Les normes applicables à la sécurité : état actuel et évolutions

Jean-Philippe Pineau, Philippe Villeneuve de Janti

LES NORMES APPLICABLES A LA SÉCURITÉ : ÉTAT ACTUEL ET ÉVOLUTIONS CAS DES AUTOMATES PROGRAMMABLES

J.P. PINEAU **Ph. VILLENEUVE de JANTI**

INERIS
Parc Technologique ALATA
BP n°2
60550 VERNEUIL EN HALATTE

Journée d'étude EXERA "Sécurité des biens, des personnes, protection de l'environnement", Courbevoie, 14 février 1996, 14 p.

I. INTRODUCTION

La sécurité peut être définie comme un état de confiance vis-à-vis de risques encourus. Une telle définition se rapporte donc aux situations dans lesquelles quelqu'un n'est exposé à aucun risque, ou tout au moins à un niveau considéré comme "acceptable" de risque d'agression physique, d'accident ou de vol... La sécurité peut aussi concerner un équipement, une installation dont il faudra éviter la défaillance ou la détérioration. Pour pouvoir être garantie, elle impose d'effectuer une analyse des risques encourus.

Le champ normatif et réglementaire concerné va donc être fort large. En fonction des éléments d'appréciation du risque apportés par ces normes et réglementations, il devient possible d'exercer un management de la sécurité d'un système, d'un procédé. Dans un tel management doivent être définis une politique de sécurité, des objectifs et des responsabilités. Pour son application, la planification des objectifs, la mesure des résultats obtenus et la maîtrise des effets sur l'homme, les biens et l'environnement doivent être prévues.

Il est nécessaire de faire la différence entre les Directives traitant de la conception et de la fabrication (en application de l'article 100A du Traité de Rome) et celles concernant l'utilisation (en application de l'article 118A de ce même traité).

Parmi les directives européennes (100A) ayant une dimension "sécurité" on peut citer la directive "machines" 89/392/CEE (y compris son amendement concernant les risques spécifiques dus à la mobilité et à l'aptitude à lever des charges(1)), la directive 89/686/CEE portant sur la conception des équipements de protection individuelle (connue sous le nom de directive "EPI"), la directive sur les jouets, la directive sur les appareils à gaz, la directive sur les appareils à pression simples, la directive sur la compatibilité électromagnétique "CEM", la directive sur les appareils et systèmes de protection destinés à être utilisés en atmosphères explosibles "ATEX" 94/9/CEE, la directive concernant les risques majeurs de certaines activités industrielles (82/501/CEE en cours de révision).

Différentes autres directives sont en projet : équipements sous pression, protection en matière de sécurité et santé des travailleurs susceptibles d'être exposés aux risques d'atmosphères explosibles (ATEX 118 A),...

Notre propos porte uniquement sur les aspects liés à la sécurité industrielle pour lesquels, ainsi que l'a fait le Comité d'Orientation Stratégique "Construction mécanique" dans un document d'analyse, on peut distinguer trois domaines :

- sécurité (individuelle) des travailleurs,
- sécurité des installations industrielles,
- sécurité des produits.

Nous avons traité l'aspect sécurité d'équipements en nous appuyant sur le travail normatif effectué pour l'application des Directives "Machine" et "ATEX" où seules la conception et la construction sont prises en compte.

Nous avons par ailleurs examiné la normalisation applicable dans le domaine des automates programmables dédiés à la sécurité et les méthodologies pouvant être retenues pour leur évaluation.

Toutefois, avant d'examiner ces différents points, nous donnerons quelques éléments sur les rôles respectifs de la réglementation et des normes.

II. RÈGLEMENTS ET NORMES

II.1. Le rôle des normes

En général et principalement, le choix d'appliquer une norme est un acte volontaire du concepteur, du fabricant ou de l'utilisateur de matériel. Ainsi, il doit être clair que, lors de l'établissement d'une norme, même si des valeurs limites sont données, elles ne doivent être considérées que comme des valeurs de référence ; comme le souligne GAMBELLI (2) de telles valeurs doivent être réalisables, déterminées par l'état de la technique et sont utiles pour fixer des niveaux de performance auquels le concepteur, le constructeur ou l'utilisateur peut avoir recours, afin d'évaluer l'efficacité des mesures prises pour réduire un phénomène dangereux.

