→ D. Pagliero, M. Kneppert,
D. Dei-Svaldi, Département
Ingénierie des équipements de travail,
Centre de Lorraine, INRS ,
54230 Neuves-Maisons,
avec la collaboration de
MM. Losson, Sté Siemens,
93200 Saint-Denis,
Palmier, Sté Renault Automation,
81100 Castres,
et Guillemant, Sté PCI-SCEMM,
42000 Saint-Etienne

Analyse du niveau de sécurité d'une commande d'axe à sécurité intégrée

(cartes d'axe, commandes d'axes...)

ANALYSIS OF THE SAFETY LEVEL OF A SAFETY INTEGRATED MOTION CONTROLLER
(MOTION BOARD, MOTION CONTROL, ETC.)

The use of "safety integrated" motion controllers in an industrial setting, in particular on numerically-controlled machines and machining centres, allows among other things an improvement in operator safety, but does not however prevent all the risks and can sometimes cause new ones. It is for this reason that the recent use of these devices has led INRS to look into their ability to ensure the safety of people involved in conformity with the claims of the manufacturer, particularly as regards the safety levels they offer compared to conventional equipment. This article is a follow-up to the technical safety guide entitled "high-speed machining centres" published by INRS ([1]). It sets out the concept of "safety integrated" and examines the integration of this specific device within a control circuit.
Contents: problems encountered in high-speed machining, the Sinumerik® safety integrated motion controller of Siemens, schematic diagram, architecture of this motion controller, safety function management, concept of safety integrated, review of and discussion about this innovative concept, conclusion, box with a reminder of certain definitions and terminology.
([1]) See: ND 2138 [1].

• safety integrated • motion controller • control circuit • numerical control • machining center • machine • high speed

La mise en œuvre de commandes d'axe à « sécurité intégrée » en milieu industriel et en particulier sur des machines à commande numérique ou sur des centres d'usinage, permet entre autres d'améliorer la sécurité des opérateurs, mais ne supprime pas pour autant tous les risques et peut parfois en engendrer de nouveaux.
C'est pourquoi, l'exploitation récente de ces dispositifs a conduit l'INRS à s'interroger sur leur capacité à assurer la sécurité des intervenants, conformément aux revendications du constructeur, notamment sur le niveau de sécurité qu'ils offrent vis-à-vis des équipements conventionnels.
Ce document constitue une suite du guide technique de sécurité intitulé « centres d'usinage à grande vitesse (UGV) publié par l'INRS ([1]). Il précise le concept de « sécurité intégrée » et étudie l'intégration de ce dispositif particulier au sein d'un circuit de commande.
Au sommaire : Problématique posée par l'usinage grande vitesse, la commande d'axe Sinumerik® à sécurité intégrée de la société Siemens, schéma de principe, architecture de cette commande d'axe, gestion des fonctions de sécurité, concept de sécurité intégrée, réflexion et discussion sur ce concept novateur, conclusion, encadré pour rappeler certaines définitions et terminologies.

• sécurité intégrée • commande d'axe • circuit de commande • commande numérique • centre d'usinage • machine • grande vitesse

L'usinage à grande vitesse (UGV) se généralise dans les différents secteurs de l'industrie et plus particulièrement dans le domaine de la machine-outil à commande numérique. Avec ces nouveaux outils de production, les vitesses de rotation et de déplacement ont été multipliées par dix et parfois plus par rapport aux centres d'usinage conventionnels des années 1990.

Cette augmentation des performances n'est pas sans créer de nouveaux risques tels que ceux de collision ou encore d'éclatement d'un outil. Pour y remédier, certains constructeurs ont développé de nouvelles techniques de sécurité afin d'assurer la protection des opérateurs amenés à côtoyer de telles machines.

La conception des circuits de commande, les protections, les procédures d'intervention et les équipements périphériques ont du être repensés, modifiés ou adaptés à ces nouvelles cadences.

Plusieurs questions viennent immédiatement à l'esprit :
- Quel est le comportement de ces nouveaux dispositifs en présence d'un dysfonctionnement interne (matériel ou logiciel), notamment sur leurs performances d'arrêt ?
- Comment peut-on autoriser un opérateur à côtoyer ou à accéder en sécurité à la zone d'usinage ?

([1]) Voir : Guide technique de sécurité ND 2138 [1].

● Est-il possible de limiter ou d'interdire les manipulations erronées ?…

Au travers de ces questions, dans un contexte nouveau de production, l'INRS se propose aujourd'hui de faire un bilan sur le concept de sécurité baptisé « sécurité intégrée » (safety integrated) applicable aux circuits de commande de machine. Les risques mécaniques liés à l'usinage à grande vitesse ont déjà été abordés dans deux articles, publiés par l'INRS [1,2] (2).

Définitions et terminologie

Certains termes cités dans ce document demandent à être précisés pour la bonne compréhension du texte ; ils sont regroupés dans l'*encadré 1.*

(2) Avertissement : les auteurs utilisent volontairement le terme de « sécurité intégrée » (safety integrated) dans ce texte, afin de rester en cohérence avec l'appellation des concepteurs de machines-outils à commande numérique et ceux des centres d'usinage à grande vitesse. Cette notion est toutefois récente ; elle appartient à la firme Siemens, qui a été précurseur en la matière. Les lecteurs trouveront au sein de cet article quelques similitudes avec le matériel Sinumerik développé par Siemens, car il fait toujours à ce jour référence dans ce domaine, malgré l'annonce de la présence sur le marché international de plusieurs équivalences européennes et japonaises.

ENCADRÉ 1

DÉFINITIONS ET TERMINOLOGIE
- Definitions and terminology

Machine (NF EN 292-1 [7]
« Ensemble de pièces ou d'organes liés entre eux, dont au moins un est mobile et, le cas échéant, d'actionneurs, de circuits de commande et de puissance, etc., réunis de façon solidaire en vue d'une application définie, notamment pour la transformation, le traitement, le déplacement et le conditionnement d'un matériau.

Est également considéré comme « machine » un ensemble de machines qui, afin de concourir à un seul et même résultat, sont disposées et commandées de manière à être solidaires dans leur fonctionnement. »

Centres d'usinage - *Devant l'absence de définition normative, nous considérons que :*
Ce sont des machines-outils qui travaillent par enlèvement de matière et permettent de réaliser automatiquement des opérations d'usinage (fraisage, perçage, taraudage, etc.). Elles sont en général équipées d'un magasin d'outils avec chargeur automatique ; elles peuvent aussi être asservies d'un dispositif de chargement de pièces.

Risque (NF EN 292-1) [7]
Le risque généré par un process ou une machine dépend de deux facteurs principaux :
- la probabilité et la fréquence du risque,
- la possibilité d'éviter le phénomène dangereux.

Zone dangereuse (NF EN 292-1) [7]
Toute zone à l'intérieur et/ou autour d'une machine, dans laquelle une personne est exposée à un risque de lésion ou d'atteinte à sa santé.

Estimation du risque (NF EN 292-1) [7]
Estimation globale de la probabilité et de la gravité d'une lésion ou d'une atteinte à la santé pouvant survenir dans une situation dangereuse, en vue de sélectionner des mesures de sécurité appropriées.

Sécurité positive (NF EN 292-1) [7]
« Situation théorique qui serait réalisée si une fonction de sécurité restait assurée en cas de défaillance du système d'alimentation en énergie ou de tout composant contribuant à la réalisation de cette situation.

Dans la pratique, on se rapproche d'autant plus de la réalisation de cette situation que l'effet des défaillances sur la fonction de sécurité considérée est plus réduit. ».

Prévention intrinsèque (NF EN 292-1) [7]
« mesures de sécurité qui consistent à :
- éviter ou réduire autant de phénomènes dangereux dès que possible en choisissant convenablement certaines caractéristiques de conception et,
- limiter l'exposition des personnes aux phénomènes dangereux inévitables ou qui ne peuvent être suffisamment réduits ; ceci s'obtient en réduisant le besoin, pour l'opérateur, d'intervenir dans des zones dangereuses. »

Fonction de sécurité (EN 292-1) [7]
« Fonction d'une machine dont la défaillance peut accroître la probabilité de blessure ou d'atteinte à la santé. »

Fonctions de sécurité directe (NF EN 292-1) [7]
« fonctions d'une machine dont le dysfonctionnement augmenterait immédiatement le risque de lésion ou d'atteinte à la santé.

Il y a deux catégories de fonctions de sécurité directe :

a) Les fonctions de sécurité proprement dites, qui sont des fonctions de sécurité directe spécifiquement destinées à assurer la sécurité.

Exemples :
- fonction prévenant la mise en marche imprévue/intempestive (dispositif de verrouillage associé à un protecteur),
- fonction de non-répétition de cycle,
- fonction de commande bimanuelle,
- etc.

b) Les fonctions conditionnant la sécurité, qui sont des fonctions de sécurité directe autres que les fonctions de sécurité proprement dites.

Exemples :
- commande manuelle d'un mécanisme dangereux pendant des phases de réglage, les dispositifs de protection ayant été neutralisés,
- régulation de la vitesse ou de la température maintenant la machine dans des limites de fonctionnement sûres. »

Fonctions de sécurité indirecte (NF EN 292-1) [7]
« Fonctions dont la défaillance n'engendre pas immédiatement un risque, mais abaisse cependant le niveau de sécurité. En fait partie, notamment, l'autosurveillance des fonctions de sécurité directe (par exemple l'autosurveillance du bon fonctionnement d'un détecteur de position dans un dispositif de verrouillage). »

>>

ENCADRÉ 1 (suite)

DÉFINITIONS ET TERMINOLOGIE
- Definitions and terminology

Dispositif de verrouillage (NF EN 292-1) [7]
« Dispositif de protection mécanique, électrique ou d'une autre technologie, destiné à empêcher certains éléments de la machine de fonctionner dans certaines conditions, généralement tant qu'un protecteur n'est pas fermé. »

Autosurveillance (NF EN 292-1) [7]
« Fonction de sécurité indirecte grâce à laquelle une action de sécurité est déclenchée si l'aptitude d'un composant ou d'un constituant à assurer sa fonction diminue, ou si les conditions de fonctionnement sont modifiées de telle façon qu'il en résulte un risque.

