Circulaire Ministérielle du 10 mai 1995

Aux Préfets et DDE

Relative à la sûreté de fonctionnement des systèmes numériques programmés utilisés dans les appareillages de sécurité des installations de remontées mécaniques et annexe.

L'utilisation des systèmes numériques programmés tend à se généraliser sur les remontées mécaniques, tant pour la construction d'installations neuves que pour la rénovation des installations existantes. Cette utilisation évolue vers le traitement par les systèmes numériques programmés de toutes les fonctions de sécurité.
Dans ces conditions, il est apparu que les règles suivies jusqu'à présent pour respecter les prescriptions des articles 2.8211 et 2.8212 de l'instruction du 17/05/1989 concernant la construction et l'exploitation des téléphériques à voyageurs devaient être complétées et précisées.
En conséquence, j'ai décidé d'arrêter et de rendre applicables dès la campagne de construction de 1995 les prescriptions annexées à la présente circulaire qui s'ajoutent à l'instruction susvisée.

ANNEXE:

Dès lors que dans un appareillage de sécurité des systèmes numériques programmés réalisent seuls une fonction, ils doivent respecter les prescriptions suivantes:

1 - Prescriptions générales:

1.1 - Concernant la démontrabilité de la sécurité, il est préférable de séparer nettement les systèmes numériques programmés réalisant des fonctions de sécurité de ceux réalisant des fonctions de commande.
Toutefois, si cette séparation n'existe pas, le processus de conception et de validation devra respecter les prescriptions définies dans la présente annexe à moins de prouver que des techniques efficaces sont utilisées pour éviter la "pollution" entre les systèmes à vocations différentes.

1.2 - Les systèmes numériques programmés choisis ainsi que tous les outils utilisés dans la chaîne d'élaboration des logiciels (outils de développement, de compilation, d'édition de lien et de chargement) doivent être largement éprouvés et faire l'objet d'une reconnaissance à l'échelle nationale ou internationale.
Les justifications correspondantes sont à apporter sous la forme soit d'un "certificat de validation" par un organisme reconnu par le service du contrôle soit de références produites par le constructeur des systèmes numériques programmés.

1.3 - Domaine d'exclusion relatif au 2ème frein de sécurité défini à l'article 2.73 de l'instruction du 17/05/1989:
Au moins une commande d'arrêt obtenu par le 2ème frein mécanique de sécurité doit être réalisée exclusivement avec des composants électromécaniques câblés. Cette commande doit être à la disposition du personnel et ne doit pas dépendre de systèmes numériques programmés.

2 - Prescriptions concernant le matériel:

2.1 - Toutes les défaillances ou combinaisons de défaillances qui auraient des conséquences critiques concernant la sécurité des personnes transportées ou empêcheraient la remontée mécanique de rejoindre immédiatement son état de sécurité doivent avoir une probabilité horaire d'apparition inférieure à 10(-9).
Seules sont à prendre en compte les défaillances ou combinaisons de défaillances comprises entre l'entrée et la sortie du système ou de l'assemblage de systèmes numériques programmés formant l'appareillage de sécurité.

2.2 - Le constructeur doit prouver la conformité de son produit à la prescription précédente par une étude qui prend en considération:
- le mauvais fonctionnement et les détériorations dus à des causes externes,
- les défaillances multiples et les défaillances dormantes,
- l'efficacité des moyens de surveillance et d'alarme; ceux-ci sont, d'une part, les moyens prévus par le constructeur des systèmes numériques programmés et rendus actifs par l'application concernée et, d'autre part, ceux que définit le constructeur de remontées mécaniques et qui, de ce fait, dépendent de l'architecture adoptée et du processus,
- la possibilité d'erreur pendant la maintenance propre du produit,
- l'efficacité, dans la mesure du possible, des actions correctives apportées par les opérateurs.
Dans cette étude, les taux de défaillance utilisés pourront être considérés comme constants.
Cette étude, pour la configuration adoptée, doit faire clairement apparaître les préconisations de câblage et/ou de programmation nécessaires pour atteindre l'objectif de sécurité. Elle doit être validée par un organisme indépendant du constructeur et reconnu compétent par le service du contrôle.

2.3 - Le constructeur doit présenter un dossier relatif aux tests périodiques servant à atteindre l'objectif de sécurité défini ci-dessus ainsi qu'aux tests annuels servant à garantir la pérennité du niveau de sécurité obtenu. Ce dossier doit définir les éléments de l'appareillage concernés par les tests et préciser la nature, la périodicité et l'efficacité des tests.

3 - Prescriptions concernant les logiciels.

3.1 - La sûreté de fonctionnement des logiciels "utilisateur" est réputée acceptable dès lors que :
- leur conception et leur développement respectent un Plan Qualité Logiciel équivalent à celui défini dans le fascicule de documentation AFNOR Z 67.130,
- un plan de développement et un plan de validation sont définis et suivis,
- les équipes de développement, de validation et de contrôle sont indépendantes,
- l'objectif de test défini est le plus proche possible des 100% et que le respect de cet objectif est évalué,
- un organisme indépendant du constructeur et accepté par le service du contrôle vérifie:
* la cohérence des dossiers de conception et de validation issus du cycle de développement,
* l'exhaustivité des tests prévus,
* la bonne écriture du code.
Le constructeur remettra l'ensemble des dossiers de développement de ces logiciels.

3.2 - La sûreté de fonctionnement des logiciels "résident" est réputée acceptable dès lors que leur conception et leur développement respectent un Plan Qualité Logiciel similaire à celui défini dans la fascicule Z 67.130. Le constructeur remettra les documents décrivant l'organisation mise en oeuvre par le(s) fournisseur(s) des systèmes numériques programmés pour le développement des logiciels "résident".

4 - Préconisation.

En référence à la norme EN 60 204, il est rappelé que, dans une architecture faisant appel à plus d'un système numérique programmé pour assurer une fonction dans le but d'acquérir un niveau de sécurité suffisant, l'utilisation de systèmes différents ou fonctionnant selon des principes différents peut réduire la probabilité de défaillances ou de pannes susceptibles de présenter un risque.