Des normes homologuées peuvent être rendues obligatoires, par exemple lorsqu'il y est fait référence dans le cadre de marchés publics ou assimilés.

Il s'agit fondamentalement d'une relation contractuelle, le contrat fixant l'obligation des parties.

Enfin, des normes peuvent être rendues obligatoires par arrêté ministériel.

Comme le souligne J.P. LACORE (7), chargé de mission "Normalisation" à l'INRS : Dans l'état actuel des réflexions, on peut avancer que, **pour un produit donné, l'état de la technique dans l'esprit de la nouvelle approche, celui que doivent refléter les normes, est celui qui procure aux utilisateurs de ce produit le niveau de sécurité le plus élevé que permettent d'atteindre, lorsqu'on les prend en compte conjointement et avec une volonté d'harmonisation, les connaissances scientifiques, les possibilités techniques et les contraintes économiques du moment.** Ce n'est pas, en particulier, ce qu'il est possible de réaliser de mieux à un moment donné en mettant en oeuvre tout ce qui est techniquement possible et en ne considérant que la faisabilité, à l'exclusion de toute autre contrainte.

Un memorandum sur la normalisation en matière de sécurité destinée à appuyer les directives "nouvelle approche" avec application au domaine des machines (3) précise notamment :

* la prise en compte de l'état de la technique lors de l'élaboration des normes,

* la prise en compte de l'expérience de l'utilisateur lors de la définition de l'utilisation normale d'un équipement,

II.2. Articulation normalisation/réglementation

Nous avons repris dans ce qui suit certains points de l'édition juin 95 du document "qui fait quoi : sécurité des machines" publié par l'AFNOR (3);

Les directives communautaires basées sur l'article 100A du Traité de Rome (établissement et fonctionnement du marché intérieur) ne contiennent plus les spécifications techniques détaillées des produits ou des matériels auxquels elles s'appliquent. Elles visent à harmoniser uniquement les exigences essentielles auxquelles doivent satisfaire les produits pour avoir accès au marché européen, laissant aux organismes européens de normalisation (CEN, CENELEC et l'ETSI) le soin de définir les spécifications (prescriptions) techniques nécessaires au respect des dites exigences.

Il est reconnu aux produits conformes aux normes européennes harmonisées une présomption de conformité aux exigences essentielles de la directive couvertes par la norme, les modalités de certification pouvant être différentes selon qu'il y a ou non application de normes.

A côté d'un objectif purement économique, la libre circulation des biens, l'Union européenne s'est fixée un objectif social : garantir aux travailleurs un niveau de protection élevé.

Outre la réponse aux besoins des directives basées sur l'article 100A du Traité de Rome, les acteurs socio-économiques font également appel à la normalisation dans le cadre des directives fondées sur l'article 118 A, qui visent à promouvoir l'amélioration de la sécurité et de la santé des salariés sur les lieux de travail. Bien que ces directives ne renvoient pas aux normes, leur mise en application peut impliquer de disposer de documents normatifs, en particulier pour spécifier des méthodes de contrôle et de mesurage des seuils d'exposition à des agents physiques ou biologiques.

III. SÉCURITÉ DANS LA CONCEPTION DES ÉQUIPEMENTS

Seuls les cas de la Directive Machine et ATEX sont traités ici à titre d'exemple.

III.1. Directive Machine 89/392/CEE modifiée pour la dernière fois par 93/68/CEE

Dans cette directive, les exigences essentielles de sécurité et de santé ont été regroupées en fonction des risques qu'elles couvrent, par exemple les risques mécaniques et d'autres risques dus à l'énergie électrique, à l'électricité statique, au bruit, aux incendies, aux explosions...Le fabricant a l'obligation d'effectuer une analyse des risques afin de rechercher tous ceux qui s'appliquent à sa machine.