Il existe deux catégories d'autosurveillance :

- autosurveillance « continue », par laquelle une mesure de sécurité est immédiatement déclenchée lorsque se produit une défaillance.
- autosurveillance « discontinue », par laquelle une mesure de sécurité est déclenchée pendant un cycle ultérieur du fonctionnement de la machine si une défaillance s'est produite. »

Installation complexe (NF EN 292-1) [7]
« Groupe de machines fonctionnant ensemble de façon coordonnée. »

Système automatisé (CEI 61131-1) [13]
« Système de commande dans lequel des configurations d'automate programmable sont incorporées par ou pour l'utilisateur, mais qui contient également d'autres éléments constitutifs y compris leurs programmes d'application. »

Système électronique programmable (CEI 61508-4) [5]
« Système de commande, de protection ou de surveillance basé sur un ou plusieurs dispositifs électroniques programmables. Ce terme recouvre tous les éléments du système, tels que l'alimentation, les capteurs, ou autres dispositifs d'entrée, jusqu'aux actionneurs, ou autres dispositifs de sortie, en passant par les autoroutes de données ou autres voies de communication. »

Système relatif à la sécurité (CEI 61508-4) [5]
« Un tel système est un système qui, à la fois :

- met en œuvre les fonctions de sécurité requises pour atteindre un état de sécurité de l'équipement commandé ou pour maintenir un tel état ;
- est prévu pour atteindre, par lui-même ou grâce à des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, ou des systèmes relatifs à la sécurité basés sur une autre technologie ou des dispositifs externes de réduction de risque, le niveau d'intégrité de sécurité nécessaire à la mise en oeuvre des fonctions de sécurité requises. »

Système de commande (CEI 61508-4) [5]
« Système qui réagit à des signaux d'entrée provenant du processus et/ou d'un opérateur et qui produit des signaux de sortie qui font que l'équipement commandé fonctionne de façon souhaitée. »

Automate programmable (CEI 61131-1) [13]
« Système électronique fonctionnant de manière numérique, destiné à être utilisé dans un environnement industriel, qui utilise une mémoire programmable pour le stockage interne des instructions orientées utilisateur aux fins de mise en œuvre de fonctions spécifiques, telles que des fonctions de logique, de mise en séquence, de temporisation, de comptage et de calcul arithmétique, pour commander au moyen d'entrées et de sorties TOR ou analogiques divers types de machines ou de process. L'automate programmable (AP) et ses périphériques associés sont conçus pour pouvoir facilement s'intégrer à un système d'automatisme industriel et être facilement utilisés dans toutes leurs fonctions prévues. »

Circuit de commande (NF EN 60204-1) [8]
« Circuit servant à commander le fonctionnement de la machine et à la protection des circuits de puissance. »

Logiciel (CEI 61508-4) [5]
« Création intellectuelle comprenant les programmes, les données, les procédures et règles, ainsi que toute documentation se référant au fonctionnement d'un système de traitement de données. »

Logiciel système (CEI 61131-1) [13]
« Logiciel, écrit par le constructeur du dispositif, qui définit le fonctionnement du dispositif avec ou sans programme d'application. Généralement, un ensemble de sous-programmes qui agit comme un interpréteur en convertissant les instructions du programme d'application entré par l'utilisateur en code machine requis par le matériel du dispositif. »

Logiciel applicatif - *Devant l'absence de définition normative, nous considérons que :*
Le logiciel applicatif pour automate programmable désigne tous les logiciels développés ou modifiés pour un besoin de l'utilisateur spécifique (application) et peut constituer un ou plusieurs programmes, données, configurations et documentation associée implémentée sur un ou plusieurs automates programmables.

Logiciel de sécurité (CEI 61508-4) [5]
« Logiciel utilisé pour exécuter des fonctions de sécurité dans un système relatif à la sécurité. »

Système de programmation (Z 61-000) [14]
« Ensemble comprenant un ou plusieurs langages de programmation ainsi que le logiciel nécessaire pour l'emploi de ces langages sur un matériel particulier de traitement automatique de l'information. »

Programme (CEI 61131-1) [13]
« Série d'actions proposées pour obtenir un certain résultat »

Programme d'application (CEI 61131-1) [13]
« Ensemble logique de tous les éléments et constructions de langage de programmation nécessaire pour le traitement des signaux destinés à commander une machine ou un processus au moyen d'une configuration d'automate programmable. »

(suite de l'article) >

1. Problématique posée par l'usinage à grande vitesse

Les besoins qui ont poussé les constructeurs à développer cette nouvelle approche de « sécurité intégrée » se résument comme suit :
- rapidité d'action (temps de réponse de l'ordre de quelques millisecondes),
- travail à porte ouverte à vitesse réduite,
- contrôle sûr des paramètres de sécurité (vitesse, position, arrêt de fonctionnement, etc.),
- préservation de l'outillage contre les chocs mécaniques.

En réduisant les temps et les distances d'arrêt, la commande à sécurité intégrée permet de répondre à ces besoins. En effet, l'électronique de commande réagit très rapidement en présence d'un dysfonctionnement de la machine. Le gain de temps par rapport au réflexe humain est dans un rapport de 100. Cela se traduit par des performances d'arrêt inégalables par les automatismes conventionnels commandés par un opérateur.

Quelles en sont les applications ?

La possibilité de détecter rapidement une anomalie de fonctionnement, conjuguée à un freinage à forte décélération autorise la présence d'un opérateur dans l'enceinte d'usinage, en respectant toutefois les limitations de vitesse et d'accélération préconisées et compatibles avec cette présence. Cela permet aujourd'hui de traiter tous les modes de marche en sécurité (mode dégradé, mode maintenance, mode réglage, etc.), ce qui n'était pas possible jusqu'à présent. De même, lorsque la machine est conçue pour assurer un usinage de précision, de l'ordre du $1/10^{e}$ de micron (µm), cette performance d'arrêt est nécessaire pour minimiser les effets d'un choc mécanique.

Quels sont les risques résiduels ?

Malgré la présence d'une commande à sécurité intégrée, certains risques subsistent :
- Projection de particules métalliques à haute énergie (éclatement de l'outil de coupe),
- Explosion lors du travail de certains métaux (magnésium),
- Exposition aux vapeurs d'huile.

Ces risques réclament des moyens de protection supplémentaires qui ne sont pas abordés dans cette note.

Quels sont les modes de marche où les risques peuvent persister ?

Remarque : On considèrera que la sécurité intégrée est opérationnelle dans tous les modes de marche et fait partie intégrante de la machine.

On distingue trois modes principaux de marche.

a) Mode d'exploitation (enceinte fermée)

Dans ce cas, il n'y a pas de risques dans la limite ou l'enceinte peut résister à l'éclatement d'un outil et ou son ouverture ne peut se faire que tout mouvement interrompu (interverrouillage).

b) Mode contrôle (enceinte ouverte sans mouvement)

Risque particulier lié à des problèmes de manutention.

c) Mode réglage (enceinte ouverte avec mouvements à vitesse réduite)

Dans ce mode de fonctionnement, la sécurité de l'intervenant ne peut être assurée au même niveau que les deux précédents.

Remarque : Une machine-outil à commande numérique ne renferme pas exclusivement des actionneurs électriques. D'autres sources d'énergie sont souvent mises en œuvre. Dans ce contexte, l'arrêt de la machine devient plus critique. En effet, il ne s'agit plus de couper uniquement la source électrique, mais aussi d'agir avec le même niveau de sécurité sur les autres sources d'énergie (pneumatique, hydraulique, etc.). C'est le cas par exemple des préhenseurs de pièce ou d'outil, où l'on doit maintenir le serrage, voir l'interverrouillage, pour éviter la chute ou l'éjection de ces éléments.

2. La commande d'axe à sécurité intégrée Sinumerik®

L'objectif de ce concept est de garantir, quel que soit le mode de marche de la machine (exploitation, contrôle, entretien), un arrêt sûr des mouvements de la machine lorsqu'une anomalie est décelée. Le but est de ne pas porter atteinte à l'intégrité physique des opérateurs mais également d'éviter les incidents mécaniques par collision ou choc entre les outils et la pièce.

En quoi cette nouvelle approche diffère-t-elle des anciennes règles en matière de traitement des fonctions de sécurité ?

Il faut tout d'abord faire une distinction entre les protections externes et les sécurités internes.

Parmi les protections externes, citons pour exemples :

■■ Les capotages intégraux qui, lorsque la porte d'accès est ouverte n'autorisent aucun mouvement dangereux. Cela exclut en général certaines tâches pratiques comme le suivi de trajectoire ou le dépistage de faute. Ce type de protecteur conduit bien souvent à faire exécuter en aveugle des opérations d'usinage, afin de déceler les anomalies de production et bon nombre de pièces sont ainsi jetées au rebus.

■■ Les dispositifs sensibles qui ont pour mission de détecter un passage ou une présence dans une zone de danger. Ils délivrent un ordre qui provoque l'arrêt du mouvement dangereux. Ils autorisent une bonne vision des opérations en cours ; en revanche, ils ne protégent pas des projections de pièces ou d'outils.

La gestion des protections externes peut être confiée soit à une logique câblée, soit traitée directement par les circuits de commande à sécurité intégrée.

Protections internes : on entend par « internes » les fonctions de sécurité qui sont assurées directement par la commande de la machine. Elles ont un rôle de surveillance des consignes de sécurité paramétrées par l'utilisateur.

A titre d'exemples, citons les consignes de vitesse, de position et d'arrêt, qui sont gérées aujourd'hui par la commande d'axe à sécurité intégrée.

La différence essentielle entre une gestion traditionnelle de la sécurité et ce nouveau concept réside dans l'intégration directe des fonctions de détection d'anomalies de fonctionnement (dépassement de consigne) et des moyens d'arrêt sûrs (coupure de la puissance) au sein des circuits de commande et d'entraînement. La *figure 1* schématise la différence des structures utilisées en commande d'axe.

Le traitement entièrement numérique permet de réaliser des fonctions de sécurité sous la responsabilité de l'électronique de commande et des logiciels de l'équipement.

Cette réalisation, adaptée pour assurer les fonctions de sécurité interne, permet également de traiter les fonctions de sécurité classiques, à travers une structure à multiprocesseurs. Ces fonctions de sécurité sont gérées de manière redondante dans le circuit de commande (CN) et dans le circuit d'entraînement (variateur de vitesse) comme le montre, plus en détail le schéma de principe de la *figure 2 (page suivante).*

2.1. Schéma de principe

Se reporter à la figure 2.

2.1.1. Description du concept de « sécurité intégrée »

L'approche théorique du concept de « sécurité intégrée » proposé est basée sur les points suivants :

- Le traitement des informations de sécurité se fait par deux canaux indépendants.
- La comparaison des données s'effectue avec dynamisation forcée ([3]) et comparaison croisée ([4]), afin de déceler des défauts internes.
- L'accès aux données du processeur du variateur est découplé par un automate programmable et par une interface spécialisée des entrées/sorties. Du côté du processeur de la commande numérique, l'accès périphérique se fait directement par la

([3]) La dynamisation forcée permet de déceler des défauts latents dans le logiciel et le matériel des deux canaux de surveillance. Cette dynamisation doit agir au moins une fois dans une période définie (8 heures par exemple). Ainsi, chaque défaut latent présent dans un canal de surveillance sera décelé par la comparaison croisée et le fonctionnement de la machine sera suspendu. Une sollicitation de la dynamisation forcée peut être demandée à chaque ouverture de la porte de protection pour réduire l'intervalle des tests.

([4]) La comparaison croisée permet de déceler des défauts dans les données de sécurité des deux canaux de surveillance.

Fig. 1. Différentes structures utilisées en commande d'axe
- Different structures used in motion control

