La norme IEC61508 est maintenant connue depuis une dizaine d'années. Critiquée à ses débuts pour sa grande complexité, elle est devenue aujourd'hui un référentiel bien accepté pour développer les applications de sécurité basés sur des systèmes électriques et électroniques, programmables ou pas. L'arrivée de normes filles, sectorielles et faciles à mettre en œuvre, assoit un peu plus le succès de l'IEC 61508.

POUR LA SÉCURITÉ DE PROCESS, TOUT TOURNE AUTOUR DE L'IEC 61508

SOMMAIRE

Emerson

Il y a encore des accidents, parfois mortels. Et il y en aura toujours. Parce que la sécurité coûte cher et que les solutions déployées assument toujours un "risque calculé". Dans ce dossier, nous nous sommes limités à un aspect particulier de la sécurité des process, à savoir la sûreté de fonctionnement des installations de contrôle de process. La solution la plus répandue consiste à prévoir un automate de sécurité chargé de surveiller que le process ne franchisse pas certaines limites (au-delà desquelles il pourrait devenir dangereux) et d'actionner les organes de sécurité lorsqu'un tel danger se présente.
Toute la difficulté est d'estimer le risque que présente le process et d'évaluer la diminution du risque que doit apporter le système instrumenté de sécurité. La norme IEC61508 présente le gros intérêt de formaliser la démarche. Pour être plus facilement mise en œuvre, des normes filles sectorielles ont été imaginées : c'est le cas notamment de l'IEC61511, spécialement pensée pour mettre en œuvre les systèmes instrumentés de sécurité.
Ce dossier aborde différents aspects techniques pour mettre en œuvre cette norme, notamment l'incidence des redondances de l'automate de sécurité. Il aborde également des thèmes plus généraux, concernant notamment la perception par les industriels français des nouvelles normes…

RÉGLEMENTATION

La sécurité fonctionnelle, on commence à y voir plus clair

Avant, il y a quelques décennies, chacun faisait plus ou moins la sécurité qu'il voulait. Puis les lois, les directives et les normes sont arrivées pour rationaliser les approches. Au fil du temps, les choses finissent par se mettre en place, avec une organisation cohérente et commune. L'Ineris a développé une approche globale d'évaluation des fonctions de sécurité des procédés. Dans le prolongement d'une analyse de risque, celle-ci consiste à évaluer les Equipements dits Importants Pour la Sécurité, en tenant compte des conditions d'utilisation et d'installation.

Tout d'abord le contexte. La sécurité des procédés industriels telle qu'elle s'organise aujourd'hui pour les installations classées, prend fortement en compte l'arrêté et la circulaire ministériels du 10 mai 2000 qui transposent en droit français la directive européenne "Seveso II" (96/82/CE). Celle-ci demande aux exploitants des établissements considérés comme les plus dangereux de mettre en place une politique de prévention des accidents majeurs et un Système de Gestion de la Sécurité (SGS). Aujourd'hui, en France, plus de 1 000 sites sont concernés et ont mis en place un SGS. Toujours selon cette directive, chaque Etat se doit de transcrire les exigences de sécurité prescrites. Et de dépasser ce prérequis s'il le souhaite. « *C'est une différence importante avec d'autres directives, comme la directive Atex (94/9/CE) notamment, qui imposent aux Etats de transposer strictement le texte* », souligne Dominique Charpentier, responsable du laboratoire des équipements électriques à l'*Ineris* (*Institut National de l'Environnement Industriel et des Risques*) et délégué scientifique à la direction de la certification. C'est ainsi que l'Etat français a repris tous les éléments de la directive Seveso et a introduit une notion supplémentaire : celle des EIPS, ou Eléments Importants Pour la Sécurité.

doc. Ineris

Dans le prolongement d'une analyse de risque, l'Ineris a développé une méthode d'évaluation des fonctions de sécurité des process.

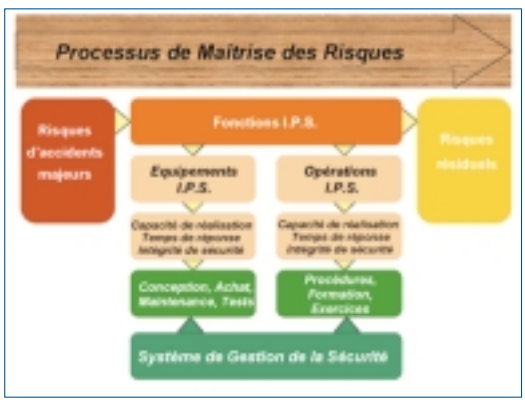
EIPS, une notion française

Cette notion "made in France" vient, à l'origine, du secteur du nucléaire où l'on parle d'EPS, Eléments Pour la Sécurité. Un élément IPS peut être un équipement, un dispositif ou un groupe de dispositifs de protection, ou encore une opération réalisée par un individu. On distingue les éléments matériels passifs (soupapes…), actifs (systèmes instrumentés de sécurité) et les éléments organisationnels (procédures, méthodes, facteurs humains…).

L'arrêté et la circulaire ne définissent pas précisément la notion d'EIPS, laissant à l'exploitant la responsabilité de ses choix. Elle reste ainsi sujette à interprétation. Pour certains, tout dispositif technique ou organisationnel de sécurité est "Important Pour la Sécurité". Pour d'autres, seuls quelques-uns de ces dispositifs doivent être qualifiés d'IPS. « *Il y a eu au départ un peu d'hésitation*, précise M. Charpentier. *Certains industriels ne voulaient en dénombrer aucun, estimant que tous étaient importants. A l'inverse, d'autres les comptaient pas milliers* ». Aujourd'hui, on estime que l'ordre de grandeur doit être de deux à trois cents fonctions IPS au maximum pour les plus gros sites industriels.

Il arrive aussi, par un raccourci de langage, de parler de "paramètre IPS" parce que, souvent, un élément IPS vise à contrôler les dérives dangereuses d'un ou plusieurs paramètres physiques ou chimiques (niveau, pression, température, conductivité, résistance, pH, concentration…). C'est notamment le cas dans les systèmes instrumentés de sécurité (SIS) qui sont constitués au minimum d'un capteur, d'une intelligence (un automate, un calculateur…) et d'un actionneur.

Suite à l'explosion de l'usine AZF en 2001 à Toulouse, la réglementation de la sécurité industrielle s'est encore renforcée. Une loi paraît au Journal Officiel du 30 juillet 2003 relative à la prévention des risques technologiques et naturels. Les chapitres les plus importants de cette loi abordent la maîtrise de l'urbanisation autour des établissements industriels à risques et prévoient la mise en œuvre de ce que l'on nomme aujourd'hui un PPRT, c'est-à-dire un plan de prévention des risques technologiques. Elle introduit également une notion qui ne peut plus échapper aux industriels : la notion d'étude



Le processus de maîtrise des risques permet de passer de risques d'accidents majeurs à des risques dits "résiduels".

de danger probabiliste. L'article 4 du chapitre 2 précise en effet : « *Le demandeur fournit une étude de dangers qui précise les risques auxquels l'installation peut exposer, directement ou indirectement, les intérêts… Cette étude donne lieu à une analyse de risques qui prend en compte la probabilité d'occurrence, la cinétique et la gravité des accidents potentiels selon une méthodologie qu'elle explicite…* ». Cette approche probabiliste rompt avec les pratiques déterministes auxquelles des générations d'ingénieurs ont été habituées. Le calendrier faisant parfois bien les choses, quelques mois après, en décembre 2003, paraît la norme IEC 61511. D'essence probabiliste, comme la norme plus générale sur la sécurité fonctionnelle IEC/EN 61508 dont elle est issue, la 61511 (qui est devenue aussi une norme européenne en avril 2005) se penche sur les systèmes instrumentés de sécurité pour les procédés industriels. Elle peut donc apporter une réponse pour se conformer à la loi du 30 juillet 2003. « *A condition que l'on ait affaire à un site qui s'y prête*, souligne M. Charpentier. Ce n'est pas le cas de *certains procédés, dans le domaine de l'eau ou dans le stockage par exemple, pour lesquels les éléments de sécurité sont en grande majorité organisationnels* ».

Une approche globale

C'est dans ce contexte-là que *l'Ineris* propose aujourd'hui une approche globale pour la mise en place d'un système de gestion de sécurité préconisé par la directive européenne Seveso II, tout en respectant la démarche probabiliste de la loi française du 30 juillet 2003.

Classiquement, l'analyse des risques est au cœur de cette approche. C'est-à-dire qu'elle débute par un gigantesque remue-méninges en groupe qui vise à imaginer tous les scénarios d'accidents possibles, leur probabilité d'occurrence, leur gravité, leur conséquence… Une seconde étape consiste à identifier les barrières de défense qui, si elles sont correctement dimensionnées, minimisent d'une manière significative les risques identifiés. Ainsi, pour chacun des scénarios d'accident majeur, le groupe de travail doit définir les fonctions IPS à assurer. Pour chacune de ces fonctions de sécurité, il dresse la liste des barrières de sécurité pouvant remplir *a priori* la fonction considérée. A ce stade, *l'Ineris* choisit de classer les barrières en fonction de leurs performances pour accomplir la fonction IPS désirée. Dans une première évaluation, *L'Ineris* s'appuie sur des critères simples, établis sous forme d'une grille d'évaluation et qui suffiront pour la majorité des éléments (voir encadré "les bonnes questions").

Quelques bonnes questions

Critères	Exemples de questions à se poser
Indépendance du système de sécurité	Le système considéré est-il dédié à des actions de sécurité ? Est-il indépendant du système de contrôle des installations ? La cause de l'accident peut-elle être à l'origine de la défaillance du système ?
Dimensionnement adapté	Le dimensionnement (capacité de réponse, temps de réponse) est-il adapté aux risques devant être maîtrisés ?
Concept éprouvé	S'agit-il d'un système classique pour lequel un retour d'expérience important est disponible ?
Sécurité positive	Comment le système se comporte-t-il en cas de pertes d'utilité ?
Tolérance à la première défaillance	La défaillance d'un composant peut-elle entraîner la défaillance du système ou des redondances permettent-elles de maintenir la fonction de sécurité
Résistance aux contraintes spécifiques	Le système est-il apte (moyennant des mesures particulières) à travailler dans des conditions particulières (ambiances agressives…) ?
Testabilité	Le système peut-il être testé et à quelle périodicité ? Quelles opérations sont mises en œuvre lors des tests ?
Inspection et maintenance	Le système fait-il l'objet d'inspections et d'opérations de maintenance ? Comment la fonction de sécurité est-elle assurée lorsque le système est indisponible pour cause de maintenance ?

Critères non exhaustifs, inspirés des travaux de l'Union des Industries Chimiques (1999), pouvant servir de base de réflexion pour l'évaluation des performances des barrières de sécurité.