Dans le cadre de la nouvelle approche, pour établir les prescriptions techniques associées au respect des exigences essentielles de sécurité de la Directive Machine, 710 sujets étaient au 1er juillet 1995 traités ou en cours d'élaboration par 44 comités techniques. Ainsi, le CEN, CT 114 "Sécurité des Machines" avec ses 17 groupes de travail, avait écrit ou en cours d'écriture 43 normes.

Le signe extérieur de conformité à la Directive est un marquage spécifique CE.

Notons que les composants de sécurité de l'Annexe IV font l'objet d'une attestation d'Examen CE de type par des organismes notifiés auprès de la CEE : l'INRS, L'INERIS et le CETIM pour la France (J.O des CE du 25/10/95).

III.2. Directive Appareils et systèmes de protection destinés à être utilisés en atmosphères explosibles 94/9/CEE.

Dans cette directive (4) le risque provient du fait que les machines fonctionnent dans une atmosphère susceptible de devenir explosive du fait de la présence dans l'air de substances inflammables sous forme de gaz, vapeurs, brouillards ou poussières. Pour ce risque particulier, cette directive vient compléter la Directive Machine. D'autres risques tels que ceux dus aux surfaces chauffées, aux contacts directs ou indirects doivent être examinés.

En ce qui concerne les équipements contribuant à la sécurité, ils doivent fonctionner indépendamment des dispositifs de mesurage et de commande nécessaires à l'exploitation. Dans toute la mesure du possible, la défaillance d'un dispositif de sécurité doit être détectée suffisamment rapidement à l'aide de moyens techniques appropriés pour qu'il n'existe "qu'une très faible probabilité d'occurrence d'une situation dangereuse".

Un paragraphe concerne explicitement les risques provenant du logiciel, dans le cas de dispositifs de sécurité programmables.

Cette directive est en cours de transposition en droit français.

IV. LES SYSTÈMES ELECTRONIQUES PROGRAMMABLES RELATIFS A LA SÉCURITÉ DES INSTALLATIONS INDUSTRIELLES

IV.1. Panorama sur la normalisation

Il est utile de dresser un tableau aussi général que possible de la normalisation, au niveau européen et international sur le sujet. Plusieurs éclairages sont possibles. A titre d'exemple, le TÜV et un fabricant d'instrumentation de sécurité (Pepperl et Fuchs) ont schématisé la situation dans les tableaux annexés ci-après.

Trois projets de norme sont importants et peuvent s'appliquer aux automatismes pour la gestion des sécurités : les projets de normes allemandes DIN V 19250 et DIN V 0801, le projet de norme internationale CEI 1508 et le projet de norme européenne pr EN 954 :

- Projet CEI 1508 : sécurité fonctionnelle : systèmes dédiés à la sécurité,
- Measurement and control - Fundamental safety aspects for measuring and control protective equipment, DIN V 19250 et DIN V 0801.
- Safety of Machinery ; Safety related parts of control systems : Part 1 : General principles for design, Part 2 : Validation, pr EN 954-1 et EN 954-2.

Les conditions d'applicabilité de ces trois projets ont été étudiées par l'INERIS (5, 6).

Dans une de ses parties, le projet international CEI 1508 (comité technique 65A) concerne plus particulièrement les systèmes de protection pour les procédés continus des industries chimiques et de production d'énergie, mettant en oeuvre des techniques électriques, électroniques et programmables. Les automates programmables dédiés à la sécurité sont ici directement concernés. D'une façon générale les systèmes de protection considérés mettent en oeuvre un nombre élevé d'informations d'entrée, parfois analogiques, des fonctions de sécurité variées et des temps de réponse pouvant aller jusqu'à quelques secondes.

Le projet de norme allemand DIN V 19250 s'applique bien au cas des dispositifs chargés d'assurer la sécurité d'installations industrielles.

Le projet européen EN 954 s'inscrit dans le cadre de l'application de la Directive Machine et s'adresse plutôt au cas des machines dangereuses de l'industrie manufacturière et des automatismes pour la protection de leurs opérateurs. Un nombre restreint de capteurs et d'actionneurs sont concernés et les temps de réponse sont souvent brefs (de l'ordre de quelques centaines de millisecondes). Tous les types de technologies sont considérés.