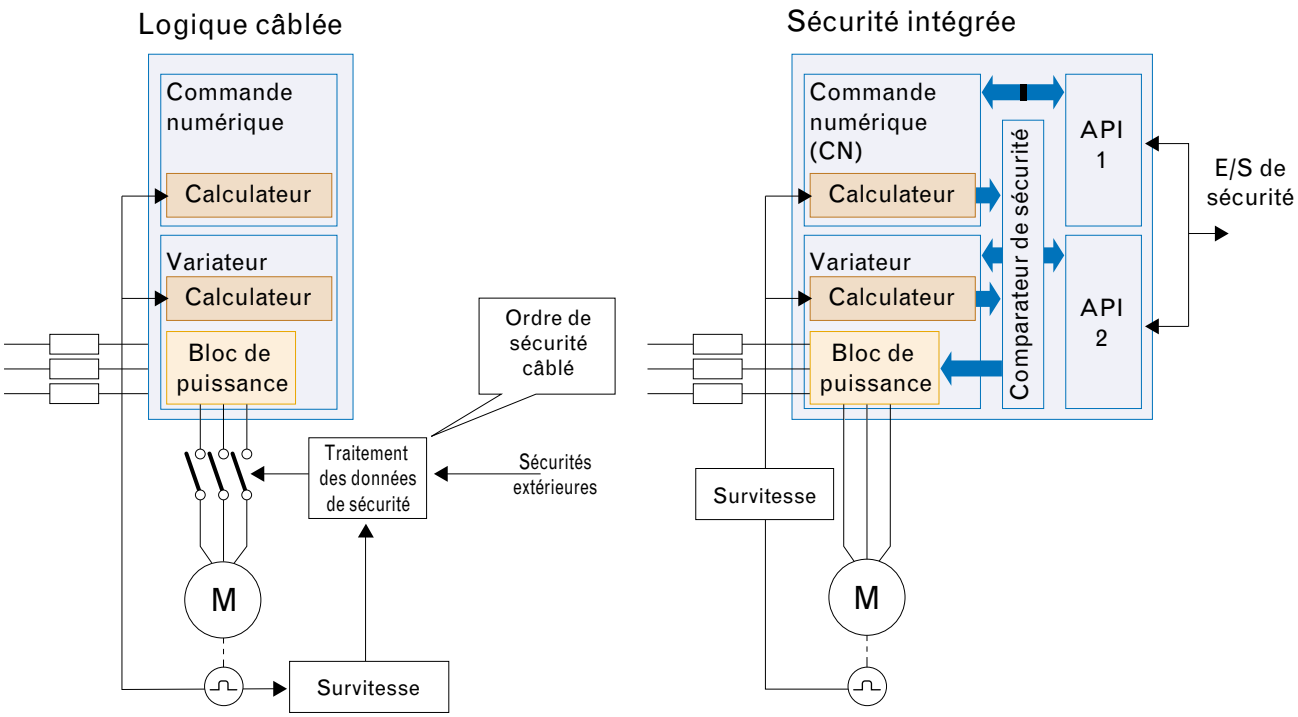
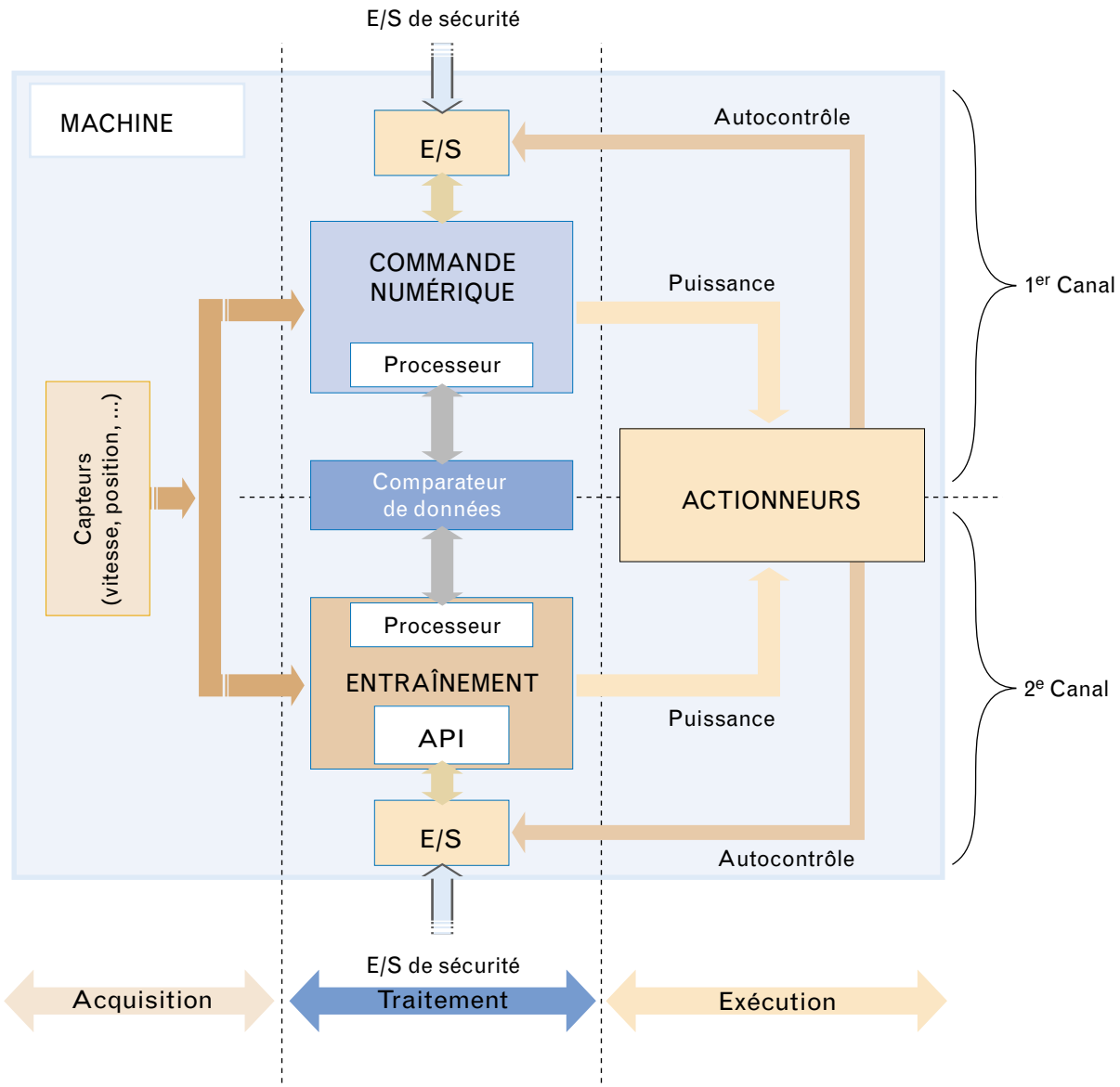


Fig. 2. Principe du concept de sécurité intégrée proposé par la Sté Siemens
- Principle of the concept of safety integrated proposed by Siemens



connexion de l'interface d'entrées/sorties du bus numérique.

■■ Les capteurs de vitesse et de position agissent sur chacun des canaux.

■■ Les actionneurs (moteurs électriques) sont pilotés par les deux canaux de commande des circuits de puissance. Chaque actionneur restitue vitesse et position (autocontrôle).

2.1.1. Fonctions de sécurité

Les fonctions de sécurité sont disponibles dans tous les modes de fonctionnement et peuvent communiquer avec le processus par l'intermédiaire de signaux d'entrée/sortie de sécurité. Ils répondent à la catégorie 3 selon les normes EN 954-1 et 2 [3, 4], ou au niveau SIL 2, selon la norme CEI 61508 [5].

Immobilisation sûre

L'immobilisation sûre n'est pas une fonction indépendante. Elle décrit seulement un processus pouvant être réalisé avec l'aide des fonctions Sinumerik® (safety-integrated). Cette fonction permet d'interrompre les entraînements en mouvement de manière sûre lors de l'action d'une fonction de sécurité (par exemple franchissement d'une barrière immatérielle) et assure le maintien à l'arrêt.

De manière générale, tous les défauts liés à la sécurité dans le système mènent à une immobilisation coordonnée des mouvements dangereux ou à une coupure d'énergie rapide du moteur. Cette coupure d'énergie entre variateur et moteur (les entraînements sont sans couple), nécessaire dans le cas de défaut, se fait sans contact et peut être commandée de manière spécifique sur un axe dans un temps de réaction extrêmement court. L'immobilisation des entraînements résulte d'une stratégie liée à l'exploitation de la machine et peut, tenant compte des possibilités offertes, se faire de manière optimale. Cela signifie un travail en sécurité pour le personnel en mode manuel et, en mode de fonctionnement automatique, une protection supplémentaire pour la machine, l'outil et la pièce.

L'activation de mécanismes de freinage externes complète les fonctions intégrées (vitesse sûre, arrêt sûr, cames sûres, etc.) et permet d'obtenir, lors d'une immobilisation sûre, une distance de freinage au plus court. Les mécanismes de freinage externes peuvent être par exemples :
- des freins mécaniques externes : frein de maintien ou de service,
- des freins électriques externes : frein par court-circuit de l'induit ou par courant de Foucault.

Un contacteur n'est en principe plus nécessaire si la machine possède un commutateur principal assurant la séparation galvanique. Les détecteurs attribués au fonctionnement de la sécurité locale d'une cellule d'usinage, comme par exemple boutons d'arrêt d'urgence, barrières immatérielles, tapis sensible, etc. sont activés lorsque l'un d'eux est sollicité (par exemple porte de protection). Ils agissent de ce fait tout d'abord de manière locale sur cette cellule. Le processus fonctionnant en parallèle dans les autres cellules d'usinage peut se poursuivre. Les capteurs disposés de manière centrale agissent quant à eux sur l'ensemble de la machine.

Vitesse réduite sûre – VS

La fonction VS sert à la surveillance sûre de la vitesse d'un entraînement.

Dans ce cas, la vitesse réelle de l'entraînement est comparée cycliquement (à la fréquence de surveillance), avec la limite de vitesse sélectionnée. Au total 4 limites de vitesse sont disponibles par entraînement. Ceci permet de protéger les personnes et la machine en mode de fonctionnement manuel mais aussi en mode de fonctionnement automatique.

Fins de course logiciels sûrs – PS

Les fins de course logiciels sûrs (PS) permettent de réaliser une délimitation de la zone de travail/protection pour chaque axe. Cela permet par exemple de supprimer les fins de course matériels sur la mécanique. Deux paires de fins de course sont disponibles par axe.

Cames logicielles sûres – CS

La fonction « Cames logicielles sûres (CS) permet de réaliser une détection sûre de zone et de remplacer ainsi la « solution matérielle ».

Quatre paires de cames sont disponibles par axe.

Rampe sûre de freinage – RSF

Après une demande d'arrêt, la vitesse réelle doit diminuer progressivement (surveillance de la vitesse de rotation).

Lors du déclenchement d'une demande d'arrêt, la vitesse réelle atteinte à cet instant, adjoint de la tolérance de vitesse définie pour la machine (paramètre), est retenue comme limite de vitesse. Cette limite, actualisée cycliquement, est comparée à la vitesse réelle (elle doit diminuer ou rester égale). Ainsi, toute nouvelle accélération de l'axe pendant le processus de freinage sera détectée le plus vite possible et une réaction sera déclenchée.

Signaux d'entrée/sortie de sécurité – SES / SSS

Les signaux d'entrée et de sortie de sécurité servent d'interface avec le processus. Ce sont des signaux numériques (tout ou rien) qui sont acheminés sur deux canaux et par différents périphériques (API et CN) au système, ou qui émanent du système.

Logique programmable sûre – SPL

La logique programmable sûre permet pour la première fois un raccordement direct des capteurs et actionneurs de sécurité et de leurs combinaisons logiques. La logique combinatoire est intégrée de manière redondante dans la CN et l'API.

2.1.2. Les modes d'arrêts

Arrêt sûr – AS

En cas de défaut, l'arrêt sûr sert à couper « de manière sûre » l'alimentation du moteur en énergie. Cette opération se fait indépendamment pour chaque axe. La suppression des impulsions de commande des transistors de puissance des entraînements provoque une coupure sûre par électronique de l'alimentation en énergie. La base de la fonction d'arrêt sûr est constituée par la suppression d'impulsions intégrées dans les modules d'entraînement du SIMODRIVE 611D (variateur de vitesse).

Le constructeur de la machine doit prendre des mesures pour éviter tout déplacement après que l'alimentation du moteur en énergie soit coupée (par exemple contre l'affaissement d'axes suspendus).

Caractéristiques fonctionnelles :
- aucun démarrage involontaire du moteur ne peut avoir lieu,
- l'alimentation du moteur en énergie est interrompue de manière sûre,
- il n'y a pas de séparation galvanique entre le moteur et le module d'entraînement.

Arrêt sûr de fonctionnement – ASF

La fonction sert à la surveillance sûre de la position d'arrêt d'un axe ou d'une broche. Les entraînements restent en effet sous asservissement, soit en régulation de position, soit en régulation de vitesse.

Lorsque la surveillance est active, il est possible ainsi d'accéder à une zone de sécurité en mode de fonctionnement manuel (par exemple pour accéder au magasin d'outils) sans devoir couper préalablement les énergies de la machine.

Pour cette fonction, un codeur incrémental suffit. La surveillance repose sur les variations de la valeur réelle de position.