Si cette évaluation "sur papier" ne suffit pas, des études au cas par cas peuvent être entreprises. Les performances des équipements seront alors évaluées à partir de trois principaux critères :

- Leur réalisation. Exemple : vérifier qu'une tour de neutralisation de gaz toxique est suffisante pour limiter grandement les effets associés à une fuite particulière. Dans ce cas, il s'agira de réaliser un calcul de distances d'effets en prenant en compte le taux d'abattage de cette tour.
- Leur temps de réponse. Exemple valider le temps de réponse de débitmètres devant détecter une chute de débit sur une longue canalisation. Il s'agira alors de mener une étude hydraulique en étudiant la décompression dans la canalisation
- Leur intégrité de sécurité à partir d'outils issus de la Sûreté de Fonctionnement. En raison de leur coût, de telles études particulières doivent être réservées à des cas jugés particulièrement critiques.

L'évaluation des différents éléments n'est pas une fin en soi car c'est toute l'architecture globale qui doit prouver son efficacité. « *L'évaluation de l'architecture est de mon point de vue la plus importante, car rien ne sert de mettre un très bon automate de sécurité s'il est connecté à de très mauvais capteurs* », note M. Charpentier. Il est également indispensable de s'assurer de l'adéquation entre les performances et l'utilisation sur site des "Equipements Importants Pour la Sécurité". On ne demandera pas les mêmes

EIPS ou les barrières de défense

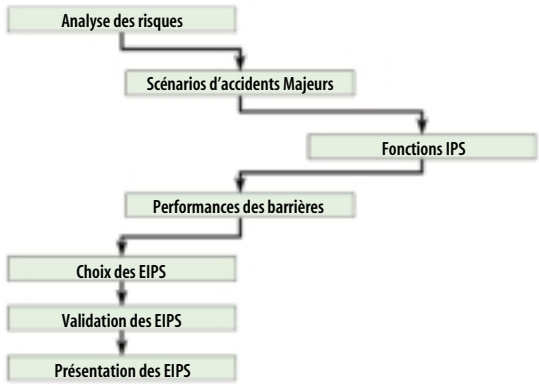
L'exploitant a la responsabilité de choisir ses Eléments Importants Pour la Sécurité (EIPS). Selon l'Ineris, pour être qualifié d'IPS, un élément (opération ou équipement) doit être choisi parmi les barrières de défense destinées à prévenir l'occurrence ou à limiter les conséquences d'un événement redouté susceptible de conduire à un accident majeur. L'institut classe les barrières de sécurité selon leur fonction (prévention, protection ou intervention) et leur type active ou passive.

Une barrière active nécessite une source d'énergie ou une sollicitation automatique ou manuelle (exemples : barrière infrarouge, actionneur). A l'inverse, une barrière passive n'a pas besoin d'énergie ni de sollicitation (exemple : soupape). Une barrière de prévention permet de prévenir un événement redouté. Elle peut aussi assurer une surveillance d'un paramètre (exemple : les systèmes de sécurité instrumentés) qui, en cas de dérive, peut entraîner la perte de contrôle de l'installation. Enfin, une barrière de protection permet de limiter les conséquences d'un événement redouté afin d'en limiter les conséquences (exemples : le confinement d'un produit dans un bâtiment, un réservoir).

Guide pratique d'application de la norme CEI/EN 61511

L'*Exera* vient de publier un guide pratique destiné à toute personne chargée de la conception, de l'utilisation et de la maintenance de systèmes instrumentés de sécurité. Il s'agit d'un mode opératoire de la norme CEI/EN 61511. Il est construit à partir d'une étude de cas basée sur une installation d'un méthaneur qui sert de fil conducteur tout au long du document. Ce guide a été rédigé par Ahmed Adjadj et Dominique Charpentier, de la direction de certification de l'*Ineris*. (Rens. exera@wanadoo.fr)

Identification des EIPS dans les études de dangers



La détermination des EIPS (éléments importants pour la sécurité) se fonde principalement sur l'analyse des risques qui permet d'envisager les scénarios d'accidents majeurs.

caractéristiques pour une sonde plongée dans l'eau ou dans un hydrocarbure. De même, le taux de défaillance d'une soupape sur une unité de vapeur n'est pas le même que celui de la même soupape installée sur une conduite de fluides sales. Ce travail de terrain se fait forcement en collaboration avec l'industriel. Plus ce dernier aura un retour d'expérience, plus il pourra affiner son analyse de risque. « *C'est ce qui nous manque parfois le plus, le manque d'historique sur le site ou sur des sites équivalents* », relève M. Charpentier. Autre difficulté, les données d'entrée des matériels. Le taux de défaillance donné par les fournisseurs est théorique, il ne prend pas en compte l'usage. De plus, une indication par exemple sur le MTBF (*Mean Time between Failure*) n'apporte pas d'information sur la nature des dysfonctionnements (est-ce une led qui ne clignote plus ou l'équipement tout entier qui s'arrête de fonctionner?). Et rien ne dit si ces dysfonctionnements peuvent porter atteinte ou non à la fonction sécurité de l'équipement.

Du SIL de partout

On les retrouve dans toutes les normes qui sont élaborées à partir de la CEI/EN 61508, à savoir la EN 61511 pour les procédés industriels, la EN 61513 pour le nucléaire, les normes EN 50128/50129 pour le secteur ferroviaire ou encore la EN 62061 pour les machines. Par définition, quand on monte d'un niveau (en passant d'un SIL1 à un SIL2, ou d'un SIL2 à un SIL3), la probabilité de défaillance d'un équipement est réduite d'un facteur 10 « *La définition des SIL permet d'avoir un langage commun*, souligne M. Charpentier. *Aujourd'hui, quand on parle "SIL", tout le monde de la sécurité connaît* ». Le concept SIL constitue un référentiel de conception des équipements de sécurité, qui deviendra d'application obligatoire dans certains domaines. Par exemple, le projet de norme (pr EN 50402) pour les détecteurs de gaz pour atmosphère explosible reprend cette notion de SIL ; lorsque cette norme fera partie des normes harmonisées de la directive Atex, la majorité des constructeurs de détecteurs de gaz l'appliquera.

Une évaluation probabiliste des EIPS

C'est la raison pour laquelle la Direction de la Certification de *l'Ineris* a mené un programme de recherche sur les méthodes d'évaluation et les essais associés. Aujourd'hui, à l'instar des TüV en Allemagne qui en furent les initiateurs, il est en mesure de certifier des équipements en terme de sûreté de fonctionnement. Conforme à une approche probabiliste, *l'Ineris* s'appuie là encore sur la norme de la sécurité fonctionnelle CEI/EN 61508. Elle détermine ainsi pour l'équipement un niveau de confiance, équivalent aux niveaux de sécurité SIL (*Security Integrity Level*) définis dans la norme CEI/EN 61508. *L'Ineris* s'attache uniquement à la certification de matériels électriques, mais aux matériels mécaniques et encore moins aux éléments non matériels (procédures). « *La norme CEI/EN 61508 a été écrite par des électroniciens*, remarque M. Charpentier, *et elle est plus difficile à mettre en œuvre pour des éléments non électriques* ». On peut aussi lui reprocher un manque de précision : pour un SIL donné, la probabilité de défaillance sur sollicitation peut varier d'un facteur 10. Le type de défaillance à considérer mériterait d'être mieux précisé. « *Il faut toujours associer une probabilité de défaillance ou pour être plus exact, une probabilité de défaillance dangereuse qu'on n'arrive pas à détecter. Car les défaillances non dangereuses, ou les défaillances dangereuses facilement détectables, ne sont pas en soi un risque pour la sécurité* ».

Mais attention, dans ce cadre-là, l'évaluation d'un équipement porte uniquement sur ses fonctions de sécurité. « *On raisonne sécurité et non disponibilité* ». Ainsi, pour un variateur de vitesse l'évaluation portera sur sa fonction "arrêt d'urgence". Il en est de même pour un détecteur de gaz où l'on examinera le déclenchement d'alarme en cas de défaut et non le déclenchement intempestif de l'alarme. Le niveau requis est, quant à lui, défini dès le début au niveau de l'analyse de risque.

« *Nous avons déjà certifié des équipements pour des fournisseurs français. A la demande de Schneider Electric, nous avons évalué des équipements ayant des fonctions de sécurité* ». Mais pour *l'Ineris*, la certification d'un équipement ne peut suffire si l'on ne prend pas en compte son environnement d'utilisation. A cette fin, il a inclus dans son référentiel d'évaluation la délivrance d'un avis technique. Celui-ci prend en compte les conditions d'installation et d'utilisation de l'équipement qu'il énonce sous la forme de recommandations ou de prescriptions.

La mission de *l'Ineris* s'arrête ainsi à la qualification des systèmes dans leur environnement industriel. Même s'il préconise une périodicité de maintenance et quelques précautions d'usage, il ne s'engage en rien sur l'évolution dans le temps des systèmes de sécurité.

Marie-Pierre Vivarat-Perrin

NORMES

L'IEC 61508 s'impose, sa famille aussi…

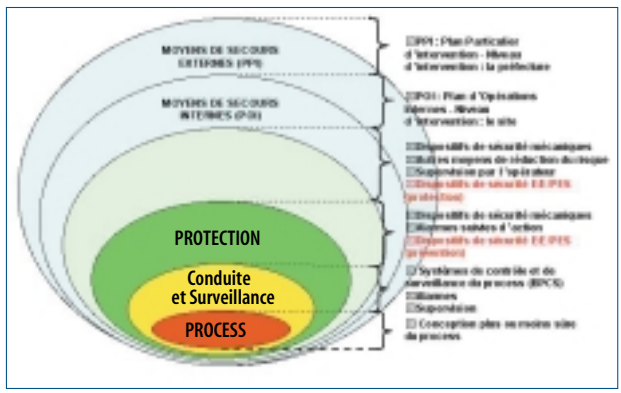
Il est devenu difficile de tenir une conversation sur la sécurité sans faire référence à l'IEC 61508. Cette norme qui a pratiquement dix ans et qui est devenue une norme française en 1999, constitue un véritable guide méthodologique pour concevoir et mettre en œuvre un système de sécurité électronique ou électrique, semble s'imposer. Pour faciliter sa mise en œuvre, des normes sectorielles ont été développées, notamment la 61511 pour les systèmes instrumentés de sécurité pour process industriels.

La principale vocation de la sécurité est d'éliminer les risques inacceptables qui pourraient être responsable de blessures physiques, d'atteindre la santé des personnes ou dégrader l'environnement. Pour assurer cette sécurité, il faut d'abord avoir une bonne organisation. Chacun peut utiliser ses propres approches. Un effort de standardisation avait été fait avec la norme Iso 18000 mais celle-ci n'a jamais réellement vu le jour car les différents organismes nationaux participant à l'élaboration de cette norme internationale n'ont pu se mettre d'accord. Ceci a permis à d'autres référentiels de s'imposer : c'est l e cas de l'OSHAS 18000.