IV.2. Classification du risque et classes d'exigence

Il s'agit, à partir d'une évaluation des risques encourus en cas de défaillance du système de sécurité, d'établir des exigences en terme de résistance aux défaillances.

Cette estimation du risque repose sur un graphe de risque, prenant en compte des paramètres tels que la gravité des dommages corporels, la fréquence et la durée d'exposition et la possibilité d'éviter un phénomène dangereux. En fonction de cette estimation, on sélectionne des classes d'exigence de sécurité plus ou moins sévères.

Si pour établir le graphe de risque d'une situation on s'appuie sur le référentiel normatif CEI 1508, les paramètres à prendre en compte sont les suivants :

Cx : Possibilité d'avoir des personnes blessées ou tuées (C = 1, 2, 3 ou 4)

Fx : Durée de séjour dans la zone dangereuse (F = 1 ou 2)

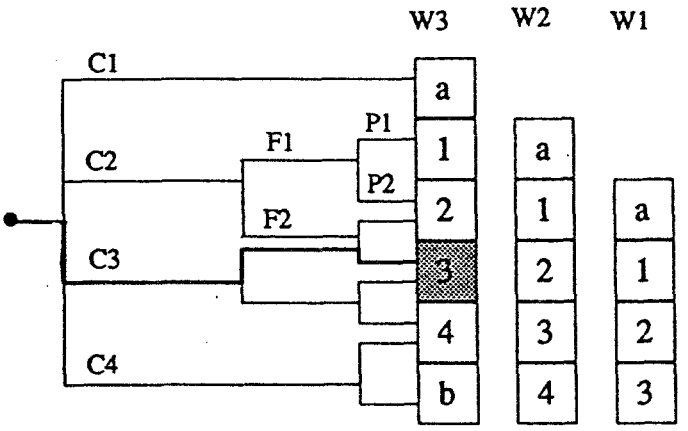
Px : Possibilité d'éviter un phénomène dangereux (P = 1 ou 2)

Wx : Probabilité d'occurence d'une situation dangereuse en l'absence du système de gestion de sécurité (W = 1, 2 ou 3).

La combinaison de ces paramètres permet de définir la classe d'exigence (6 classes).

Considérons les hypothèses suivantes :

Mort de plusieurs personnes,	C = 3
Temps de séjour court dans la zone dangereuse,	F = 1
Faible possibilité d'éviter le phénomène dangereux,	P = 2
Probabilité d'occurrence élevée.	W = 3



Dans ces conditions, la classe d'exigence (zone grisée) est 3. Si on avait choisi une probabilité d'occurrence plus faible, W2 par exemple, la classe d'exigence aurait été 2.

Le même cas examiné selon le référentiel DIN V 19250 conduirait à déterminer une classe d'exigence parmi les 8 existantes.

Les experts s'accordent sur une assez bonne correspondance entre les classes d'exigences des deux référentiels.

Classes d'exigence	
CEI 1508	DIN V 19250
a : Pas d'exigences particulières des sécurités	1
1 2 degrés de résistance aux 3 défaillances de plus en plus 4 sévères	2,3 degrés de résistance aux 4 défaillances de plus en plus 5,6 sévères 7
b : la technologie électronique programmable est insuffisante	8

Une correspondance avec les 4 niveaux d'exigence du projet EN 954 est malaisée car les échelles de gravité et la caractérisation de l'aspect dangereux des phénomènes diffèrent.

Mais les classes d'exigence précédentes correspondent à des objectifs de performance en terme de résistance aux défaillances. Seul le projet international CEI 1508 s'intéresse à quantifier la probabilité de défaillance dangereuse du système dédié à la sécurité pour pouvoir la comparer à des niveaux de seuils tolérables appelés "niveau de sécurité" ou "niveau de résistance aux défaillances dangereuses" du système. Des fourchettes de valeurs sont indiquées pour chaque classe d'exigence du Système Electronique Programmable "PES" incluant les capteurs et actionneurs.