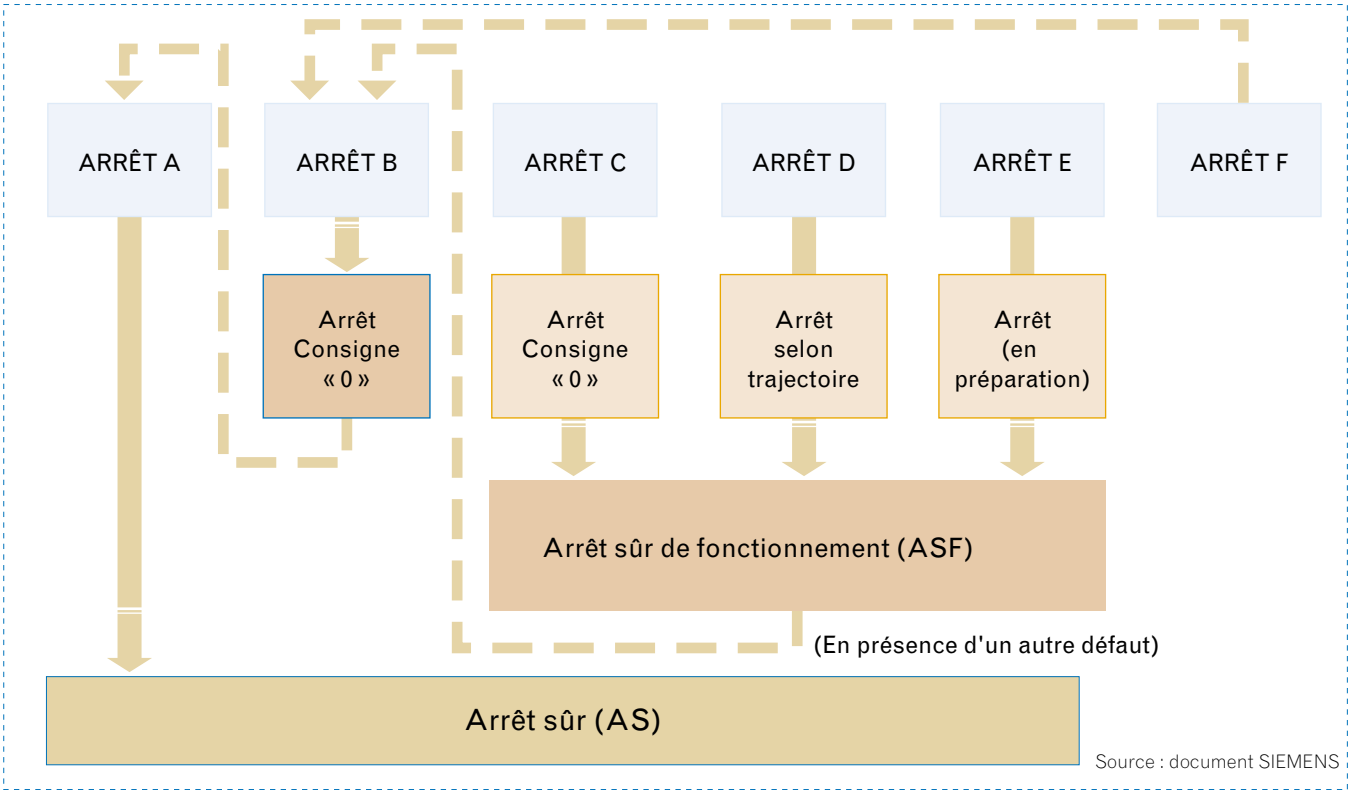
Caractéristiques fonctionnelles :
- l'axe demeure en asservissement,
- la fenêtre de tolérance d'immobilisation est paramétrable,
- le type d'arrêt lors de l'activation de la surveillance est un ASF (arrêt B).

2.1.3. Les types d'arrêts

Une distinction est opérée entre les types d'arrêt A, B, C, D, E, F. Le type de réaction d'arrêt peut être défini de manière fixe par le système lors de la surveillance d'un défaut ou être configurée par le constructeur de la machine.

La *figure 3* décrit ces arrêts.

Fig. 3. Les différents types d'arrêt - *The different types of stop*



Effets des types d'arrêts

Arrêt A

L'entraînement est en roue libre si aucun mécanisme de freinage externe tel qu'un court-circuit d'induit et/ou un frein de maintien est déclenché à la fin de l'arrêt A.

Arrêt B

L'entraînement est freiné aux limites du courant de l'asservissement et passe en arrêt sûr (AS).

Arrêt C

L'entraînement est freiné aux limites du courant de l'asservissement et passe en arrêt de fonctionnement sûr (ASF).

Arrêt D

L'entraînement est freiné le long de la trajectoire, y compris les axes à déplacement simultané puis passe en arrêt de fonctionnement sûr (ASF).

Arrêt E

L'entraînement est freiné le long de la trajectoire, y compris les mouvements de retrait d'urgence puis passe en arrêt de fonctionnement sûr (ASF).

Arrêt F

Le type d'arrêt F est déclenché par la comparaison croisée des résultats et des données. Les défauts latents sont décelés du côté de l'entraînement et de la commande. Un arrêt B est déclenché. A la fin de l'arrêt B, l'arrêt sûr (AS) est efficace.

Rappel :
la norme EN 60204-1 définit trois catégories d'arrêt :
- Catégorie 0 : arrêt par suppression immédiate de la puissance sur les actionneurs (par exemple, arrêt non contrôlé qui correspond à un arrêt du mouvement de la machine par suppression de la puissance aux actionneurs, tous les freins et autres dispositifs d'arrêt étant activés).
- Catégorie 1 : arrêt contrôlé en maintenant la puissance sur les actionneurs pour obtenir l'arrêt de la machine, puis coupure de la puissance quand l'arrêt est obtenu ;
- Catégorie 2 : arrêt contrôlé en maintenant la puissance sur les actionneurs.

Chaque machine doit être équipée d'un arrêt de catégorie 0. Les arrêts de catégorie 1 ou de catégorie 2 doivent être fournis si la sécurité et les spécifications fonctionnelles de la machine l'exigent. Les arrêts de catégorie 0 et 1 doivent être opérationnels, quel que soit le mode opératoire et l'arrêt de catégorie 0 sera prioritaire. Les fonctions « Arrêt » doivent procéder par coupure du courant du circuit correspondant et doivent être prioritaires sur les fonctions « Marche » correspondantes.

2.2. Architecture de la commande d'axe Sinumerik®

Le système de commande d'axe à sécurité intégrée (safety integrated) a été développé par Siemens, afin de pouvoir répondre à la catégorie 3 de la norme européenne EN 954-1. La conformité à cette prescription a été établie par le BIA [5] pour cet équipement, dans le cadre d'une application spécifique en 1997.

Nous rappelons que pour satisfaire à la catégorie 3, le comportement du système doit être tel que

- lorsque le premier défaut survient, la fonction de sécurité est maintenue,
- certains défauts sont décelés, d'autres ne le sont pas,

[5] BIA : Berufsgenossenschaftlichen Institut für Arbeitssicherheit (Sankt Augustin, Allemagne). Site web : www.hvbg.de|bia.

- une accumulation de défauts non décelés peut entraîner la perte de la fonction de sécurité.

Pour atteindre cet objectif, la société Siemens a mis en œuvre une structure redondante avec comparaison croisée des sorties qui apparaît sur la *figure 4*. Cette dernière est complétée par une dynamisation forcée lorsque les signaux d'entrée sont statiques (cf. note (3)).

Il faut aussi souligner que cette structure requiert l'utilisation des composants spécifiques Siemens, à savoir :

- une commande CNC de type Sinumerik 840 D®,
- des variateurs Simodrive 611 D® équipés de cartes de régulation à interface numérique,
- des modules de périphérie compatibles Simatic S7®,
- des moteurs d'axe intégrant un capteur optique (catégorie 3).

Un exemple de configuration

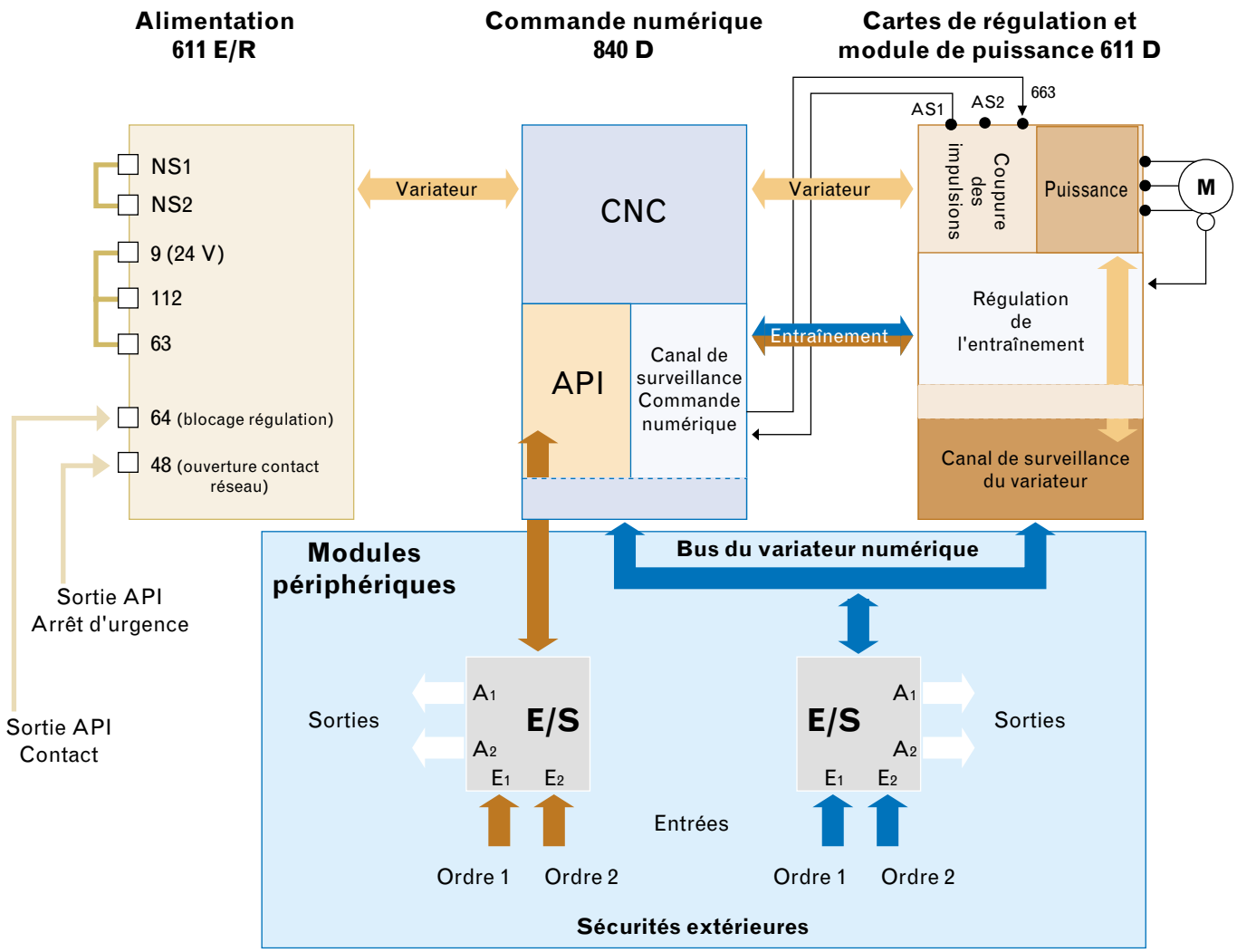
Les généralités sur chacun des modules constituant la Sinumerik® sont rappelées ci-après.