La sécurité, ce n'est évidemment pas que de l'organisation. C'est aussi des méthodologies à suivre, des moyens techniques à déployer. Et pour cela, une norme s'est imposée à l'échelon international : l'IEC 61508. Il s'agit d'une norme orientée "performances", c'est-à-dire qu'elle laisse à l'utilisateur le soin de réaliser son analyse du risque et elle lui propose des moyens pour réduire ce risque. Elle porte plus particulièrement sur le système E/E/PE (Electrical/Electronic/Programmable Electronic Safety-related systems), c'est-à-dire les systèmes électroniques et électriques de sécurité. En principe, elle ne concerne pas les systèmes simples, pour lesquels le mode de défaillance de chaque élément est clairement défini et pour lesquels le comportement du système peut être totalement déterminé dans le cas d'une défaillance. Par exemple, un système comportant des fins de course et des relais électromécaniques reliés à un disjoncteur peut être étudié sans avoir recours à l'IEC 61508.

Cette norme comprend 7 parties, afin de couvrir les multiples aspects des systèmes E/E/PE :

- 61508-1 : Prescriptions générales
- 61508-2 : Prescriptions propres aux systèmes E/E/PE
- 61508-3 : Prescriptions relatives au logiciel
- 61508-4 : Définitions et abréviations
- 61508-5 : Exemples de méthodes pour déterminer le niveau d'intégrité de la sécurité
- 61508-6 : Guides pour l'application des parties 2 et 3 de la norme
- 61508-7 : Tour d'horizon des techniques et des mesures



Les systèmes instrumentés de sécurité (SIS) ne constituent qu'un tout petit élément du vaste problème de la sécurité.

La norme propose une approche opérationnelle pour mettre en place un système de sécurité E/E/PE, en partant de l'étude des exigences de sécurité (avec une définition du périmètre couvert, une analyse et une évaluation du risque) et en prenant en compte toutes les étapes du cycle de vie du système E/E/PE. Un des intérêts de cette norme est d'être générique et donc d'être applicable dans tous les secteurs où la sécurité peut être traitée avec des systèmes E/E/PE : industries manufacturières, industries des process continus, pharmaceutiques, nucléaire, ferroviaire, etc. Malgré tout, peut-on lire dans un document édité par *ISA France* et le *Club Automation* (téléchargeable sur Internet), "le déploiement de l'IEC 61508 et de ses normes filles se heurte à des difficultés diverses. La disparité des institutions réglementant la sécurité des installations, les intérêts contradictoires des acteurs industriels, les aspects juridiques et le manque de formation sont autant d'obstacles à une diffusion large de ces normes dont la mise en œuvre n'est déjà plus un choix". Ailleurs, dans le même document, on relève en guise d'explication que l'approche proposée est inhabituelle pour les utilisateurs français, généralement confrontés à des normes déterministes définissant des architectures et des prescriptions techniques très strictes. L'IEC 61508 leur laisse au contraire beaucoup d'initiative.

Deux paramètres essentiels : le PFD et le PFH

L'IEC 61508 traite de la sécurité fonctionnelle, qui a un champ d'application plus réduit que celui de la sécurité globale car elle ne s'intéresse qu'aux systèmes E/E/PE. Un système de déclenchement pour mettre un process chimique dans une situation non dangereuse, un arrêt d'urgence sur une machine constituent des exemples de systèmes E/E/PE. Pour spécifier de tels systèmes, il faut commencer par faire une analyse approfondie des phénomènes dangereux et voir comment on va s'y prendre pour amener le risque à un niveau acceptable.

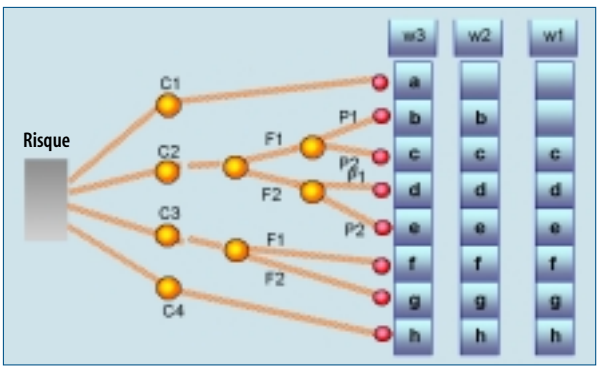
Le système instrumenté de sécurité constitue un des moyens pour réduire ce risque. Pour définir le niveau de réduction du risque,

l'IEC 61508 a défini le SIL (Security Integrity Level), c'est-à-dire le niveau d'intégrité de la sécurité que doit avoir le système de protection. Plus le SIL a une valeur élevée, plus la réduction du risque est importante. Par exemple, un système de sécurité SIL4 apporte une réduction de risque comprise entre 10 à 100 000 alors que pour un système SIL1, cette réduction est comprise entre 10 à 100 seulement.

La norme IEC s'applique aussi bien aux systèmes de sécurité qui fonctionnent sur sollicitation (lorsqu'une défaillance apparaît) que ceux qui travaillent en permanence pour maintenir un process dans un état non dangereux. Le premier cas (système sur sollicitation) peut être illustré par un système d'arrêt d'urgence qui va commander l'ouverture d'une vanne de sécurité si la pression dans un ballon devient trop élevée.

Estimation du risque

Risque = C x F x P x W	
Conséquences du risque (C)	
C1	Mineures
C2	Blessures d'une ou plusieurs personnes, décès d'une personne
C3	Décès de plusieurs personnes
C4	Décès de très nombreuses personnes
Fréquence d'exposition (F)	
F1	Rare à assez souvent
F2	Fréquent à permanent
Possibilité d'éviter l'événement (P)	
P1	Possible sous certaines conditions
P2	Pratiquement impossible
Probabilité d'événement indésiré (W)	
W1	Très faible
W2	Faible
W3	Relativement élevé



Niveau de sécurité à atteindre	Niveau d'intégrité de la sécurité
a	néant
b, c	SIL1
d	SIL2
e, f	SIL3
g	SIL4
h	Protection par SIS impossible

Doc. Hima

Le deuxième cas (fonctionnement permanent) peut être illustré par le contrôle de la vitesse d'une machine à papier, qui doit être maintenu à une vitesse très lente pendant que les opérateurs sont en train de réaliser une opération de maintenance. Pour définir ces deux cas, le SIL est spécifié de deux façons : PFD (Probability of Failure on Demand) et PFH (Probability of dangerous Failure per Hour).

Dans la conception d'un système E/E/PE de sécurité, le défi est d'éviter les pannes dangereuses ou de les contrôler si elles surviennent. Les causes de ces pannes sont très nombreuses : erreurs sur les spécifications (avec des oublis, par exemple), pannes matérielles (systématiques ou aléatoires), erreurs sur les logiciels, erreurs de mode commun, influence de l'environnement (électromagnétique, température, vibrations), perturbations de l'alimentation électrique. Tous ces éléments doivent être pris en compte pour calculer le PFD ou le PFH du système. Ces calculs reposent sur des analyses mathématiques probabilistes.

Dans le calcul du PFD (ou du PFH), de nombreux éléments interviennent, notamment le taux de défaillance. Le PFD se dégrade avec le temps et le rôle de l'intervalle de test est de définir la durée pendant laquelle le PFD restera dans les limites annoncées, par exemple entre 10^{-3} et 10^{-4} (correspondant à SIL3). Si l'intervalle de test est de 3 ans et qu'on n'effectue pas de test, au-delà de 3 ans, le dispositif ne peut plus être garanti SIL3.

SIL pour les composants individuels ?

Normalement, l'IEC 61508 s'applique à l'ensemble du système E/E/PE de sécurité, c'est-à-dire à la boucle complète, avec le capteur, l'automate et la vanne. Le SIL concerne donc le système dans son ensemble, pas les éléments qui le composent. Cela n'a pas empêché les fabricants de produits entrant dans la conception de ces systèmes d'attribuer un SIL à leurs produits. Cela n'a pas de sens à proprement parler mais ça peut permettre de faciliter la sélection des éléments de sécurité. Pour preuve, les groupes de travail de la *CEI* qui ont œuvré pour la 61508 travaillent en ce moment sur une norme "produit" relative aux variateurs de vitesse. En prenant tout de même quelques précautions au niveau du vocabulaire, du genre "variateur avec une capacité SIL2", ou "variateur apte à être utilisé dans une fonction SIL3". Une précision qui a son importance parce que l'IEC 61508 exige uniquement qu'une valeur de PFH/PFD soit spécifiée

pour chaque fonction de sécurité. Le fabricant d'un élément de sécurité ne peut s'engager que sur la fraction de la valeur globale du PFH/PFD pour laquelle l'élément est prévu. Par exemple, s'il annonce un PFH de 0,0008, son produit entre dans la catégorie SIL3 mais il ne couvre pas toute cette catégorie (pour laquelle le PFH est compris entre 0,0001 et 0,001).

Un document rédigé par un technicien de *Vega* portait le titre "IEC 61508 and 61511 means 2 + 2 = 3 and 2 + 2 = 1". Ce titre veut dire que lorsque l'on a plusieurs éléments de sécurité avec chacun un SIL donné, le niveau d'intégrité de sécurité résultant n'est pas obtenu par une addition des différents SIL.

La première équation "2 + 2 = 3" signifie que si on met deux éléments SIL2 en redondance, l'ensemble peut atteindre SIL3 (à condition que la redondance soit bien faite). Quant à la deuxième équation ("2 + 2 = 1"), elle signifie que la mise en série de deux éléments de sécurité SIL2 peut donner un niveau global SIL1.

Voyons cela plus précisément. Lorsqu'un système comporte plusieurs éléments, et c'est le cas de tous les systèmes instrumentés de sécurité, le PFD de l'ensemble est obtenu en additionnant les PFD des différents éléments. Par exemple, pour un système comportant un capteur, un automate et une vanne, on aura :

$PFD_{SIS} = PFD_{capteur} + PFD_{automate} + PFD_{vanne}$

Si on utilise un capteur donné avec un PFD de 0,005 (SIL2), un automate avec un PFD de 0,0005 (SIL3) et une vanne avec un PFD de 0,05 (SIL1), on obtient un PFD_{SIS} égal à 0,0555, ce qui correspond à SIL1. C'est le maillon le plus faible de la boucle qui a le plus d'incidence sur la valeur du SIL.

Dans le même ordre d'idée, si tous les éléments de la boucle ont le même niveau SIL, ce n'est pas pour autant que l'ensemble de la boucle a le même niveau de SIL. Prenons le cas d'un capteur avec un PFD de 0,006 (SIL2), un automate avec un PFD de 0,0015 (SIL2) et une vanne avec un PFD de 0,008 (SIL2), l'addition des trois donne un PDF de 0,0155,ce qui correspond à un SIL1…

Des normes filles ciblées

De l'avis général, l'IEC 61508 est assez complexe à appréhender parce que très générale. C'est pour cela que ses concepteurs ont développé des normes filles s'appliquant à des secteurs bien précis. En voici quelques-unes :

- 61511 : process industriels
- 62061 : machines
- 61513 : nucléaire
- 50126/8/9 : ferroviaire

Dans ces normes sectorielles, une distinction est faite entre l'application du système E/E/PE de sécurité (qui dépend du secteur) et les spécifications détaillées de conception (qui sont indépendantes du secteur). Les spécifications indépendantes du secteur font référence à des parties et paragraphes de l'IEC 61508 et évitent les répétitions. Les utilisateurs qui veulent mettre en œuvre une norme sectorielle ont donc besoin de l'IEC 61508. Du coup, le message que font passer certains professionnels selon lequel l'IEC 61508 concerne les constructeurs et les normes sectorielles les utilisateurs est sans doute un peu réducteur. D'autant que l'IEC 61508 concerne normalement la chaîne complète, pas les produits…

Les directives européennes pourraient servir de tremplin pour certaines directives européennes. Chacun sait en effet que la sécurité est au cœur de nombreuses, si ce n'est de la plupart, des directives européennes. Pour faciliter leur mise en pratique, les directives comportent en général une liste de normes dites "harmonisées" : si ces normes sont correctement appliquées, le produit concerné bénéficie d'une présomption de conformité. Si l'industriel utilise des normes autres que les normes harmonisées, il est libre de le faire mais il faut alors qu'il démontre que ses choix permettent de répondre aux prescriptions de la directive.