Classes d'exigence (1)	Niveaux de sécurité	
	Fonctionnement continu de la fonction de sécurité (probabilité de défaillance dangereuse par heures)	Fonctionnement sur demande de la fonction de sécurité (probabilité de défaillance de la fonction sur demande)
4	$10^{-8} < \lambda^{DU} < 10^{-9}$	$10^{-4} < PFD_{avg} < 10^{-5}$
3	$10^{-7} < \lambda^{DU} < 10^{-8}$	$10^{-3} < PFD_{avg} < 10^{-4}$
2	$10^{-6} < \lambda^{DU} < 10^{-7}$	$10^{-2} < PFD_{avg} < 10^{-3}$
1	$10^{-5} < \lambda^{DU} < 10^{-6}$	$10^{-1} < PFD_{avg} < 10^{-2}$

(1) appelé dans la norme CEI 1508 "Safety integrity level"

Vis-à-vis de la disponibilité du procédé industriel, l'évènement redouté est le repli intempestif. Il est quantifié par le "MTTF spurious" qui est un temps moyen de disponibilité. Des valeurs sont indiquées dans le projet de norme en correspondance avec des limites pour les intervalles de temps entre opérations de maintenance systématique. Un déclenchement intempestif peut avoir des conséquences sur la sécurité elle-même, et sur la durée de vie des installations.

Il est à noter que ces 3 projets ne considèrent que l'aspect des dommages corporels dans les grilles de classification des risques. Les aspects dommages à l'installation ou pollution de l'environnement, qui sont bien pris en compte aujourd'hui par les exploitants industriels dans leur démarche d'études et de réalisation des systèmes de sécurité instrumentés, n'apparaissent pas dans ces projets de norme.

D'autre part les niveaux d'exigence ou "catégories" du projet EN 954 précisent des objectifs de caractère déterministe sur le maintien opérationnel du système de sécurité en présence de défaillances. Il s'ensuit actuellement une certaine difficulté pour valider la conformité d'un dispositif donné aux exigences de cette norme, à un coût et dans des délais acceptables par les constructeurs.

IV.3. Perspectives d'évolution

A. PR EN 954

La partie 1 (principe généraux de conception, partie de système de commande dédiée aux fonctions de sécurité) devrait être soumise au vote formel en 1996. Les travaux en cours pour élaborer la partie 2 (validation) mettent en évidence les difficultés du concept de catégories quand il s'agit de leur validation alors que les circuits comportent en général des composants complexes fortement intégrés ou programmables, dont la liste de fautes ne peut être établie de façon exhaustive. La vérification de conformité aux exigences de comportement sur défauts, dans des conditions reproductibles d'un laboratoire à l'autre, fait l'objet actuellement de nombreux travaux (7).

Une approche par la recherche des fautes estimées comme étant les plus critiques pour la sécurité au niveau des blocs fonctionnels, est proposée par les experts allemands. Elle devrait être validée par des essais d'injection de fautes correspondantes.

L'INERIS, en étroite concertation avec l'INRS et le CETIM, coordonne actuellement le montage d'un projet au niveau européen dans le programme "Normes, Mesures, Essais" pour établir des procédures harmonisées pour la validation des dispositifs électroniques complexes de sécurité.

B. Projet CEI 1508

Le domaine d'application de ce projet de norme, basé à l'origine sur les projets ISA 84 (démarche quantitative par calculs des probabilités de défaillances) et VDE 0801 (démarche qualitative avec spécifications détaillées des architectures et des modes de réalisation matérielle et logicielle) est extrêmement large :

- procédés industriels,
- industries manufacturières (robots...),
- transport (ferroviaire, ascenseurs)
- médical.

Le projet actuel (environ 350 pages) devrait être soumis au vote final en janvier 1996, mais il est loin de faire l'unanimité, en particulier en raison de son aspect difficilement applicable car s'adressant à trop de domaines. Le SC 65 A a mandaté un groupe de travail, le "Task Force C" pour en tirer une version adaptée et directement applicable aux procédés industriels, notamment de la chimie. Les participants français sont AEG-SCHNEIDER AUTOMATION et INERIS. Un renfort de participants "utilisateurs" serait le bienvenu. La prochaine réunion se tiendra à Paris du 6 au 8 décembre 1995.