2.2.1. Commande numérique

Sur les machines à commande numérique ou les centres d'usinage, le contrôle de l'ensemble des mouvements nécessaires aux déplacements des axes, aux changements d'outils et à l'usinage proprement dit est assuré automatiquement par une unité centrale couramment appelée « Directeur de Commande Numérique (DCN) » inclus dans la CN. Les besoins de l'usinage grande vitesse des formes complexes exigent qu'aujourd'hui ces directeurs de commande soient de plus en plus performants. On observe ainsi la mise en œuvre de plusieurs microprocesseurs décentralisés afin de gérer les tâches simultanées d'une machine outil ou d'un centre d'usinage. Cette caractéristique a été mise à profit par les constructeurs pour développer le « concept de sécurité intégrée ». Un des processeurs interne à la CN, se voit donc affecté d'une tâche supplémentaire à savoir le traitement des informations de sécurité. Ce processeur n'aura cependant pas d'influence sur la gestion des arrêts, tâche dévolue au comparateur de sécurité implanté dans la CN.

Ces machines sont conçues en outre pour assurer des conditions d'exploitation particulières notamment l'emploi successif et parfois simultané, de plusieurs outils différents. Pour assurer cette multitâche et afin de limiter les temps morts, certaines fonctions sont mises en œuvre par anticipation. Cet aspect doit être pris en considération car il peut interférer dans la gestion des fonctions de sécurité et plus particulièrement en mode intervention « portillon ouvert ».

Fig. 4. Structure redondante - *Redundant structure*



2.2.2. Variateurs de vitesse

La variation de vitesse ou convertisseur de fréquence est maintenant largement utilisé pour piloter les moteurs électriques. Il permet d'adapter rapidement les paramètres moteurs à la tâche à exécuter (vitesse, couple, rampe d'accélération et de décélération, etc.).

2.2.3.1. Caractéristiques générales d'un variateur de vitesse

Son raccordement au réseau électrique s'effectue par l'intermédiaire d'un module d'alimentation qui délivre à la fois la tension du circuit intermédiaire (600 V) et la tension d'alimentation de l'électronique. Ce module alimente le ou les modules de puissance qui eux-mêmes alimentent les actionneurs ou moteurs.

Adjoints de cartes de régulation, ces modules de puissance deviennent des variateurs de vitesse. Ils peuvent ainsi piloter des axes de type « avance » ou des axes de type « broche ».

La communication avec la commande numérique s'effectue par le bus spécialisé d'entraînement.

La structure simplifiée d'une commande d'axe est représentée sur la *figure 5.*

2.2.3.2. Principe de fonctionnement d'un arrêt

On recense aujourd'hui trois solutions pour générer un arrêt sur un variateur de vitesse :

- couper les impulsions de commande qui pilotent la fréquence,
- imposer au variateur une consigne de vitesse « zéro »,
- couper l'énergie électrique de l'actionneur.

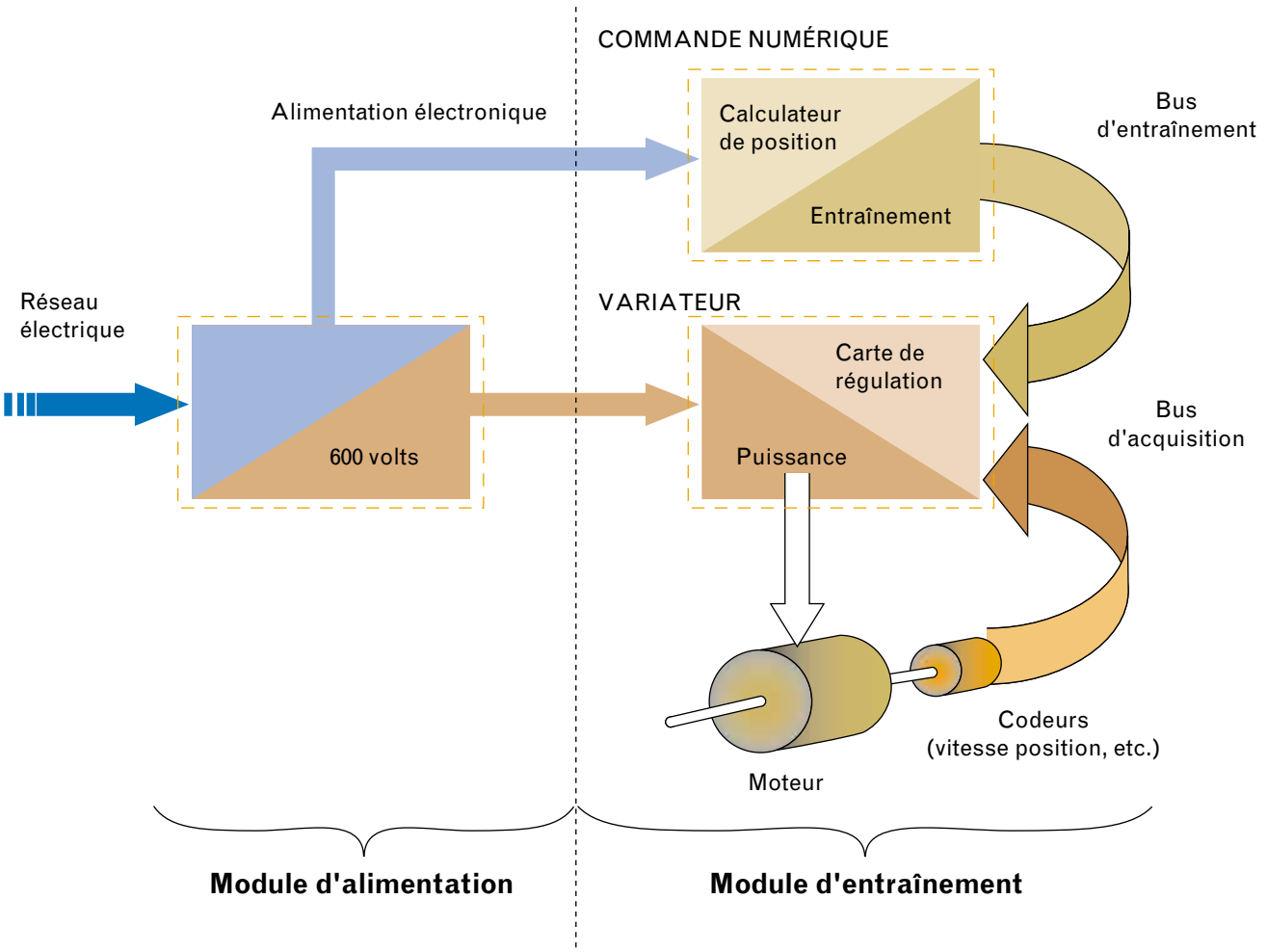
Suivant le principe mis en œuvre, les performances d'arrêt ne sont toutefois pas identiques. On observe ainsi des écarts importants qu'il convient de maîtriser pour obtenir un arrêt dit de sécurité.

On peut en effet s'interroger sur chaque principe et sur les conséquences de sa mise en œuvre éventuelle :

Coupure des impulsions de commande

Lorsque l'on coupe les impulsions de commande d'un variateur de vitesse, l'énergie électrique transmise devient nulle et l'actionneur est laissé en roue libre. Il en résulte que l'énergie cinétique emmagasinée par le mécanisme entretient le mouvement. Ce mouvement s'annulera plus ou moins rapidement, selon l'inertie des masses en mouvement et le coefficient de frottement des entraînements liés à l'actionneur. Par conséquent établir un arrêt d'urgence basé sur une simple coupure des impulsions de commande du variateur n'est pas une solution satisfaisante.

Fig. 5. Structure simplifiée d'une commande d'axe - *Simplified structure of a motion controller*



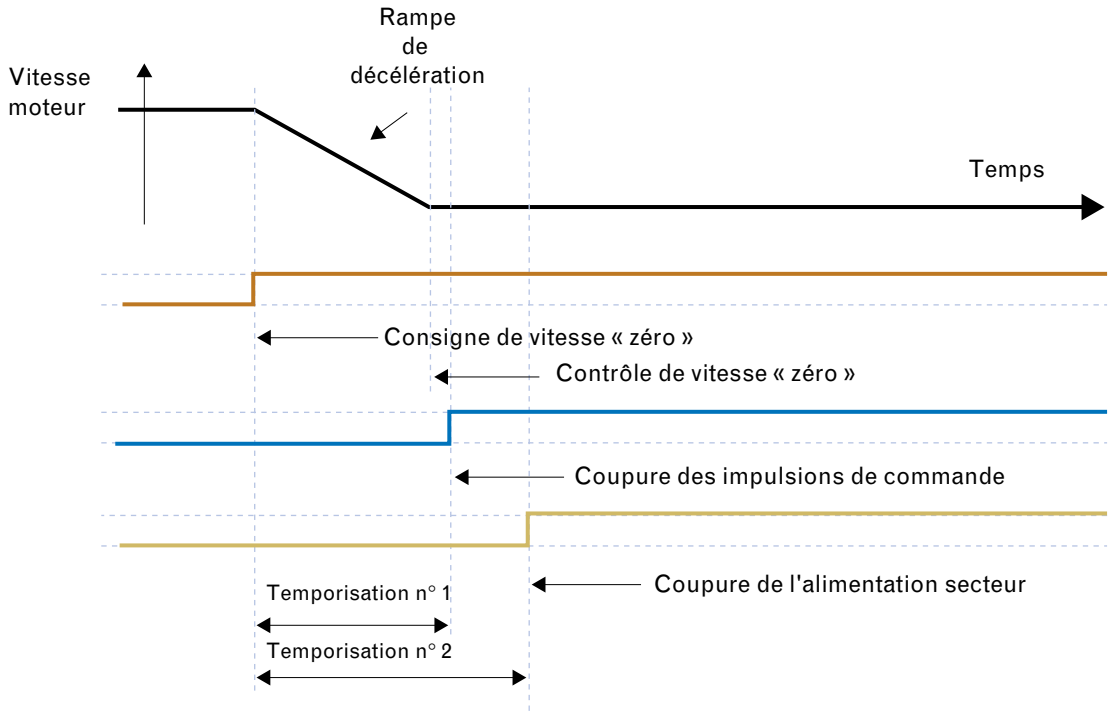


Fig. 6.
Séquencement d'un arrêt sûr (AS)
- Sequencing of safe stop

Consigne de vitesse « zéro » / freinage électrique

On sollicite, à travers la commande du variateur une consigne de vitesse nulle. Cette dernière sera obtenue plus ou moins rapidement en fonction de la rampe de décélération. Outre les contraintes mécaniques de l'application, cette décélération est limitée par le constructeur afin de ne pas détériorer les circuits électriques de freinage. Cette énergie de récupération par contre-courant doit en effet être absorbée sans provoquer une élévation thermique trop importante conduisant à la destruction des éléments de dissipation. Généralement, ce moyen de freinage est très performant. Il permet de maintenir un suivi des mouvements car les asservissements sont maintenus sous tension. De ce fait tout redémarrage « à chaud » est permis sans procédure particulière et sans réinitialiser les axes.

Maintenir les asservissements sous tension en présence de moteurs linéaires offre aussi l'intérêt, d'entretenir des champs électromagnétiques. Ce dernier engendre un couple mécanique qui maintiendra en position et à l'arrêt les moteurs linéaires.

Coupure de l'énergie électrique

Le sectionnement instantané de l'énergie électrique sur un variateur de vitesse a plusieurs effets selon le type d'actionneur mis en œuvre.

■■ Si l'actionneur est un moteur linéaire : on se retrouve dans le même contexte que la coupure des impulsions de commande, c'est à dire en présence d'un actionneur libre de tout mouvement.

■■ Si l'actionneur est un moteur asynchrone ou synchrone :

● non équipé d'un freinage mécanique par manque de tension, on observe les mêmes conséquences qu'avec un moteur linéaire, avec toutefois moins d'inertie car l'entraînement, généralement constitué d'une vis sans fin, est souvent plus rigide et plus lent ;

● équipé d'un freinage mécanique par manque de tension, la performance d'arrêt est liée à l'efficacité du frein. Généralement ce type de freinage est rapide, mais il est très éprouvant pour la mécanique. Malgré cette caractéristique, un arrêt par freinage électrique (consigne « zéro ») est souvent plus efficace et plus approprié pour la mécanique. De plus, les dispositifs de freinage montés sur ces moteurs sont statiques (frein de parking), non prévus pour des freinages dynamiques fréquents.