La directive Seveso II modifiée (2003/105/CE) est a priori celle qui est la mieux concernée par les normes IEC 61508 et 61511. Toutes deux couvrent en effet le domaine des process continus. La seule réserve est que les industries impliquées ont déjà une culture de la sécurité et qu'elles ont leurs propres normes. D'autre part, cette directive porte surtout sur l'organisation de la sécurité et n'est pas prescriptive sur le plan technique.

La directive "Machines" met en œuvre des systèmes électroniques de sécurité et elle est prescriptive. Les normes IEC 61508 sont donc applicables. Mais dans cet univers très disparate (il y a beaucoup de types de machines), il existe de nombreuses normes harmonisées sectorielles. Dans la note d'application de cette norme rédigée par l'ISA et le *Club Automation*, on peut lire : "La norme IEC 62061 a été rédigée dans l'objectif de devenir une norme européenne harmonisée pour la directive machines. Ceci a été rendu possible en réduisant le périmètre de l'IEC 61508 pour n'inclure que des exigences concernant des produits. Il faut toutefois noter que bien que cela fournira une présomption de conformité à certaines exigences essentielles de la directive machine, cela n'empêchera pas d'utiliser d'autres moyens (d'autres normes) pour remplir ces exigences.

"La commission européenne reconnaît implicitement que l'EN 954-1 (Iso 13489) est notoirement insuffisante dès que les chaînes de sécurité des machines contiennent des automatismes programmés. Elle recommande (sans encore l'imposer) d'appliquer l'IEC 62061".

Par ailleurs, un groupe de travail de la CEI prépare actuellement une nouvelle norme sur la sécurité fonctionnelle des variateurs de vitesse concernés par la sécurité. Il s'agit de l'IEC 61800-5-2 qui portera sur les composants, prenant en compte le fait que dans de nombreux cas, le variateur de vitesse est un composant d'une installation concernée par la sécurité.

Cet article s'appuie sur de nombreux articles publiés sur le site Internet ww.safetyusersgroup.com, très complet (mais la plupart des articles sont en anglais). De nombreux éléments ont également été puisés dans le document très pratique (et en français) rédigé par Bertrand Ricque et Jean Vieille portant le titre "Guide d'interprétation et d'application de la norme IEC 61508 et des normes dérivées" qui est téléchargeable gratuitement. Citons enfin le document "Vers une sécurité accrue de vos équipements et installation" publié par le Gimelec sur www.eleclive.com.

JFP

Échelle des niveaux SIL

	Sollicitations du SIS		
SIL*	rares PFD**	fréquentes PFH***	Facteur de réduction du risque
4	$\geq 10^{-5}$ à $< 10^{-4}$	$\geq 10^{-9}$ à $< 10^{-8}$	10 000 à 100 000
3	$\geq 10^{-4}$ à $< 10^{-3}$	$\geq 10^{-8}$ à $< 10^{-7}$	1 000 à 10 000
2	$\geq 10^{-3}$ à $< 10^{-2}$	$\geq 10^{-7}$ à $< 10^{-6}$	100 à 1 000
1	$\geq 10^{-2}$ à $< 10^{-1}$	$\geq 10^{-6}$ à $< 10^{-5}$	10 à 100

** Safety Integrity level, niveau d'intégrité de la sécurité*

***Probability of Failure on low Demand, probabilité d'avoir une défaillance (pour réaliser la fonction de sécurité prévue) au moment d'une sollicitation*

****Probability of a dangerous Failure per Hour ou Probability of Failure on High demand, probabilité d'une défaillance dangereuse par heure*

MISE EN ŒUVRE DE L'IEC 61508

Dans la sécurité, ce qui compte avant tout, c'est la démarche…

Bureau Veritas est impliqué de longue date dans les applications de sécurité et a été un des premiers à soutenir la norme IEC 61508. La société insiste ici sur l'importance de la démarche et invite chacun à ne pas se laisser obnubiler par les SIL qui sont distribués parfois un peu trop à la légère. Elle déplore aussi que les Français soient aussi timorés dans l'application des nouvelles normes…

Mesures. Pouvez-vous résumer très brièvement l'activité du *Bureau Veritas*.

Michel Suzan. Pas simple, pour un groupe qui emploie aujourd'hui plus de 20000 personnes, est présent dans 140 pays et a plus de 200000 clients. Pour résumer, disons que le groupe assure des activités de certification de systèmes de management (qualité sécurité, santé, environnement), d'attestation de conformité, de formation et enfin de conseil et assistance technique.

Michel Suzan, Responsable "Equipements et Procédés industriels" à Bureau Veritas.

Ces différentes activités sont relativement cloisonnées. C'est ainsi qu'il y a une totale indépendance entre les prestations de vérification de conformité réglementaire d'une part, et de conseil et assistance technique d'autre part. Ces deux prestations sont assurées par des équipes différentes. Il est exclu que l'équipe spécialisée dans le conseil prolonge sa prestation par de la vérification de conformité.

Mesures. Cela semble pourtant s'inscrire dans une certaine logique. Vous montreriez à vos clients que les conseils que vous leur donnez ne sont pas "gratuits", et qu'en les mettant en pratique pour aboutir à une vérification de conformité, vous prendriez vos responsabilités…

Michel Suzan. Peut-être mais la question ne se pose pas : les autorités administratives, et notamment le *Cofrac*, qui nous ont mandatés pour délivrer des attestations de conformité imposent de ne pas mélanger les genres. C'est aussi une règle d'éthique et de bon sens. Notre indépendance, une de nos valeurs fondamentales, en dépend.

J'ajouterai que nos différentes prestations ne sont pas seulement assurées par des équipes différentes, elles peuvent être assurées par des sociétés différentes à l'intérieur du groupe. Par exemple, la certification des systèmes de management est assurée par BVQI, et non par *Bureau Veritas*. Par contre, c'est *Bureau Veritas* qui délivrera l'attestation de conformité d'une boucle de sécurité,

J'ajouterai que dans le groupe, nous avons aussi une activité de certification des produits électriques et électroniques : celle-ci est assurée par le LCIE. Ainsi, l'attestation de conformité et la certification de la sécurité fonctionnelle de produits sont désormais confiées au LCIE.

Mesures. Venons-en aux activités dans le domaine de la sécurité. Vous êtes depuis la première heure un ardent défenseur de l'IEC 61508 et de ses dérivées. On voit de plus en plus de conférences sur le sujet. Cette reconnaissance est plutôt bon signe, non?

Michel Suzan. C'est vrai que beaucoup nous ont emboîté le pas, ce qui montre bien que cette norme, malgré les critiques dont elle a été l'objet à un moment (on lui prêtait une certaine complexité), est en train de faire l'unanimité auprès des professionnels. Certains s'y sont ralliés un peu à la manière des "ouvriers de la 25ème heure". A *Bureau Veritas*, nous nous y sommes intéressés dès sa genèse. Soutenue au départ par *Bureau Veritas Consulting*, son utilisation a été étendue aujourd'hui à l'ensemble du groupe. Elle constitue pour nous un véritable référentiel pour traiter les problèmes de sécurité.

Et puis il y a eu des avancées importantes faites autour de l'IEC 61508, notamment au niveau de sa mise en pratique. Pour rendre les choses plus simples, l'IEC 61508 a été déclinée pour répondre à des besoins particuliers : la 61511 pour les systèmes instrumentés de sécurité, la 61512 pour les procédés batch, la 62061 pour la sécurité des machines, la 61513 pour le nucléaire, les EN 50128 et EN 50129 pour le ferroviaire. D'autres sont en préparation.

Un autre élément est venu renforcer sa crédibilité : c'est la loi du 30 juillet 2003 sur les risques technologiques et naturels majeurs, dite "loi Bachelot", qui introduit la notion de probabilités dans l'évaluation des risques, ce qui ne peut qu'apporter de l'eau au moulin de l'IEC 61508, qui est d'essence probabiliste. Ceux qui ne juraient que par l'approche déterministe pour traiter les problèmes de sécurité ont dû réviser leur jugement.

Patrick Teixeira. Cette loi impose de faire la preuve de la diminution de la probabilité de risque, ce qui n'était pas le cas auparavant. La loi n'impose pas en tant que tel de quantifier cette probabilité mais de mettre

en place un indicateur d'évolution de la probabilité du risque.

Mesures. Comment se concrétise sur le terrain toute cette effervescence autour de l'IEC 61508?

Michel Suzan. Au niveau des acteurs de la sécurité, ainsi que je l'ai dit, l'IEC 61508 est devenue un standard. Depuis qu'elle a reçu l'onction officielle, cette norme sert d'argument marketing pour les constructeurs d'automates ou de capteurs destinés aux applications de sécurité. Voyez les catalogues des constructeurs, vous verrez que des capteurs ou des automates qui avaient déjà une longue carrière sont désormais attifés d'un niveau SIL (le paramètre de base de l'IEC 61508) et, dans certains cas, proposés à un prix plus élevé…

Patrick Teixeira. En matière de produits destinés aux applications de sécurité, il y a une certaine confusion. Certains produits sont dûment certifiés, d'autres ne le sont pas. De plus, il y a aussi une grande disparité entre les approches des organismes de certification des produits, chacun a son propre référentiel.

Mesures. Pour l'instant, vous ne délivrez pas de certification, vous n'êtes donc pas concerné…

Patrick Teixeira. En France, on ne s'improvise pas organisme de certification de produits. Avec le *LCIE*, *Bureau Veritas* dispose d'une bonne base. Mais pour l'instant, nous ne sommes pas entrés dans ce domaine.

Ce que nous faisons, c'est délivrer des attestations de conformité, c'est-à-dire que nous prenons la responsabilité d'affirmer qu'un produit a été conçu en étant conforme à un référentiel (l'IEC 61508, par exemple) et nous fournissons les éléments permettant de le justifier.

Mesures. Revenons à l'application de la norme IEC 61508, de plus en plus prisée par les constructeurs de matériels. Est-ce que sur les sites industriels, les choses avancent?

