mechanical Engineering. July 1986

15. D.DEI-SVALDI, M. COLLIER, J.P. VAUTRIN. Machine commandée par automate programmable: amélioration de la sécurité. Le Nouvel Automatisme. Mai 1983

16. L'électronique mise à mal par son ancêtre l'électrostatique. Mesures. Avril 1987

17. YEFIM S. GUDESBLAT. Software validation in pharmatical manufacture. Programmable controls. Mai/Juin 1988

18. La redondance, clé de la sûreté. Industries et techniques, cahier spécial. Février 1988

19. P. KASGYCKI, R. TOMASETTA. Industrial workstations: protecting your PC on the plant floor. INTECH. Juillet 1988

20. J.J. PAQUES. Introduction à la sécurité des automates programmables. Au fil du bois. Avril - mai 1987

21. J.J. PAQUES. Automates programmables et sécurité. CSST 87. Mai 1987

22. J.J. PAQUES. Panel discussion about safety & programmable controls.DIGICOM 87, Section montréalaise de l'Instrument Sciety of America, Montréal, Octobre 1987

23. J.J. PAQUES. Panel discussion about safety & programmable controls. 3rd Annual canadian programmable control conference & exhibition. I.E.E.E. Hamilton. November 1987

24. Manual on the design of automated industrial systems. International Section "Machine Safety" of the International Social Safety Association. Mannheim 1988.

25. Rules for realization and safety control equipment in the automated systems. International Section "Machine Safety" of the International Social Safety Association. Mannheim 1988.

26. Safety Functions Incorporating Electronic Technology, Requirements for safety of Electrical Products. Canadian Standards Association. CSA C22.2 No. 0.8-1986. 1986.

27. Draft American National Standard - Performance Criteria for the Design, Construction, Care and Operation of Safeguarding when referenced by other B11 machine tool standards. ANSI B11.19 Draft. Rev. 1989.

28. Code for Punch Press and Brake Press Operation: Health, Safety and Guarding Requirements. Canadian Standards Association. CAN/CSA-Z142. Draft april 1990.

29. Industrial Control Devices, Controllers and Assemblies. ANSI/NEMA ICS2 1983.

30. J.-J. Paques. Basic safety rules for using programmable controllers, ISA 89. International conference and Exhibit, Instrument Society of America, Philadelphie. 1989.

31. J.-P. Morel, J.-L. Poyard. Les fonctions de sécurité dans la conception et la réalisation de l'automatisme des machines et appareils. Journal technique de l'APAVE no 237. Paris 1987.

32. Guide d'Etude des Modes de Marche et d'Arrêt. Association for promoting automatic production (ADEPA). Paris Second edition.

33. W. B. Askren, J. M. Howard. Software safety for programmable industrial machines. International Ergonomics ans Safety Conference '89. Cincinnati, Ohio, June 1989.

34. Guide pour la conception des dispositifs de verrouillage et d'interverrouillage associés à des protecteurs. Institut National de Recherche en Sécurité. ND 1473-112-83. Paris 1983.

35. Draft American National Standard for Industrial Robots and Robot Systems - Safety Requirements. BSR/RIA R15.06-19XX. Rev. 1989.

36. Draft American National Standard - Safety Requirements for Manufacturing Systems/Cell. B11.20-19XX (Draft). Rev. 1989.

37. American National Standard - Safety Standard for Guided Industrial Vehicles. ASME/ANSI B56.5-1988. 1988.

38. Programmable Electronic Systems for Use in Safety Applications. Instrument Society of America, Sub-committee SP84, Draft 1990.