En revanche, l'isolement galvanique induit par la coupure du relais est essentiel pour tout intervenant pendant les opérations de maintenance, d'entretien et de contrôle.

En résumé, l'arrêt sur un variateur de vitesse se doit d'agir le plus rapidement possible sur le mouvement qu'il pilote tout en favorisant si possible une mémorisation de la position de l'axe pendant cette action. Il doit également être capable de fournir une isolation galvanique vis-à-vis du réseau électrique et dans certains cas être en mesure de dissiper les énergies de freinage. Pour satisfaire à tous ces critères, des solutions existent, mais elles doivent s'accomplir de manière séquentielle, afin d'obtenir un arrêt de sécurité.

Le meilleur compromis est obtenu par un freinage électrique généralement de type consigne à « zéro », suivi ensuite par une interruption des impulsions de commande des transistors de puissance et enfin par une coupure de l'alimentation secteur. Il est évident que pour réaliser une telle séquence d'arrêt, les événements doivent s'effectuer séquentiellement et non pas simultanément. Des délais intermédiaires entre chaque action sont en effet nécessaires pour que le freinage puisse s'opérer dans sa totalité, même en présence d'un dysfonctionnement [6]. La première temporisation permet à l'asservissement d'agir jusqu'à l'obtention d'une vitesse nulle, la seconde permet quant à elle de garantir un arrêt sûr en présence d'une défaillance de l'électronique de commande du convertisseur. La séquence de freinage est représentée sur la *figure 6.*

2.2.4. Actionneurs

2.2.4.1. Moteurs linéaires

Cette technologie offre par rapport aux actionneurs conventionnels (moteur synchrone, moteur asynchrone et moteur à courant continu) certains avantages, notamment pour l'usinage à grande vitesse. Les machines deviennent ainsi plus dynamiques, plus précises et plus productives. Par rapport à des systèmes de vis à billes, les restrictions concernant la longueur des axes sont moins contraignantes, on atteint ainsi des longueurs d'axe allant jusqu'à plusieurs dizaines de mètres (< 50 m) ; la vitesse est multipliée par un coefficient proche de 2 (vitesse maximum constructeur < 120 m/min) et les accélérations sont supérieures (accélération maximum constructeur < 20 m/s^2). Par ailleurs, on obtient des moteurs linéaires une plus grande précision ou résolution de positionnement. La réduction du nombre d'éléments dans la chaîne cinématique entraîne une meilleure fiabilité et par voie de conséquence une maintenance moins coûteuse. Une plus grande fiabilité et un accroissement de la durée de vie, de même que leur flexibilité et leur souplesse, offrent la possibilité de monter plusieurs parties mobiles sur un seul axe.

Malgrè ces avantages, cette technologie ne domine pas le marché des centres d'usinage UGV car elle a des contraintes fortes en termes de :

- sécurité par rapport aux champs magnétiques ouverts,
- rendement et échauffement,
- poussée limitée qui oblige à multiplier les motorisations pour un même axe.

2.2.4.2. Moteurs synchrones et asynchrones

Les moteurs synchrones et asynchrones, couramment utilisés sont généralement accouplés à une mécanique telle que vis à billes ou crémaillère pour réaliser un déplacement linéaire. Cette technique éprouvée offre d'autres avantages par rapport aux moteurs linéaires. Elle permet en effet, par l'intermédiaire de réducteurs d'accroître les efforts de poussée ou de traction. En revanche, la mécanique mise en œuvre (vis à billes ou crémaillères) réclame un certain entretien pour continuer à assurer sa fonction sans aléa de fonctionnement (dans un centre d'usinage par exemple, les copeaux sont généralement source d'ennuis).

(6) BG : Berufsgenossenschaft (équivalent allemand de : Caisse d'assurance-maladie).

TABLEAU I

COMPARAISON DES PERFORMANCES DES DIFFÉRENTS TYPES DE MOTEURS (*)

- COMPARISON OF THE PERFORMANCE OF THE DIFFERENT TYPES OF MOTORS

Caractéristiques	Moteur linéaire	Moteur standard
Force maximum	< 20 000 N	< 240 000 N
Accélération maximum	< 20 m/s^2	< 15 m/s^2
Vitesse maximum	< 120 m/min	< 80 m/min
Longueur maximum	< 50 m	< 6 m

(*) Remarques :
- Les valeurs indiquées sont des valeurs théoriques sans charge. La combinaison de certaines valeurs maximums n'est pas possible.
- Des précautions de langage doivent être prises car il existe aussi des types synchrones et asynchrones pour les moteurs linéaires.

2.2.4.3. Comparaison des performances entre moteurs linéaires et moteurs standard (synchrones, asynchrones) équipés de vis à billes

Se reporter au *tableau I.*

2.3. Gestion des fonctions de sécurité extérieures (proposition Siemens)

L'apport d'une chaîne redondante, pour la gestion des fonctions de sécurité dans le circuit de commande d'une machine-outil, est d'une aide précieuse. Il faut toutefois relativiser et faire la différence entre fonctions de sécurité directe et indirecte [7] (cf. définitions). En effet, si les fonctions de sécurité indirecte ne posent pas de problème quant à leur traitement par des automates programmables industriels, il en va différemment pour les fonctions de sécurité directe.

Les textes stipulent dans la norme européenne EN 60204-1 au § 11.3 pour ce qui concerne les équipements programmables que : « il est difficile de se fier au bon fonctionnement d'un canal unique sur un équipement électronique programmable. Tant que cette situation perdurera, il n'est pas judicieux de se fier au bon fonctionnement d'un tel dispositif à canal unique » [8].

Aujourd'hui, l'apparition de dispositifs dédiés à la sécurité change la donne. Ces nouveaux matériels ont en effet été conçus pour suppléer les circuits conventionnels à logique câblée. Plusieurs organismes allemands (BIA, BG)(6) ont reconnu cette avancée et ont délivré des certificats de conformité aux normes européennes, notamment EN 60204-1 et EN 954-1. Il paraît donc utile à ce jour de vérifier dans quelle mesure ces nouvelles techniques peuvent constituer une avancée pour la prévention. Le principe de sécurité intégrée constitue un exemple type : le fait de disposer de deux voies de traitement hétérogènes au sein d'un équipement, permet en principe de réaliser un circuit de commande de catégorie 3 (cf. EN 954-1) ; la validation en pratique de tels systèmes reste difficile [9]. La *figure 7* illustre schématiquement comment sont traités les signaux d'entrées/sorties de sécurité.

3. Autres aspects du concept de commande d'axe

D'autres constructeurs étudient actuellement de nouveaux concepts dits de « sécurité intégrée ». Il convient néanmoins de s'interroger sur la meilleure façon de réaliser une sécurité intégrée sur une commande d'axe.

Deux solutions se présentent :

1°- À partir de l'équipement fonctionnel de la machine-outil, on utilise dans la structure en place existante le potentiel technique des processeurs non employés à 100 %. Dans ce cas précis, ces processeurs, en plus du traitement de leur activité de fond, se voient rajouter une tâche dite « de sécurité ». Ayant la faculté de communiquer entres eux, ces processeurs peuvent ainsi échanger un grand nombre de données ; il est donc aisé de leur faire

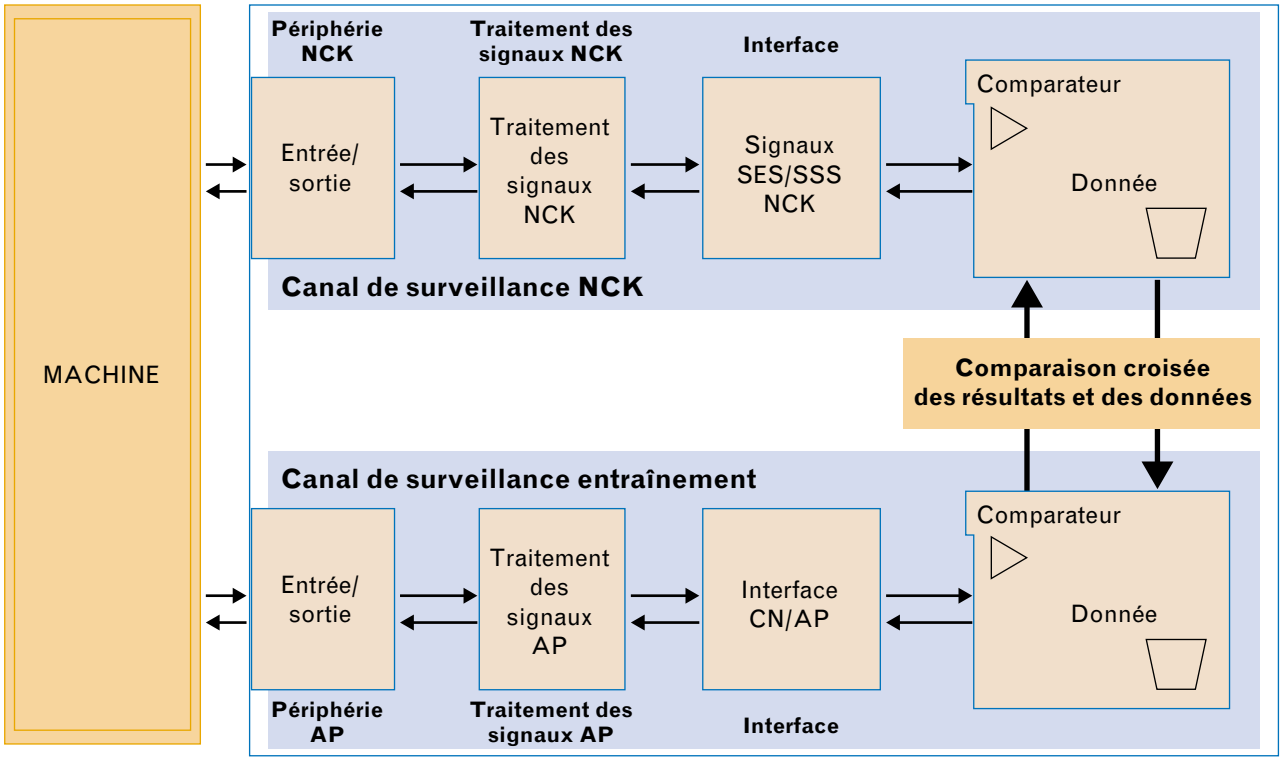


Fig. 7. Gestion des fonctions de sécurité directe d'une machine
- Management of the safety critical functions of a machine

comparer leurs résultats sous la forme d'un échange croisé. On réalise ainsi une redondance avec comparaison sans apports supplémentaires de matériels, hormis l'extension du logiciel. Dans ce cas, le seul élément matériel vraiment original dédié à la sécurité se trouve dans le variateur (il se présente sous la forme d'un module spécialisé dans la réalisation d'une commande d'arrêt sûr).

2°- Une voie spécialisée pour le traitement des sécurités a été développée indépendamment du fonctionnel. Dans ce cadre, il est nécessaire de prévoir un ou deux capteurs supplémentaires dédiés à la sécurité qui seront implantés sur le moteur électrique indépendamment des capteurs affectés au fonctionnel. De plus, une chaîne redondante avec comparaison des résultats doit être créée afin de satisfaire à la catégorie 3. La sortie du comparateur viendra ensuite agir sur le module spécialisé du variateur pour exécuter l'arrêt.