Michel Suzan. Vous avez parlé il y a un instant de l'effervescence autour de la norme. C'est vrai mais il faut tout de même voir qu'elle trahit une réalité peu glorieuse : elle donne à penser que tout est nouveau alors qu'en fait beaucoup de choses existent depuis des années. En fait, on a perdu beaucoup de temps et aujourd'hui encore, le marché n'a toujours pas réellement décollé, la 61508 et la 61511 sont encore peu appliquées en milieu industriel. Avec l'arrivée massive de matériels (capteurs, automates, vannes, etc.) conformes à l'IEC 61508, on peut penser que les choses vont s'accélérer…

Mais attention tout de même de ne pas traiter les problèmes de sécurité par le petit bout de la lorgnette. Réaliser une fonction de sécurité, ce n'est pas utiliser tel ou tel équipement conforme aux normes. C'est beaucoup plus que cela, c'est adopter une démarche. Il faut partir de la notion de sécurité fonctionnelle, évaluer le risque, choisir des moyens pour chercher à le réduire, vérifier que dans le temps le risque résiduel est maîtrisé. Et cette démarche que nous préconisons est loin d'être une pratique courante sur les sites industriels. De plus, les difficultés financières que connaissent bien des entreprises n'arrangent pas les choses.

Patrick Teixeira. Le plus difficile dans tout cela, c'est l'analyse du risque et elle est souvent mal faite.

Mesures. Pourtant, les Drire, qui sont chargées de donner l'autorisation d'exploiter les installations, doivent vérifier tout cela…

Patrick Teixeira. Oui mais leur rôle n'est pas facile. Les industriels qui exploitent des usines dangereuses ne sont pas fous, ils tiennent à ce qu'elles fonctionnent correctement. Et ceci d'autant qu'ils sont légalement responsables de tout accident qui pourrait arriver et de ses conséquences. Les industriels en question mettent en œuvre des stratégies de sécurité, avec leurs propres recettes, souvent rodées par des décennies de pratique. Et ils arrivent en général à de très bons résultats. Les Drire examinent le dossier et donnent leur feu vert d'exploitation.

Cela dit, maintenant qu'il existe des référentiels, les choses devraient changer. Les industriels ont tout intérêt à les appliquer, ne serait-ce que pour pouvoir prouver, en cas d'accident, qu'ils avaient suivi une démarche rigoureuse. Les Drire, qui connaissent bien entendu ces référentiels, deviennent quant à elles beaucoup plus exigeantes.

Mesures. Quel est précisément votre rôle?

Michel Suzan. Notre principal rôle, c'est vraiment de sensibiliser les industriels à bien appréhender le risque. Cela fait, il est relativement simple de se fixer un objectif à atteindre et des solutions techniques à mettre en œuvre. *Bureau Veritas* apporte un réel savoir-faire dans tous ces domaines. Les industriels ont parfois tendance à sous-dimensionner le risque, car ils savent que plus le risque est élevé, plus les solutions à mettre en œuvre seront coûteuses et plus il y aura des contraintes au niveau de l'organisation et du comportement des personnes. Alors qu'il y a quelques années, ils faisaient un peu l'inverse, il leur arrivait de faire de la sur-sécurité. La crise que l'on connaît a fait évoluer les comportements…

Nous sommes neutres, nous les sensibilisons à l'importance de la démarche, les aidons à se poser les bonnes questions.

Mesures. Revenons à l'IEC 61508. Outre sa complexité, certains lui ont reproché de laisser trop de place aux interprétations…

Michel Suzan. Je ne comprends pas ce reproche. Pratiquement toutes les normes ont une marge pour l'interprétation. Et c'est le rôle des spécialistes d'apporter leur

Patrick Teixeira, responsable des activités "Sûreté de fonctionnement et mise en conformité CE des machines" à Bureau Veritas.

propre interprétation pour atteindre l'objectif de sécurité. *Bureau Veritas*, en proposant son interprétation, apporte une réelle valeur ajoutée.

Mesures. Parmi ces interprétations, certains disent que l'IEC 61508 s'applique aux constructeurs et l'IEC 61511 aux intégrateurs. Etes-vous d'accord?

Michel Suzan. Que l'IEC 61511 est destinée aux intégrateurs et aux utilisateurs, c'est une certitude. Pour l'IEC 61508, on ne peut avoir un avis aussi tranché parce qu'il s'agit d'une norme générique, applicable par tous. Mais, ainsi que vous l'avez souligné, elle est difficile à mettre en œuvre. Du coup, de fait, ce sont surtout les constructeurs de matériels qui l'appliquent…

Mesures. La notion de SIL (Safety Integrity Level, niveau d'intégrité de la sécurité) fait également débat. Normalement, elle s'applique à un système complet (capteur, contrôleur, vanne). Certains attribuent pourtant un Sil à chacun des éléments du système…

Patrick Teixeira. Le niveau Sil s'applique en effet à la boucle complète. Mais dans une installation, il y a par exemple des vannes manuelles qui contribuent à la réduction du risque, au même titre qu'un système instrumenté de sécurité. Il n'y a donc pas d'hérésie à lui attribuer un niveau SIL, en tant qu'objectif de fiabilité (car la norme et les SIL tels qu'ils y sont définis, ne s'applique qu'aux systèmes électriques, électroniques et électroniques programmables). L'IEC 61508 aborde d'ailleurs la notion d'éléments de sécurité, avec un niveau SIL pour chacun d'eux. Il peut être pertinent d'affecter un SIL à un sous-ensemble. Là-dessus, les fabricants de capteurs se sont engouffrés dans la brèche et attribuent des SIL à leurs produits, sans préciser dans quelles conditions ils sont obtenus ni ce qu'il faut faire pour les maintenir dans le temps. Là, il faut être très prudent…

Michel Suzan. Prenez l'exemple d'un capteur de vitesse. Selon qu'il est utilisé sur un compresseur, une turbine à vapeur ou une pompe, les conditions d'utilisation seront radicalement différentes, les constantes de temps seront différentes. Il est difficile dans ce cas-là de dire si le niveau SIL annoncé sera tenu dans les différentes situations. Nous ne sommes pas pour autant des intégristes de l'IEC 61508. Disposer d'un niveau SIL pour un capteur, c'est mieux que rien : il faudrait simplement que les constructeurs précisent les conditions dans lesquelles il a été obtenu et son champ précis d'applications. De ce côté-là, il reste du travail à faire. Mais il faut bien reconnaître que l'affectation de SIL aux différents éléments d'un système est pour beaucoup dans l'attrait du standard…

Patrick Teixeira. Lorsque *Bureau Veritas* délivre une attestation de conformité pour un sous-ensemble, avec un SIL donné, les hypothèses faites pour arriver au résultat sont clairement explicitées. Les conditions à remplir pour que ce niveau SIL soit maintenu dans le temps (le type et la fréquence des autotests) sont également très clairement mentionnées. Ce faisant, l'intégrateur qui utilise un tel sous-ensemble a beaucoup moins de questions à se poser. Mais cette approche n'est malheureusement pas adoptée par tout le monde et nous voyons beaucoup de cas où des SIL sont attribués sans autre précision et il est nécessaire de faire des études complémentaires…

Cette réflexion est valable aussi bien pour les SIL obtenus grâce à une solide étude théorique (en utilisant des techniques de sûreté de fonctionnement, arbres de défaillances, les diagrammes de Markov et autres) que ceux attribués "par expérience" (pour attribuer un SIL, la norme, avec la notion de "proven in use", donne la possibilité d'exploiter les données obtenues en exploitation).

Mesures. Y-a-t-il un moyen de vérifier la validité du SIL obtenu?

Michel Suzan. Certains disent "Nous avons fait des millions de test sur ce produit, vous pouvez l'utiliser sans problème dans votre application de sécurité". Mais cela ne prouve pas tout! Ce qui importe, c'est l'approche retenue pour développer le constituant ou l'application de sécurité. Le référentiel IEC 61508 ne donne pas d'indications sur la manière avec laquelle doivent être effectués les tests. L'organisme qui délivre une certification de produits ou une attestation de conformité doit surtout s'attacher à valider le processus de développement qui a été mis en place pour arriver à la sécurité, à valider la pertinence des choix qui ont été retenus.

Mesures. Une autre question revient souvent dans les applications de sécurité : Faut-il séparer les systèmes traitant de la sécurité et ceux traitant du contrôle-commande?

Patrick Teixeira. La norme n'est pas si précise et comme vous le savez, il y a des bus de terrain où les signaux de contrôle-commande et de sécurité utilisent le même câble, il y a aussi des automates de contrôle-commande qui abritent l'application de sécurité.

Cela dit, quand on est évaluateur, on aime bien que tout soit séparé : il y a forcément beaucoup moins de modes communs, il est plus facile de démontrer que la sécurité est assurée…

Mesures. Un mot enfin sur le logiciel, qui fait l'objet de beaucoup moins de discussions que les matériels. Est-il bien traité dans la norme?

Patrick Teixeira. Encore une fois la norme met en valeur l'importance de la démarche. Dans un système programmable, l'aspect logiciel est aussi important que l'aspect matériel (voire plus, mais comme il est souvent moins bien maîtrisé ou qu'on y accorde trop de confiance, on s'y attarde moins). Quand nous faisons une évaluation de conformité, nous validons le système dans son ensemble.

Mesures. Donc avec le logiciel applicatif?

Patrick Teixeira. Bien entendu. Et pour cela, comme pour le reste, nous mettons l'accent sur la démarche suivie par le développeur. Nous nous assurons aussi qu'il applique un certain nombre de règles de codage, qu'il utilise des outils de vérification du code.

Mesures. Parmi ces outils de vérification, utilisez-vous la technique de la preuve formelle?

Patrick Teixeira. Le cas ne s'est pas présenté mais pourquoi pas? La méthode de la preuve formelle consiste à lister les propriétés qui découlent du cahier des charges et à apporter la preuve (mathématique) que, une par une, toutes ces propriétés sont respectées. La méthode de la preuve formelle est très efficace mais elle est lourde à mettre en œuvre et impose une application dès la conception du logiciel. Du coup, seules les applications complexes en aéronautique ou dans le transport par rail y ont recours car, dans ces cas-là, les pannes peuvent amener à des accidents catastrophiques sur le plan humain et il faut donc réduire leur probabilité à un niveau extrêmement faible.

Mesures. Peut-on envisager des certifications ou des attestations de conformité pour des logiciels applicatifs standard?

Patrick Teixeira. Bien sûr et cela se pratique déjà. C'est ainsi qu'il est possible de certifier des blocs de fonction proposés dans les ateliers logiciels des automates programmables.

Propos recueillis par Jean-François Peyrucat

AUTOMATES DE SÉCURITÉ

La redondance ? Oui, mais laquelle ?