Les objectifs sont d'établir un Committee Draft pour 1996.

C. Divergences actuelles

Aussi bien l'ACOS (Advisory Committee on Safety) du CEI que le CENELEC via le TC 44X (9) ont exprimé leur inquiétude concernant des divergences entre les deux projets de norme. Le projet international actuel devrait être publié comme une norme générique ou pilote. Chaque secteur technique ayant à établir des dispositions détaillées spécifiques à son domaine professionnel serait obligé de s'appuyer sur cette norme. A titre d'exemple, lorsqu'il n'existera pas de norme spécifique sur la sécurité des logiciels, cette norme devrait être appliquée directement.

Les constructeurs d'équipements s'inquiètent (10) également de cet état de fait qui pourrait les conduire à devoir développer une double ligne de produits (conformes à EN 954 et conformes à CEI 1508) tant que les projets coexisteront sous la forme actuelle.

V. CONCLUSIONS POUR LES AUTOMATES PROGRAMMABLES

Un référentiel d'évaluation intégrant les démarches qualitatives et quantitatives du projet international CEI 1508 est bien adapté au cas des automates programmables de sécurité, avec des prescriptions en terme de modes de réalisation relativement souples pour les constructeurs, mais en spécifiant des objectifs chiffrés de performance en terme d'intégrité de sécurité (les SIL) aussi bien qu'en terme de disponibilité de l'installation ou du procédé concerné. Un tel référentiel a été réalisé par l'INERIS, qui a pu le valider sur des équipements industriels, en collaboration avec AEG SCHNEIDER AUTOMATION et SIEMENS, et grâce au soutien de l'INRS.

Ce référentiel n'est pas applicable directement pour valider la conformité d'un automate de sécurité aux catégories telles qu'elles sont spécifiées dans la version actuelle du projet EN 954, dans lequel on ne trouve pas de quantification de niveaux de sécurité.

Le projet européen en cours de montage dans le cadre du programme "Normes, Mesures Essais" vise entre autre à réduire les divergences entre les deux projets CEI 1508 et EN 954.

RÉFÉRENCES

1) R. MARTIN et N. TOURTI - qui fait quoi : sécurité des machines Grand Programme de Normalisation "Hygiène et sécurité du travail, AFNOR, Edition juin 1995

2) Aspects juridiques de la normalisation et de la réglementation technique européenne, Eyrolles (1994, ISBN 2-212 03149-1).

3) Memorandum sur la normalisation en matière de santé et de sécurité destinée à appuyer les directives "nouvelle approche" : application au domaine des machines E 09-000, Avril 1993, AFNOR

4) B. PIQUETTE et JP PINEAU - Travailler en sécurité en atmosphère explosive, Préventique et Sécurité, supplément Sciences et Techniques n° 20 mai-avril 1996 5-7

5) J.L. DURKA et Ph. VILLENEUVE de JANTI, Communication à PREVENTECH, Paris 1995. Evaluation des systèmes électroniques programmables relatifs à la sécurité des installations industrielles dans le contexte des nouvelles normes.