Avantages et inconvénients de ces solutions

■■ La première solution, en l'occurrence celle proposée par Siemens, s'avère la moins coûteuse, puisqu'elle utilise en grande partie le matériel standard mis en place. Par contre, chaque processeur doit exécuter et le fonctionnel et les fonctions de sécurité. Il n'y a donc pas d'indépendance matérielle et logicielle. De plus, les extensions sont limitées (saturation des calculateurs) et chacune d'entres elles est difficilement validable ([7]).

■■ La deuxième solution se montre plus souple, moins pénalisante au niveau performance de la commande numérique, plus sécuritaire et plus apte à la validation. En revanche, elle nécessite une approche sécurité différente et un coût plus élevé.

([7]) « Validable » sous-entend un matériel qui se prête à la vérification de ses fonctions, notamment celles de sécurité et ce, en conformité avec les normes en vigueur (par exemple : EN 954-1).

4. Réflexions sur le concept de « sécurité intégrée »

L'analyse de la commande d'axe à sécurité intégrée proposée par Siemens, a été réalisée à l'INRS au travers d'un banc d'essai simulant une commande numérique à deux axes.

Bon nombre de questions ont été abordées lors de cette analyse, notamment sur le concept même de « sécurité intégrée ». Elles se résument comme suit :

4.1. Comment assurer la protection des opérateurs ?

Ce choix est conditionné par l'analyse des risques effectuée sur chaque famille de centre d'usinage et sur l'environnement proche de ces machines (portiques, palettiseur, etc.). Cette analyse tient compte des différents modes de fonctionnement de l'équipement de production (automatique, contrôle, entretien, maintenance, etc.).

■■ En mode automatique, c'est-à-dire portillon d'accès fermé, interverrouillé et autocontrôlé, la sécurité ultime de l'opérateur repose sur l'efficacité du carénage. Ce dernier doit rester infranchissable, quel que soit le projectile auquel il est soumis. En fonction de la taille des outils et de leur vitesse de coupe mais aussi du volume des pièces à usiner, une étude approfondie des caractéristiques propres à chaque carter de protection doit être appliquée. Cette étude devra également prendre en compte le poste de travail, c'est-à-dire intégrer le ou les emplacements privilégiés des opérateurs pour leurs opérations de contrôle routinier, les hublots de visualisation ne devront pas être moins performants que l'ensemble de la cartérisation.

■■ En mode intervention (maintenance, entretien, vérification de trajectoire, contrôle, mesure, dépistage de collision, chargement d'un outil, etc.), le portillon est ouvert. Dans ce mode particulier d'intervention, deux éventualités de fonctionnement sont à envisager :

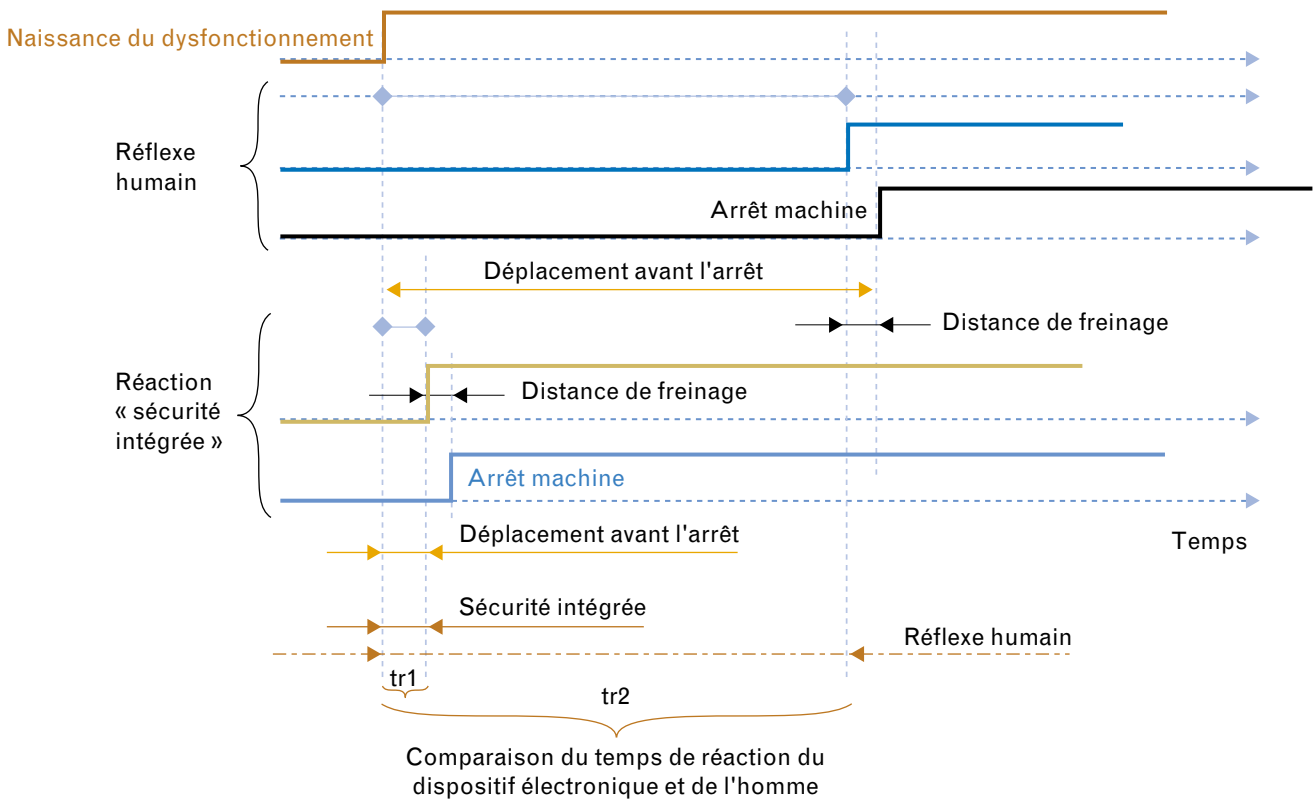
- la première n'offre pas de liberté de mouvements ; il s'agit d'un simple contrôle comme par exemple la vérification de l'état de surface d'usinage ou de l'état d'un outil. Cette opération ne présente pas, hormis le redémarrage intempestif d'un des axes restés sous asservissement, de risques nouveaux nécessitant une procédure d'intervention particulière ;
- la seconde autorise à vitesse réduite (environ 2 m/min) l'ensemble des mouvements de l'équipement, en l'occurrence du centre d'usinage et de ses périphériques (magasin d'outils, tourelle d'amenée, etc.). La présence de mouvements, certes limités, est source de risque ; des précautions particulières sont donc à mettre en œuvre pour assurer la sécurité de l'opérateur.

Plusieurs moyens y concourent aujourd'hui, à savoir :

- les mouvements ne sont autorisés que sous couvert d'un dispositif de validation (enabling device). Ce dernier est équipé de différents organes de commande tels qu'interrupteur « gâchette » ou bouton poussoir à trois positions qui ne libèrent les mouvements que lorsqu'ils sont maintenus en position médiane. Les deux autres positions agissent quant à elles comme un arrêt. Ce dispositif de validation est nécessaire quand la sécurité intégrée n'est pas activée. En revanche, si cette dernière est toujours opérationnelle, la mise en œuvre d'un dispositif de validation devient illusoire ;
- adjonction d'un pupitre mobile (manivelle) qui vient suppléer le clavier de commande résidant de l'équipement. Toutes les opérations de déplacement du centre d'usinage sont ainsi rendues manuelles mais à vitesse réduite. Ce pupitre mobile est également équipé d'un bouton « Homme mort » qui ne valide les actions que lorsqu'il est sollicité.

Bien entendu, ces dispositifs de sécurité ne sont pas suffisants à eux seuls pour assurer entièrement la sécurité des opérateurs. A l'évidence ils ne peuvent prévenir d'un ordre intempestif émis par le circuit de commande ou d'un dysfonctionnement d'un capteur de prise d'information. C'est dans ce contexte que la sécurité intégrée présente tout son intérêt. En effet, la présence d'une chaîne redondante de traitement de l'information (CN + variateur) offre la possibilité de surveiller en permanence pendant toutes les opérations de production, y compris en mode intervention, les caractéristiques de vitesse et d'ar-

Fig. 8. Comparatif des temps de réaction entre la sécurité intégrée et une intervention humaine
Comparison of the reaction time between the safety integrated function and human intervention



rêt des axes. La rapidité d'action de l'électronique actuelle est bien plus compétitive comparée à une intervention humaine déclenchée par un geste réflexe. Le diagramme représenté sur la *figure 8* illustre parfaitement ce propos.

Les temps de réaction sont disproportionnés et la performance d'arrêt qui en résulte peut varier dans un rapport (tr2/tr1) au minimum de 10 et souvent de 100.

Le temps de freinage est toujours constant, quel que soit le mode de sollicitation (sécurité intégrée ou humaine) ; toutefois, la performance d'arrêt est liée à la somme du « temps de réaction » et du temps de freinage. En effet, plus le temps de réaction est grand, plus la distance d'arrêt sera importante et par conséquent, dangereuse pour un opérateur.

Dans le domaine de l'usinage grande vitesse, notamment dans le cas des mouvements à 100 m/min, cette notion est très importante. On observe ainsi des distances d'arrêt de quelques millimètres à quelques dizaines de centimètres, pour des arrêts sous contrôle respectif soit de la sécurité intégrée, soit de l'opérateur.

On peut donc s'interroger sur la possibilité d'évitement d'un heurt par un opérateur équipé d'un dispositif de validation ou d'un dispositif « Homme mort » intervenant au cœur d'un centre d'usinage (UGV) ?

Aujourd'hui, l'approche des industriels dans ce milieu évoluant quelques fois à 120 m/min, est quasi-unanime : la sécurité intégrée n'est plus une option, elle doit être implantée d'office dans tout outil de production à usinage grande vitesse.

4.2. Comment est perçue cette avancée technique d'un point de vue sécurité ?

Il faut tout d'abord distinguer la sécurité de l'opérateur de celle du matériel.

En matière de prévention des accidents du travail, un des objectifs est de veiller à ce que l'outil de production – en l'occurrence, dans le cas présent, celui d'un centre d'usinage (UGV) – ne soit pas source d'accident. Cela implique de procéder à une estimation globale des risques engendrés par l'équipement en production dans toutes les phases d'intervention. Une telle analyse ne tient généralement pas compte de la sécurité du matériel, hormis pour les risques de projection par bris d'outil ou éjection de pièce. On entend par sécurité matérielle, les chocs mécaniques internes entre les outils et la pièce à usiner ou le bâti pouvant conduire à un arrêt de la production ou à la détérioration de l'équipement.

En usinage grande vitesse, l'analyse des risques prend partiellement en compte cette protection du matériel. En effet, profitant des performances d'arrêt actuel de la sécurité intégrée, certains constructeurs de machines-outils spécifiques réclamant une précision supérieure à la normale (> µm), ont mis à profit cette avancée technique pour s'affranchir au maximum des dommages causés en cas de collision et garantir ainsi la pérennité des caractéristiques de leurs équipements.

4.3. Qu'offre ce principe de sécurité intégrée par rapport aux circuits de commande traditionnels ?

Il est indéniable, au vu des performances d'arrêt obtenues par cette surveillance électronique, que le concept de sécurité intégrée apporte en matière de sécurité une assistance précieuse. Cette avancée a pris toute sa valeur à l'arrivée de l'usinage grande vitesse. En effet, jusqu'à cette dernière décennie, les vitesses de mouvements d'une machine à commande numérique conventionnelle restaient certes élevées, mais offraient encore des possibilités d'évitement de l'accident. Aujourd'hui, les déplacements et les vitesses de rotation sont tels que, sans préjuger des capacités de réaction d'un opérateur averti, le moindre retard d'action entraîne un mouvement linéaire ou circulaire de plusieurs dizaines de centimètres et par conséquent, une situation que l'on qualifiera de dangereuse. Pour les préventeurs, la sécurité intégrée est à considérer comme un élément non négligeable de sécurité dans le concept d'une commande d'axe à UGV.