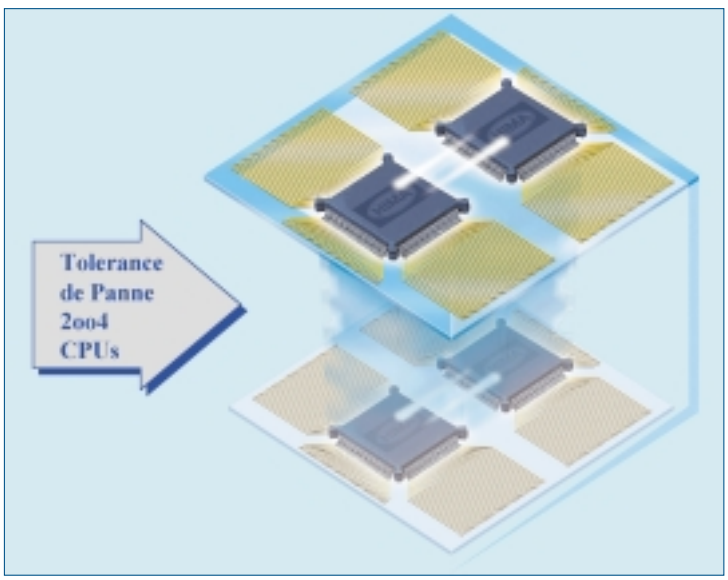
S'ils sont trop fréquents, les arrêts d'urgence sur les process industriels se révèlent économiquement préjudiciables, voire dangereux. Pour les limiter, il est impératif que les architectures des automates de sécurité fournissent à la fois de la sécurité et de la disponibilité. Ceci passe par la mise en œuvre d'architectures redondantes. Dans cet article, Hima brosse un rapide tableau des différents types d'architectures, en mettant l'accent sur la solution Quad qu'elle soutient.

Tout système électronique, quel qu'il soit, est caractérisé par une certaine sûreté de fonctionnement et une certaine disponibilité. Ces deux paramètres dépendent notamment de la manière dont sont conçus les systèmes, de la qualité des composants et des techniques de fabrication utilisés. Ils dépendent aussi de la manière dont travaillent les systèmes en interne, notamment des outils d'autodiagnostic et de la fréquence des tests embarqués mis en œuvre. Bien conçu, fabriqué avec soin, utilisé normalement, un système électronique permet d'obtenir des performances très acceptables pour répondre à la plupart des besoins.

Mais il est des applications où cela ne suffit pas. Pour aller plus loin encore, on ajoute des redondances, en multipliant le nombre des processeurs utilisés, et/ou éventuellement des entrées et/ou des sorties. Il existe plusieurs types de redondances, qui donnent des résultats différents. Dans certaines applications, comme par exemple les serveurs utilisés dans les télécoms, la redondance sera surtout pratiquée pour obtenir une très grande disponibilité du système (quel usager du téléphone ou d'Internet accepte les interruptions de service?). S'il s'agit de piloter un procédé dangereux, la redondance servira à garantir que le système de sécurité met le process dans un état sûr quelles que soient les circonstances. Selon le résultat que l'on recherche, les redondances ne se font pas de la même façon. Le choix d'une architecture plutôt qu'une autre dépend en effet du niveau de sécurité que l'on veut atteindre mais aussi du niveau de disponibilité que l'on souhaite. Avec les redondances relativement simples, on ne peut en général pas obtenir à la fois un niveau élevé de sécurité et une haute disponibilité. C'est l'un ou l'autre. Avec les redondances plus sophistiquées, il est possible d'avoir les deux, mais avec des gradations qui dépendent de l'architecture retenue.

Architecture à une seule unité centrale. Comme son nom l'indique, il n'y a pas de redondance. Si un défaut dangereux est détecté au niveau de l'unité centrale, un module de diagnostic externe (watchdog) permet de déclencher immédiatement un arrêt d'urgence de façon à mettre le process en sécurité.

Les pannes non dangereuses entraînent également un déclenchement de l'arrêt d'urgence.



Les multiples variantes des architectures dupliquées

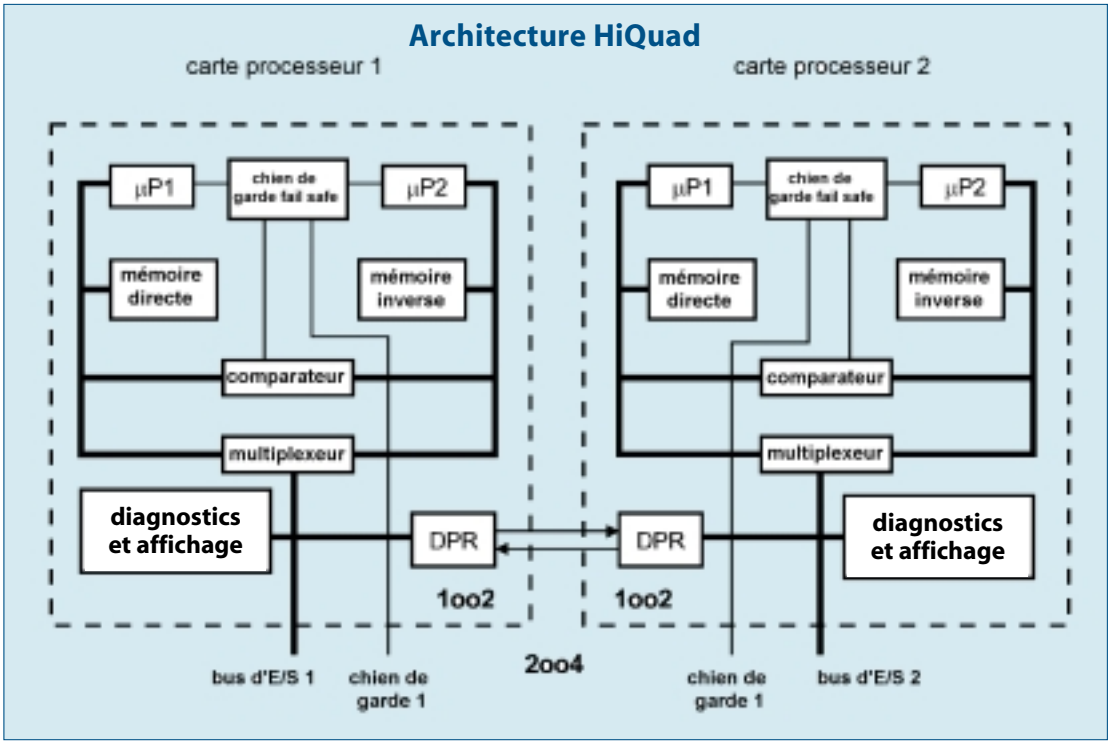
Les systèmes à deux unités centrales existent en de multiples variantes. Les deux unités centrales peuvent avoir des entrées et des sorties communes, ou alors des entrées et des sorties séparées. Ce qui distingue aussi ces systèmes, c'est la manière dont travaillent les unités centrales (types d'échanges qu'il y a entre elles) et la façon dont sont câblées les sorties qui commandent l'arrêt du process (en parallèle ou en série).

Prenons par exemple le cas d'une architecture à deux unités centrales, chacune ayant ses propres entrées et ses propres sorties. On a donc deux canaux indépendants.

Si les sorties sont câblées en série, il suffit qu'une des deux soit en défaut pour déclencher l'arrêt d'urgence du process. On se trouve alors dans une configuration 1oo2 ou, si l'on préfère 2-0. Le système est sûr mais il n'est pas tolérant aux pannes (sa disponibilité est peu élevée).

Si au contraire les sorties sont câblées en parallèle, il faut que les deux sorties soient simultanément en défaut pour déclencher l'arrêt d'urgence du process. Ceci réduit le nombre de déclenchements intempestifs. On se trouve alors dans une configuration 2oo2 (ou 2-1-0), qui assure une disponibilité élevée, mais dont la performance de sécurité est très pauvre.

Dans l'optique de fournir une disponibilité et une sécurité importantes, les architectures doubles sont maintenant réalisées dans une configuration 1oo2D, où on trouve un double câblage des sorties, à la fois série et parallèle. Cette architecture tolérante aux pannes fonctionne normalement dans un mode 2oo2 (2-1-0), mais revient à un mode 1oo2 (2-0) si une panne se produit et



ne peut pas être résolue. De ce fait, sa performance de sécurité dépend évidemment de l'efficacité des diagnostics internes du système, et sa disponibilité opérationnelle de la capacité de ce dernier à résoudre les erreurs et d'isoler le canal en faute, tout en continuant à fonctionner en sécurité sur le canal valide.

Les systèmes 1oo2D ne sont pas tous identiques, et quelques expériences significatives ont démontré un manque de disponibilité résultant de l'exécution des diagnostics de comparaison requis.

Un bon compromis : les architectures tripliquées

Tous les systèmes dupliqués un problème en commun : une sévère restriction du temps de fonctionnement en mode canal unique. Quelques fournisseurs tentent de contourner cette restriction en utilisant un modèle mathématique pour prévoir le taux d'exigence du process, et ainsi allonger le temps de fonctionnement autorisé en canal unique. Cette approche n'est certainement pas recommandée pour la sécurité car les données exploitées dans de tels modèles ne sont qu'approximatives, et les résultats obtenus sont inappropriés pour être utilisés dans des décisions critiques de sécurité.

Les systèmes tripliqués (TMR) sont constitués de trois canaux, avec des sorties câblées à la fois en série et en parallèle. Ils sont très répandus et sont souvent utilisés dans des situations sans réelle justification technique ou économique. L'architecture TMR est à la fois sûre et disponible, elle doit fonctionner en mode 2oo3 (3-2-0) pour des applications de sécurité. Le système TMR réalise des diagnostics par vote ou comparaison. De ce fait, il n'est pas autorisé à fonctionner en canal unique, car il manque de diagnostic interne détaillé et ne peut pas être considéré comme sûr. En fait, les limitations de temps sont imposées pour deux canaux en fonctionnement, et des étapes doivent être respectées pour s'assurer que le système s'arrêtera après la perte du second canal. Un autre problème affecte l'architecture TMR : sa plus grande sensibilité (3 fois supérieure) concernant une erreur de mode commun due d'une part au troisième niveau de redondance et d'autre part au fait que les canaux multiples partagent un ensemble "*hardware*" commun, telle une entrée-sortie commune, un module processeur etc. De plus, le coût initial et le coût de fonctionnement (incluant la maintenance) du système sont élevés.

Encore plus loin avec les architectures quadruplées

La nouvelle architecture Quad (QMR) est une avancée importante au regard des performances liées à la sécurité. Cette architecture propose quatre processeurs (2 par canal) et remédie aux problèmes associés aux architectures à double processeurs, comme les fautes dangereuses détectées d'un des deux processeurs. Les deux paires des processeurs sont synchronisées et utilisent le même programme. Un comparateur "*hardware*" et un chien de garde "*fail-safe*" supervisent le fonctionnement de chaque paire de processeurs pour diagnostiquer et résoudre les anomalies. De ce fait, cette architecture peut fonctionner en SIL3 (RC6) aussi bien sur un que deux canaux, pour une période de temps illimitée.

Du fait de sa structure double et redondante, l'architecture Quad est intrinsèquement plus disponible qu'une architecture tripliquée. Elle est également meilleure en terme de sécurité. Elle apporte une améliora-

Comparaison des différentes architectures

Systèmes dupliqués
- Diagnostics intrinsèques aux modules.
- Certains automates fonctionnent en disponibilité ou en sécurité : les deux options ne sont pas obligatoirement cumulables.
- Temps de fonctionnement très restreint sur une seule unité centrale : disponibilité inférieure à celle du TMR
- Sécurité comparable à celle du TMR
- Prix compétitifs.

