Villeurbanne, mardi 20 octobre 2015

Cybersécurité et sûreté de fonctionnement : ISA99 versus ISA84

Jean-Pierre Hauet

Associate Partner KB Intelligence – Président ISA-France

10 rue Lionel Terray – 92500 Rueil-Malmaison)

Tel : 33 1 41 29 05 09 E-mail : Jean-pierre.hauet@kbintelligence.com

Mots clés : *Sécurité fonctionnelle, sûreté de fonctionnement, cybersécurité, systèmes instrumentés de sécurité (SIS)*

Sûreté et *cybersécurité* font partie du langage courant de la sécurité industrielle. Cependant le concept de sûreté est, dans la langue française, relativement imprécis et emprunte, dans de nombreuses acceptions, à celui de sécurité. L'une des déclinaisons de ce concept est celle de « *sûreté de fonctionnement* », qui demeure une notion très générale mais qui trouve un sens plus précis dans la « *sécurité fonctionnelle* des systèmes électriques/électroniques et électroniques programmables », objet des normes ISA84, IEC 61508 et IEC 61511. Malheureusement, ce terme reste peu employé.

La *cybersécurité* découle directement du concept anglo-saxon de *cybersecurity* et revêt une définition plus précise. Elle fait l'objet de l'ISA99 devenue l'IEC 62443.

La présentation s'efforcera en introduction de préciser ces problèmes de terminologie.

Elle analysera ensuite les points communs et les différences entre sûreté de fonctionnement et cybersécurité, au regard de différents critères :

- L'origine des dommages (causes fortuites, systémiques ou aléatoires) ;
- Les conséquences possibles de ces dommages (matérielles, logicielles, incorporelles) ;
- Les échelles de temps (court terme, long terme)
- Les mesures de nature à renforcer le niveau de confiance au regard des deux critères (la sûreté renforce-t-elle la cybersécurité, la cybersécurité peut-elle porter préjudice à la sûreté, existe-t-il des architectures tolérantes aux pannes et résistantes aux cyberattaques ? etc.)

Les comités ISA-99 et ISA-84 ont entamé un rapprochement entre les cycles de vie des deux concepts qui est exposé dans le projet de rapport technique ISA –TR84.00.09.

Ce rapprochement est souhaitable au niveau des analyses de risques, les conséquences dommageables d'une défaillance ou d'une attaque pouvant in fine être les mêmes.

Au niveau de la conception des SIS (Systèmes Instrumentés de Sécurité), la question se pose de savoir jusqu'où ils peuvent partager, sur le plan fonctionnel ou matériel, des composant communs avec le BPCS (Basic Process Control System). L'ISA84 a manifestement une position plus ouverte que l'ISA99 qui prescrit de faire des SIS des zones de sécurité distinctes. Entre ségrégation et intégration, il y a débat.

La question se trouve également posée de savoir si le risque cybersécuritaire peut être considéré comme l'un des risques destinés à être couverts par l'ISA84 et l'IEC 61508 (dûment amendées pour le prendre en compte) ou bien si, compte tenu notamment du recouvrement avec la cybersécurité de l'informatique de gestion, il est préférable de lui conserver son caractère spécifique.