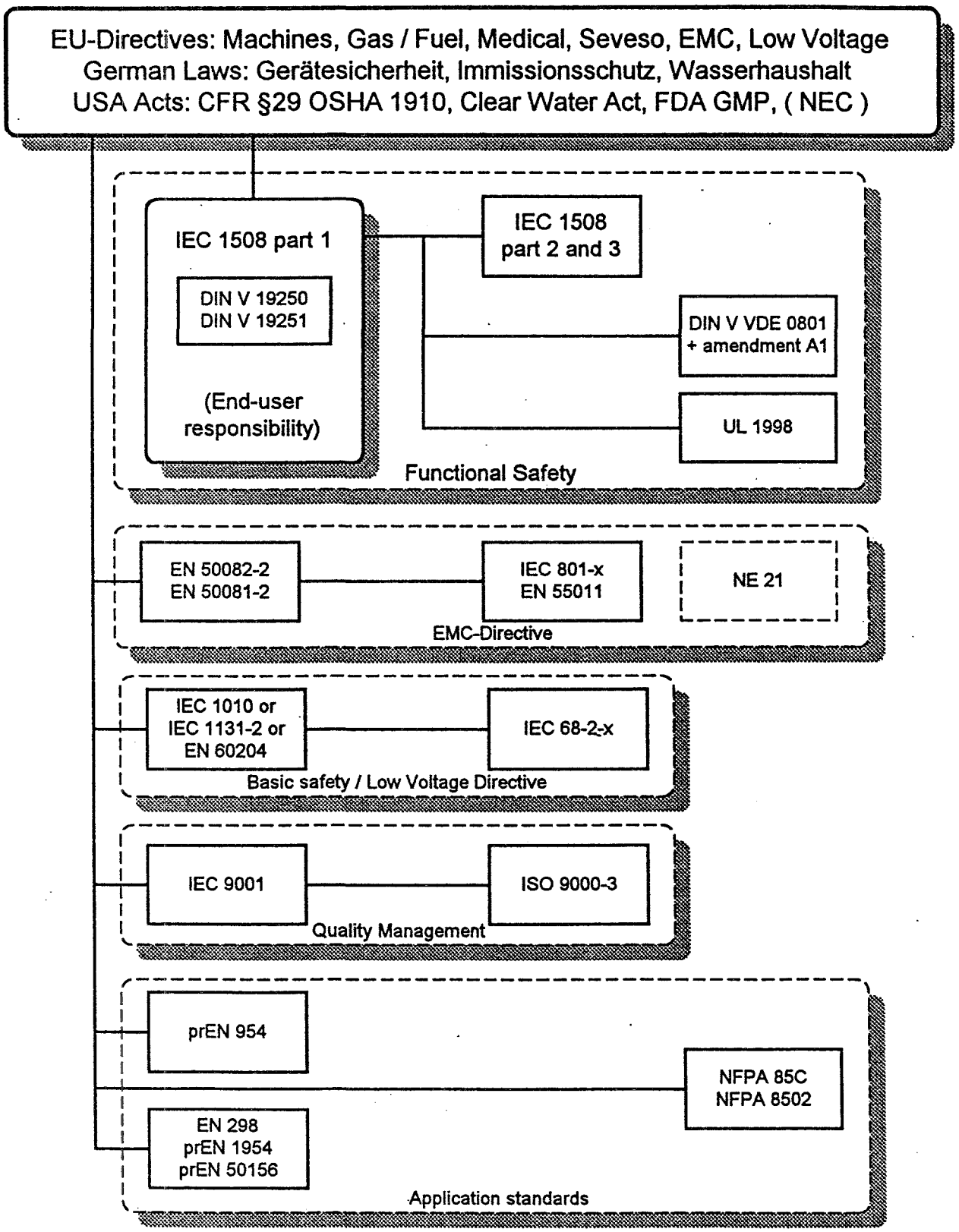
6) J.L. DURKA et Ph. VILLENEUVE de JANTI, Communication à AUTOMATION 95, Paris, 1995. Exigences techniques pour les systèmes dédiés à la sécurité comme définies dans les projets de normes actuelles.

7) Journée INRS sur les catégories, Nancy, 12 octobre 1995
- JP. VAUTRIN : "Sécurité des Machines, le concept de catégorie"
- P. CHARPENTIER : "Question posée par la validation des catégories 2, 3 et 4"
- J.P. LACORE : "La notion d'état de la technique dans l'esprit de la nouvelle approche".

8) J.L.DURKA, E. FAÉ, Ph. VILLENEUVE de JANTI. Evaluation du niveau de sécurité d'automates programmables, gestion de la sécurité des installations industrielles, Préventique Sécurité, supplément Sciences et Techniques", n° 23, septembre - octobre 1995.

9) Document GR TN E du 27/09/95 de M. HARLESS (SIEMENS) animateur du CENELEC/TC 44X/CAG et représentant du CENELEC au CEN/BTS2

10) WORKSHOP ACOS, Chicago, septembre 1995



TÜV Product Service GmbH
Industrial Electronics Division, IQSE
Ridlerstraße 31
D-80339 München
Phone: +49/89/5791-1801; Fax: -2393