Systèmes tripliqués (TMR)
- Diagnostics par comparaisons
- Certains automates fonctionnent uniquement en sécurité.
- Temps de fonctionnement restreint sur deux unités centrales
- Pas autorisé à fonctionner en mono canal (1 unité centrale).
- Beaucoup de modes communs
- Niveau de sécurité comparable à celui obtenu avec un système dupliqué
- Prix initial et maintenance élevés : oblige souvent à regrouper plusieurs unités

Systèmes quadruplés (QMR)
- Diagnostics intrinsèques aux modules
- Temps de fonctionnement illimité sur un seul canal : disponibilité supérieure à celle du TMR.
- Temps de fonctionnement illimité sur un seul canal en classe 6 (SIL3) : sécurité supérieure à celle du TMR
- Très peu de modes communs : séparation des canaux
- MTBF supérieur à celui du TMR
- Coûts d'achat et de maintenance identiques à celui du dupliqué : convient à des projets de toutes tailles.

tion d'un facteur trois, tant en disponibilité qu'en sécurité, par rapport à ce qui est normalement fourni par les architectures TMR. En outre, elle a une sensibilité significativement moindre aux erreurs de mode commun du fait d'une totale séparation, isolation et fonctionnement des canaux redondants.

Voyons plus précisément le problème de la sécurité. Dans les architectures dupliquées, le point crucial du problème concerne les erreurs dangereuses indétectées d'un des deux processeurs. Un processeur unique ne peut pas s'autocontrôler suffisamment pour être considéré comme complètement sûr, et il existe une possibilité qu'une telle erreur puisse mettre les deux canaux dans un état dangereux, et rendre l'automate incapable de se positionner dans une configuration de sécurité. C'est pourquoi de sévères restrictions de temps de fonctionnement sont imposées au niveau de SIL3 (RC6) pour les architectures doubles fonctionnant dans des conditions d'erreur.

L'architecture Quad (QMR) intègre une paire de doubles processeurs opérant dans un mode de sécurité (2-0) pour chaque canal. Cette configuration augmente de façon significative les diagnostics des processeurs en opération, répond parfaitement aux critères de sécurité concernant les fautes dangereuses indétectées, et par conséquent supprime toutes les restrictions de temps de fonctionnement du système en mode mono canal.

Une comparaison des performances de sécurité (PFD, probabilité de défaillance sur sollicitation) des différentes architectures de sécurité peut être établie. Si l'on se réfère à l'ISA TR84.02, Part 2, 1998, on voit que l'architecture Quad (2oo4) est comparable à celle de l'architecture ultra sûre 1oo3, tandis que l'architecture TMR 2oo3 est identique à l'architecture 1oo2D. Cette comparaison conclut à la prédominance de l'architecture QMR 2oo4 par rapport à l'architecture TMR 2oo3 ou dupliquée 1oo2D.

Une autre considération importante dans la performance des systèmes de sécurité est leur capacité de détection de fautes internes de façon rapide et correcte. En effet, les automates de sécurité doivent être capables de répondre

Configurations des systèmes programmables de sécurité

Type	Configuration	Mode de fonctionnement		Nombre min. de canaux opérationnels	Nombre de défauts pour déclencher
Simple	**1oo1**	1-0	Fonctionnement avec 1 CPU puis arrêt d'urgence après une panne de cette CPU	1	1
Dupliquée	**1oo2**	2-0	Fonctionnement avec 2 CPU puis arrêt d'urgence après une panne d'une des 2 CPU	2	1
Tripliquée (TMR)	**1oo3**	3-0	Fonctionnement avec 3 CPU, puis arrêt d'urgence après une panne d'une des 3 CPU	3	1
Dupliquée	**2oo2**	2-1-0	Fonctionnement avec 2 CPU, puis avec 1 CPU, puis arrêt d'urgence après une panne de la dernière CPU	1	2
Tripliquée (TMR)	**2oo3**	3-2-0	Fonctionnement avec 3 CPU, puis avec 2 CPU, puis arrêt d'urgence après une panne d'une des 2 CPU restantes	2	2
Quadruple (QMR)	**2oo4**	4-2-0	Fonctionnement avec 4 CPU, puis avec 2 CPU, puis arrêt d'urgence après une panne d'une des 2 CPU restantes	2	2

Systèmes 1ooN : *système dédié à la sécurité, ou sous-ensemble d'un tel système, constitué de N canaux indépendants qui sont connectés de telle sorte qu'il suffit qu'un seul canal soit opérationnel pour que la fonction de sécurité soit assurée.*

Systèmes 2ooN : *système dédié à la sécurité, ou sous-ensemble d'un tel système, constitué de N canaux indépendants qui sont connectés de telle sorte qu'il suffit que deux des canaux soient opérationnels pour que la fonction de sécurité soit assurée.*

dans le temps de sécurité spécifié *(safety time)*.
Le temps de sécurité du process (TSP) d'un process donné est par essence le temps de tolérance aux pannes, avant d'atteindre une situation dangereuse. Ainsi, si une situation dangereuse existe pour un temps plus long que celui spécifié dans le TSP, le process entre dans un état dangereux. Compte tenu de ces exigences, l'automate de sécurité doit maintenir un niveau de sécurité par la détection interne de fautes dangereuses et les corriger sans dépasser le TSP, ou en conséquence être considéré comme incapable de remplir les conditions de sécurité de ce process.
Comme exemple typique, on peut citer le Système de Contrôle de Brûleur (SCB.) où le TSP d'une seconde est défini par le TüV (DIN VDE 0116). Compte tenu que deux cycles d'un automate sont demandés pour détecter et corriger une panne interne, le Temps de Détection et de Correction de la Faute (TDCF) de l'automate ne peut pas dépasser 500 ms. Si l'automate de sécurité ne peut remplir cette condition, il ne peut pas être utilisé pour la sécurité d'application du SCB.

Coût de fonctionnement

Les normes de sécurité existantes et à venir demandent que le SIS (Safety Instrumented System / système instrumenté de sécurité) soit installé de façon à atténuer le risque associé au fonctionnement de process dangereux. Ignorer ces spécifications n'est pas une option à long terme. De même, le coût initial et le coût de fonctionnement du SIS doivent être considérés.
Il est reconnu que quelques architectures, du fait de leur complexité inhérente, engendrent des coûts d'achat et de fonctionnement importants. Ceci se vérifie pour des projets de petite taille ou des projets requérant un niveau de sécurité SIL1 ou SIL2. Pour de tels projets, utiliser une architecture tripliquée (TMR) n'a pas de justification économique, compte tenu du coût initial et du coût de fonctionnement.
En outre, si un process peut être d'un niveau SIL1 ou SIL2 au lieu de SIL3, des économies significatives peuvent être réalisées dans d'autres domaines (comme les capteurs), ce qui permettra de ne pas utiliser d'architectures doubles ou tripliquées comme demandées pour les applications SIL3.
L'architecture Quad peut être configurée pour répondre aux exigences de performance des SIL1, 2 et 3. Elle peut fonctionner en canal unique ou redondant, en canal simple, redondant ou tripliqué un capteur ou un actionneur est demandé pour fonctionner avec chaque boucle de sécurité. Que ce soit dans une configuration simple, sélectivement redondante ou complètement redondante, le niveau de sécurité SIL3 est atteint. Si la redondance est ajoutée, la disponibilité augmente considérablement et les performances de sécurité sont maintenues.
Ajouter la redondance ne représente pas un coût très important car les prix du processeur et des modules E/S sont significativement moins élevés que ceux des architectures alternatives. De plus, comme ces modules sont moins complexes, leur MTBF est de ce fait plus long et les dépenses de maintenance du système sont substantiellement réduites.
Du fait que cette nouvelle architecture est relativement économique, elle apporte un bénéfice additionnel au niveau du contrôleur du process dont l'automate de sécurité assure la protection. De nombreuses normes de sécurité ne voient plus d'inconvénient à regrouper le contrôleur du process et l'automate de sécurité dans un même système. De même, il n'y a désormais plus de justification économique à vouloir prendre un seul automate de sécurité pour protéger plusieurs contrôleurs de process. Il en résulte que l'installation du système de sécurité, les tests et la maintenance sont moins complexes et moins sujets à l'erreur humaine.
De plus, pour augmenter la sécurité, l'automate de sécurité dédié à un seul contrôleur de process est nettement plus facile à maintenir ou à modifier. On élimine aussi toute possibilité d'arrêt d'urgence accidentel des autres unités de process.

Pascal Paumard
Hima

Fonctionnement de la sécurité après la première erreur

Architecture de base		Comportement après la première erreur	
Simplex	1oo1	Fail Safe (classe 4/SIL 2 seulement)	
Double	1oo2D	1oo1D	Limitation sévère du temps de fonctionnement
TMR	2oo3	1oo2	Limitation du temps de fonctionnement
QMR	2oo4	1oo2D	Pas de limitation du temps de fonctionnement

Pour des applications de sécurité, les systèmes en canal unique (1-0) ne sont pas tolérants aux erreurs et doivent être *"fail safe"*.
Les architectures doubles peuvent fonctionner en *"fail safe"* ou en mode dégradé de fonctionnement en canal unique (2-1-0) sous des conditions spécifiques d'erreur, et avec des temps de limitation de fonctionnement définis dans leur rapport de certification de sécurité. Obtenir une copie de ce rapport pour tout automate est grandement recommandé.
Les deux architectures TMR (3-2-0) et Quad (4-2-0) reviennent en mode de fonctionnement 2-0 après une première erreur. Cependant, l'architecture Quad (QMR) garde ses diagnostics internes complets, elle n'a pas de restriction de temps de fonctionnement sous ce mode, et elle conserve son niveau de sécurité maximum SIL3 (RC6).
Le mode de fonctionnement dégradé au niveau de sécurité SIL3 (RC6) demande que l'automate fournisse un circuit secondaire de désactivation des sorties. Celui-ci peut être externe ou intégré dans les modules de sortie, mais il doit être en conformité avec les règles de sécurité. Les mêmes restrictions s'appliquent au fonctionnement de l'automate après une seconde erreur. Pour l'architecture TMR, la seconde erreur peut provenir de l'unité centrale ou des entrées-sorties. Une telle situation imposera l'arrêt d'urgence du système. Pour l'architecture QMR, seule une erreur de l'Unité Centrale sur le second canal entraînera un arrêt d'urgence du système, car des erreurs des entrées-sorties peuvent être gérées indépendamment, du fait de ses diagnostics internes plus complets. En outre, l'architecture QMR propose une tolérance additionnelle aux erreurs, et un niveau plus élevé de disponibilité opérationnelle.

CAPTEURS-VANNES

Pas de SIL qui tienne sans tests périodiques !

Le niveau SIL attribué à un système instrumenté de sécurité est calculé en prévoyant des tests périodiques sur les différents éléments qui composent le système. Pour les vannes, l'élément le plus fragile de la boucle de sécurité, ce test n'est pas pratique sauf si on arrête le process. Il existe une alternative : le test sur une petite partie de la course.

