FORUM ISA-FRANCE 2007
AUTOMATION TECHNOLOGY TRENDS
Les mercredi 9 mai et jeudi 10 mai 2007, à Nice

# Functional safety in industrial communications

**Valérie DEMASSIEUX**
***Convenor IEC SC65C/WG12 « Functional Safety for Fieldbus »***
Rockwell Automation
2, rue René Caudron - Bât A
78960 Voisins-le-Bretonneux – FRANCE

**Mots clés :** *systèmes de sûreté, sécurité fonctionnelle, norme CEI 61784-3, norme CEI 61508, profils de communication.*

Le développement des *systèmes de sûreté* a historiquement suivi un cours semblable à celui emprunté lors de la mise en œuvre des systèmes de contrôle commande standards, où l'utilisation d'équipements programmables et en réseau a permis de satisfaire aux exigences croissantes de complexité et de flexibilité des applications d'automation. Ainsi, la réalisation de *réseaux dédiés sûreté* a permis aux *systèmes de sûreté* de bénéficier des mêmes avantages en terme de réduction du câblage, de facilité de configuration et de possibilités accrues de diagnostic.

La norme CEI 61784-3 définit des principes communs pour la transmission de *messages de sûreté* entre les participants d'un réseau distribué utilisant la technologie *fieldbus*, selon les exigences de la CEI 61508 pour la *sécurité fonctionnelle*. Ces mécanismes sont conçus pour assurer la fiabilité nécessaire du transport d'information via un *fieldbus* dans un *système de sûreté*, ou bien apporter suffisamment de garanties d'un comportement sûr en cas de défaillance du *fieldbus*.

La CEI 61784-3 définit plusieurs *profils de communication de sécurité fonctionnelle*, basés sur des *profils de communication fieldbus* de la série CEI 61158. Ces profils emploient l'approche « canal noir » de la CEI 61508, supposant un média « peu fiable ». Ils spécifient donc une « *couche de communication sûreté* » supplémentaire, qui exécute toutes les mesures nécessaires à la transmission des données de sûreté en accord avec la CEI 61508.

***Key words:*** safety systems, functional safety, IEC 61784-3 standard, IEC 61508 standard, communication profiles.

Safety system development has historically followed a similar path to standard control system development, where programmable and networked equipment has fulfilled increasing complexity and flexibility requirements of automation applications. The development of safety networks has brought similar benefits to safety systems, including reduced wiring, ease of configuration and extended diagnostics capabilities.

IEC 61784-3 defines common principles for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 for functional safety. These mechanisms are intended to provide the necessary confidence in the transportation of information on a fieldbus in a safety system, or sufficient confidence of safe behaviour in the event of fieldbus failures.

IEC 61784-3 specifies several functional safety communication profiles, based on fieldbus communication profiles of the IEC 61158 series. These profiles use the “black channel” approach of IEC 61508, assuming an “unreliable” media. Therefore, they specify an additional “safety communication layer”, which performs all the measures necessary to implement transmission of safety data in accordance with IEC 61508.