Les missions de surveillance de la sécurité intégrée concernent prioritairement : la vitesse et le maintien à l'arrêt. D'autres missions lui sont attribuées telles que la surveillance des cames sûres ou de la position sûre, mais celles-ci ne semblent pas encore, avoir été utilisées systématiquement par les concepteurs. En revanche la structure redondante, qu'offre ce principe de sécurité intégrée, présente un intérêt quant à la gestion des fonctions de sécurité directe au sein d'une machine-outil.

4.4. Comment peut-on assurer la pérennité des logiciels?

La pérennité des logiciels et donc indirectement de la sécurité des opérateurs, repose sur les moyens d'inaccessibilité aux paramètres de sécurité dès lors que la machine est mise à disposition de l'utilisateur. Cette inaccessibilité dépend des « mots de passe » dont l'efficacité est plus qu'aléatoire compte tenu des pratiques actuellement utilisées dans les interventions de dépannage.

Toutefois, la complexité pour modifier les paramètres machine est telle que, jusqu'à présent, aucun utilisateur n'a pris le risque d'entreprendre une telle manœuvre par peur de mettre hors service la commande numérique ou le centre d'usinage. Dans ce contexte, on peut s'interroger sur le bien fondé d'implanter des mots de passe hiérarchisés pour l'accès aux logiciels de sécurité. En effet la protection par mot de passe est souvent dévoilée car souvent les constructeurs, pour satisfaire à un dépannage téléphonique rapide, sont obligés de les communiquer. Compte tenu de leur responsabilité et du maintien de la conformité de l'équipement, ce sujet reste d'actualité et les intégrateurs se demandent à quel niveau ils doivent interdire les accès.

5. Discussions et conclusions

Aujourd'hui, le concept de sécurité intégrée tend à s'imposer auprès des grands constructeurs de machines-outils dans la limite où il est associé à une commande d'axe performante.

En plus d'assurer une prévention plus efficace lors de certaines phases d'exploitation jusqu'alors totalement ignorée par manque de solutions adéquates, ce concept permet de réduire les investissements matériels dédiés à la sécurité puisque toute l'infrastructure est fournie d'origine.

Néanmoins, malgré ces avancées, il y a lieu de s'interroger sur les inconvénients potentiels inhérents à la complexité d'un tel produit. C'est ainsi que dans ce document, ont été abordés les aspects qui posent problème notamment :

- la mise en œuvre (matériel et logiciel),
- la validation de l'équipement « commande d'axe à sécurité intégrée »,
- les transferts de risques.

5.1. Mise en œuvre correcte du concept

■■ Dans un premier temps, il convient de bien définir tous les risques et d'appliquer pour chacun d'eux le type de solution appropriée, à savoir mettre en œuvre :

- une stratégie adaptée,
- un arrêt rapide (avec possibilité de dégrader la mécanique),
- un arrêt progressif (beaucoup plus long),
- un arrêt avec coupure des énergies,
- le dispositif de validation (enabling device),
- verrouillage/interverrouillage des capots de protection,
- …

■■ Dans un second temps, il importe de distinguer les sécurités externes (arrêt d'urgence, barrages immatériels, contacts de portes, etc.) des sécurités internes (vitesse sûre, cames sûres, etc.) mises à la disposition dans la commande numérique. En effet, le traitement des sécurités internes transite uniquement par deux voies en logique programmée alors que les sécurités externes peuvent transiter, soit par les mêmes voies à logique programmée, soit par une logique câblée selon les besoins définis lors de l'analyse du risque. Le choix est souvent dicté par des raisons de validation, cette dernière étant beaucoup plus aisée à ce jour en logique câblée.

5.2. Validation du système

Malgré la validation du concept de la « sécurité intégrée » par un organisme habilité en Allemagne, la validation de l'application dans son ensemble pose problème. En effet il n'existe pas encore de référentiel normatif spécifique pour ce type de système, ni d'outils permettant de valider le logiciel applicatif. Ce dernier point est toujours d'actualité ; il fait l'objet de recherches au sein des organismes de sécurité.

5.3. Des mouvements, bien que ralentis, mais toujours présents

Le fait d'autoriser les opérateurs à observer porte ouverte et à vitesse réduite un programme d'usinage, soulève de la part des préventeurs une certaine inquiétude. En effet, la machine exécute des mouvements certes au ralenti mais qui peuvent s'avérer dangereux si l'opérateur pénètre dans l'enceinte d'usinage. Dans ce contexte, des précautions particulières sont donc à appliquer, notamment celles liées aux procédures d'intervention, afin de limiter au mieux les situations critiques, voire dangereuses si les mouvements ne sont pas immobilisés rapidement. Les dispositifs de validation (enabling device) permettent quant à eux de donner aux intervenants un moyen de stopper ou d'interdire les mouvements ; néanmoins cette solution repose sur leur vigilance et lucidité en présence d'un danger.

5.4. Transfert de risques

On réduit la vigilance des opérateurs, ce qui les rend plus vulnérables à une situation imprévue. En effet l'introduction de ce concept dans le monde industriel s'est fait d'une telle manière qu'actuellement les utilisateurs y font une confiance totale. Le fait de se sentir sous contrôle d'un système de sécurité peut cependant, à la longue, conduire l'opérateur à accomplir des actions dangereuses. L'accoutumance est un phénomène nouveau qui est apparu récemment dans le domaine de l'usinage grande vitesse. Il risque de s'accentuer si aucune démarche n'est entreprise pour informer les opérateurs des risques qu'ils encourent. Pour y pallier, nous ne pouvons que conseiller aux intégrateurs de mettre en œuvre des moyens de sensibilisation et d'information sur ce caractère négatif qu'engendre ce concept de sécurité intégrée. Plus les opérateurs seront informés, plus les procédures seront respectées et plus le niveau de sécurité sera satisfaisant.

En outre, l'apport de nouvelles technologies telles que les moteurs linéaires ou les variateurs de vitesse posent certains soucis notamment pour les arrêts d'urgence. En effet, si la puissance électrique est sèchement interrompue par l'action d'un sectionneur, on ne peut contrôler les performances d'arrêt (distance et temps) de ces équipements. Sans énergie, les moteurs linéaires ne sont plus stabilisés en position (maintien en position par la boucle électromagnétique), de même tout variateur privé de son alimentation électrique, rend libre le mouvement qu'il est sensé contrôler en vitesse.

Pour conclure, la mise en œuvre d'un dispositif dédié à la sécurité, afin d'assurer la protection du personnel, n'est pas une condition sine qua non. Il faut en effet veiller à ce que ce dispositif soit implanté suivant les règles de l'art et qu'il réalise la mission pour laquelle il est dévolu. En outre, l'appellation « dédié à la sécurité » n'est pas synonyme de risque « zéro » en matière d'accidents ; l'expérience le prouve car toute mauvaise application peut être au contraire initiatrice de risques nouveaux. Il ne faut pas non plus négliger l'aspect « accoutumance » et laisser croire aux opérateurs que toutes leurs erreurs seront prises en considération par le dispositif dédié à la sécurité. Ils ne peuvent en effet effectuer toutes opérations non réfléchies du seul fait qu'ils sont sous couvert d'un dispositif dédié à la sécurité. Ce dispositif réagira certes pour les tâches auxquelles il est programmé, mais en aucun cas il ne pourra pallier les défaillances de conception (mauvais paramétrage, seuils de sécurité mal définis, etc.).

Enfin, nous avons pu observer une nouvelle fois, après l'étude sur les Automates Programmables Industriels dédiés à la sécurité (APIdS) [10, 11], que la validation d'un matériel électronique complexe dédié à la sécurité n'est pas simple lorsque le matériel est commercialisé. C'est pourquoi à l'avenir, dans le cadre de nouvelles validations, l'INRS s'appuiera sur les certificats déjà établis par les organismes européens notifiés en ce domaine.

BIBLIOGRAPHIE

[1] LUPIN H. – Centres d'usinage à grande vitesse (centres « UGV »). *Cahiers de notes documentaires — Hygiène et Sécurité du Travail, 2000, 181, ND 2138, pp. 40-53.*

[2] Dossier – Sécurité accélérée pour usinage à grande vitesse. *Travail et Sécurité, nov. 1999, 590, pp. 30-39.*

[3] NF EN 954-1 – Sécurité des machines. Parties des systèmes de commandes relatives à la sécurité. Partie 1 : Principes généraux de conception. *Paris, AFNOR, févr. 1997, 38 p.*

[4] prNF EN 954-2 : révision 1999 – Sécurité des machines. Parties des systèmes de commandes relatives à la sécurité. Partie 2 : Validation. *Paris, AFNOR, mars 2000, 68 p.*

[5] CEI 61508-1 à 61508-7 – Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité. Partie 1 : prescriptions générales. Partie 2 : prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité. Partie 3 : prescriptions concernant les logiciels. Partie 4 : définitions et abréviations. Partie 5 : exemples de méthodes de détermination des niveaux d'intégrité de sécurité. Partie 6 : lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3. Partie 7 : Présentation de techniques de mesures. *Genève, CEI/IEC, Partie 1 : déc. 1998, 115 p. Partie 2 : mai 2000, 143 p. Partie 3 : déc. 1998, 95 p. Partie 4 : nov. 1998, 53 p. Partie 5 : nov. 1998, 57 p. Partie 6 : avril 1998, 145 p. Partie 7 : mars 2000, 229 p.*

[6] KNEPPERT M. – Sécurité intégrée. Conception d'un automatisme. *Travail et Sécurité, 1995, 536, pp. 309-315.*

[7] NF EN 292-1 – Sécurité des machines. Notions fondamentales, principes généraux de conception. Partie 1 : terminologie de base. *Paris, AFNOR, déc. 1991, 33 p.*

[8] NF EN 60204-1 – Sécurité des machines. Équipements électriques des machines. Partie 1 : prescriptions générales. *Paris, AFNOR, avril 1998, 99 p.*

[9] Note du ministère de l'Emploi et de la Solidarité. Direction des relations du Travail. Bureau CT5 – Note relative à l'acceptation de certains automates programmables pour gérer des fonctions de sécurité sur machines. *Paris, ministère chargé du Travail, DRT, 1998, 6 p.*

[10] VIGNERON C. – Analyse des automates dédiés à la sécurité. Eléments méthodologiques. *Cahiers de notes documentaires — Hygiène et Sécurité du Travail, 1997, 166, ND 2039, pp. 37-42.*

[11] Dossier – Des automates pour la sécurité. *Travail et Sécurité, déc. 1997, 567, pp. 20-30.*

[12] NF EN 1050 – Sécurité des machines. Principes pour l'appréciation du risque. *Paris, AFNOR, janv. 1997, 28 p.*

[13] CEI 61131-1 – Automates programmables. Partie 1 : Informations générales. *Genève, CEI/IEC, nov. 1992, 63 p.*

[14] Z 61-100 – Traitement de l'information. Vocabulaire international de l'informatique. *Paris, AFNOR, déc. 1980, 373 p (fascicule de documentation).*

Documents Siemens :

■ **Safety Integrated : Manuel d'application pour la sécurité intégrée (The safety program for industries throughout the World).** *Saint-Denis, Siemens - Automation & drives, mars 2000, 197 p.*

■ **SINUMERIK 840D / 810 / FM – NC – Descriptions des fonctions. N° de référence : 6FC5 297 – 0AB80 – 0DP1.** *Saint-Denis, Siemens, août 1997, 289 p.*

■ **SINUMERIK 611 – Manuel de configuration. N° de référence : 6SN1197 – 0AA00 – 0DP2.** *Saint-Denis, Siemens, févr. 1998, 258 p.*

■ **SIMODRIVE – Linear Motors. N° de référence : 6SN1197-0AB70-0BP0.** *Saint-Denis, Siemens, juin 1999, 156 p.*

■