Dans l'application de la norme IEC 51508 et de celles qui en sont issues, la performance d'un équipement de sécurité est quantifiée par son SIL (Safety Integrity Level), c'est-à-dire son niveau d'intégrité de la sécurité. Le SIL définit la probabilité de défaillance dangereuse que l'on s'autorise. Le SIL ne peut prendre que 4 valeurs possibles (de 1 à 4), et on ne cherche donc pas à définir des valeurs précises des probabilités de défaillance dangereuses, mais il faut que la valeur obtenue se trouve à l'intérieur de la fourchette définie par le SIL. Pour un SIL donné, la valeur de cette probabilité de défaillance peut varier dans un rapport 10. Le concepteur d'une application de sécurité peut donc s'autoriser une marge d'erreur, sans que la valeur du SIL soit remise en cause.

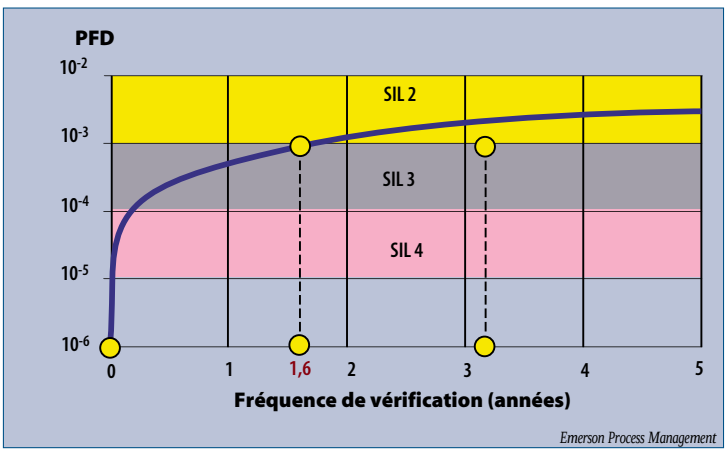
Ceci étant, lorsque l'on se trouve aux extrémités de la fourchette autorisée, l'erreur même minime peut vite conduire à un déclassement, et un système qui était par exemple SIL3 peut se retrouver en catégorie SIL2.

Il faut savoir aussi qu'un niveau SIL n'est pas garanti à vie. Les éléments du système de sécurité vieillissent, leurs performances se dégradent. C'est la raison pour laquelle le niveau SIL est considéré comme valable tant que l'on ne dépasse pas une durée bien définie.

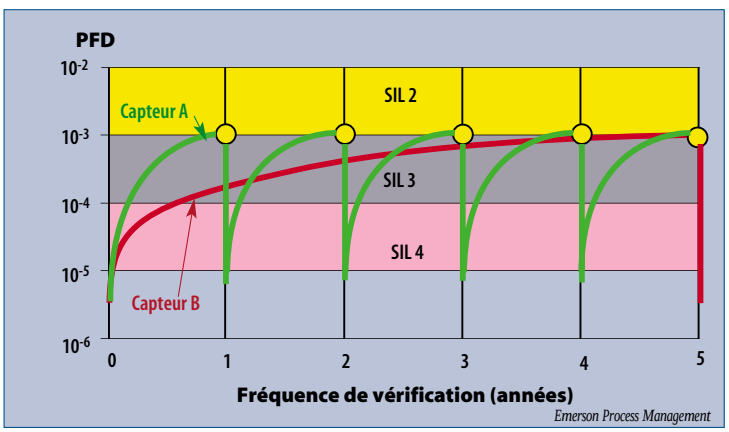
Le test en ligne et hors ligne des systèmes de sécurité est clairement mentionné dans les normes IEC 61508 et IEC 61511 comme étant une condition sine qua non pour maintenir le niveau SIL annoncé. Si toutes les défaillances étaient auto-détectées, il ne serait pas nécessaire de vérifier périodiquement les éléments entrant dans la composition d'un SIS. Des détecteurs de niveau qui sont bloqués, des relais de commande d'un pressostat qui sont collés, des vannes d'arrêt qui sont bloquées, cela est fréquent et cela peut être très dangereux si de tels défauts se révèlent au moment où le système de sécurité est sollicité. Le seul et unique objectif du test en ligne est de révéler ces défauts. Bien entendu, dans un système instrumenté de sécurité, la fréquence de test dépend du type d'élément et de l'importance du rôle qu'il joue dans le système. La fréquence des tests est calculée à partir des éléments fournis par les constructeurs.

Pour les automates dédiés à la sécurité, les périodes de test atteignent facilement plusieurs années. Certains sont annoncés avec des périodes supérieures à un siècle ! Bien entendu, plus il y a des redondances, plus la période de test sera importante. Mais à structure équivalente, il peut aussi y avoir des grosses différences au niveau de la période de test. Le choix des composants électroniques joue en effet un rôle important.

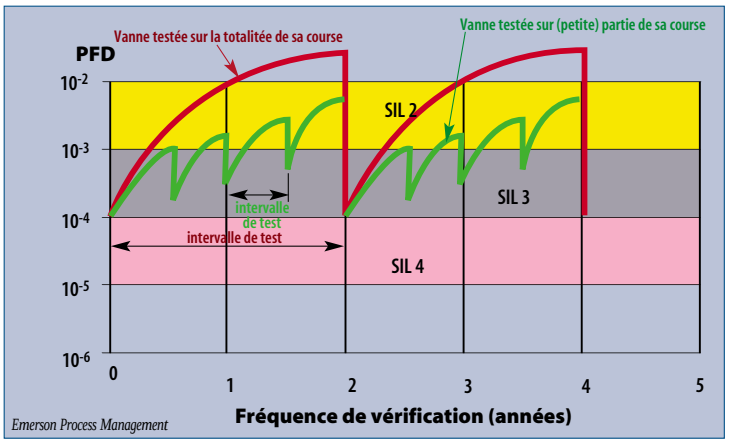
Dans tout système instrumenté de sécurité, la vanne est le composant le plus fragile. Cela se comprend aisément, les vannes restent sans bouger pendant de longues périodes, et l'obturateur aura tendance à se coller. Et



Comme on peut le voir ici, la valeur de la probabilité sur sollicitation (PFD) se dégrade au fil du temps. La courbe obtenue ici correspond à un capteur de pression spécifié pour une application SIL3. Il reste SIL3 pendant 1,6 an, ensuite il passe en niveau SIL2.



Cette illustration présente les valeurs PFD de deux capteurs de pression, tous deux spécifiés pour une application SIL3.
Le capteur A est SIL3 pendant 1 an. Au bout de cette période, si on effectue un test et que ce test atteste du bon état de fonctionnement du capteur, le capteur peut continuer à être utilisé dans une application SIL3. Et ainsi de suite tous les ans.
Le capteur B, par contre, conserve son niveau SIL3 pendant 5 ans, sans qu'aucun test ne soit nécessaire pendant toute cette période.



Pour maintenir un niveau de PFD relativement faible (et donc un SIL élevé), les vannes de sécurité doivent être soumises à des tests périodiques. Comme on le voit ici sur la courbe rouge, il est impossible d'avoir à la fois un SIL élevé et une période de test longue. Une période de test longue serait pourtant bien pratique car les tests des vannes nécessitent d'arrêter le process (il existe des alternatives mais elles sont coûteuses et peuvent être dangereuses). Si on veut un SIL élevé sur une longue période sans test, la solution classique consiste à prévoir une redondance au niveau de la vanne (mais c'est une solution coûteuse).
La courbe verte présente une alternative. Ici on pratique un test à intervalles rapprochés mais sur une course partielle de la vanne, ce qui évite d'avoir à arrêter le process. On voit qu'il est dès lors possible de garantir un niveau SIL2 (voire SIL3) pendant une longue durée, avec une seule vanne.

donc à ne pas se décoller le jour où la vanne devra être actionnée. *Emerson Process Management* estime que 50 % des défaillances viennent des vannes tout-ou-rien. Il faut donc, bien évidemment, pratiquer des tests périodiques. Le problème, c'est que les arrêts des process pour maintenance sont de moins en moins fréquents : il y avait autrefois un arrêt par an, la tendance est de faire un arrêt tous les trois à cinq ans. Autrement dit, si on veut continuer à faire comme par le passé un test annuel complet d'ouverture de la vanne, il faut prévoir des dispositifs permettant de réaliser quand même ces tests. Il est par exemple possible de prévoir des dispositifs pneumatiques ou des bypass. Ces solutions sont ou coûteuses ou potentiellement dangereuses. Dans le cas d'un test réalisé à l'aide d'un bypass, qui nécessite des interventions manuelles, que se passe-t-il si, au moment de réaliser les tests, le système sécurité doit entrer en action? Pour contourner ces limitations, *Emerson Process Management* propose de réaliser des tests en ligne d'ouverture partielle (de 1 à 30 %) de la vanne, histoire de s'assurer que la vanne n'est pas collée. Bien entendu, si c'est le cas, l'information est remontée au contrôleur. Le gros avantage de cette technique est que les tests partiels peuvent être pratiqués à des périodes très rapprochées, ce qui permet de maintenir le SIL au niveau initial. Bien entendu, cela ne dispense pas de réaliser des tests périodiques approfondis mais ceux-ci peuvent être beaucoup plus espacés et être pratiqués lors des arrêts du process. ■

L'intérêt du test sur une partie de la course d'une vanne

Le tableau ci-contre montre les valeurs de SFF obtenues pour les vannes dans le cas où on pratique un test complet aux périodes normales (espacées) et dans le cas où on pratique un test sur une partie de la course (périodes beaucoup plus rapprochées).

	Test périodique normal	Avec test sur une partie de la course
Défaillance dangereuse détectée (DD)		810
Défaillance dangereuse non détectée (DU)	1 350	540
Défaillance non dangereuse détectée (SD)		1 650
Défaillance non dangereuse non détectée (SF)	1 650	
Pourcentage de défaillance en sécurité $SFF = \frac{DD + SD + SF}{DD + DU + SD + SF}$	**55 %**	**82 %**

Le tableau ci-contre donne l'incidence de la valeur du SFF sur l'architecture du système de sécurité (au niveau de la vanne). Une tolérance à la faute de "n" signifie que s'il y a "n + 1" fautes, le système de sécurité n'est plus opérationnel. Autrement dit, si on veut une tolérance à 1 défaillance, il faut prévoir une redondance simple et si on veut une tolérance à 2 défaillances, il faut prévoir une redondance double. Supposons que l'application exige un SIL2. Ce tableau montre que pour une vanne prévue avec un test périodique normal (donnée pour un SFF de 55 %), on ne peut atteindre un SIL2 qu'à condition de prévoir une redondance simple (chiffre marqué en rouge). Si on utilise une vanne avec un test sur une partie de la course (SFF = 82 %), il est possible d'atteindre un SIL2 sans redondance (chiffre en vert).

SFF	Tolérance aux défaillances		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - 90 %	SIL2	SIL3	SIL4
90 % - 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

Pour les mêmes raisons, un SIL3 ne peut être atteint dans le premier cas qu'avec une redondance double. Dans le deuxième cas (test sur une partie de la course), il peut être atteint avec une redondance simple.