Performance des Systèmes Instrumentés de Sécurité (SIS) : Evaluation et problématiques de la tolérance aux fautes

Michel Chandevau
Senior Member ISA
ISA Leader ISA France
mchandevau@yahoo.fr

Mots-clés : *haute disponibilité, intégrité de sécurité(SIL), systèmes E/E/PES, tolérance aux fautes, redondance, diagnostics, sécurité fonctionnelle, normes IEC 61508 & IEC 61511*

Les exigences en termes de fiabilité et de disponibilité des Systèmes Instrumentés de Sécurité (SIS) s'inscrivent dans un contexte de performance globale tant d'intégrité de sécurité que de productivité industrielle, les enjeux techniques et économiques étant multiples.

La prise en compte des modes de défaillance de ces systèmes et de leurs incidences sur les procédés contrôlés permet une réduction importante des risques potentiels, les architectures utilisées étant fondées sur des topologies dotées de redondances matérielles plus ou moins complexes excluant tout défaut de mode commun. La recherche de systèmes (SIS) à « haute disponibilité » (*High Availaibility*), présentant un degré élevé de sécurité (*High Integrity/Safety*) caractérisé par une probabilité moyenne de défaillances (sur demande) faible (PFD Avg) conduit à l'utilisation de systèmes *Electric/Electronic/Programmable Electronic Safety* (E/E/PES) comportant des architectures « tolérantes aux fautes » (HFT/*Hardware Fault Tolerant*) utilisant des techniques de diagnostic et de test permettant la détection, l'identification et la localisation des défauts.

L'apport d'indicateurs quantitatifs aux diverses analyses de fiabilité et de sécurité des SIS, telle que la fraction de défaillances sûres (SFF), facilite l'adaptation des contraintes architecturales de tolérance aux fautes aux niveaux d'intégrité (SIL) recherchés. Outre ce paramètre « SFF», les taux de couverture en diagnostic (*Diagnostic Coverage /DC*) sont déterminants quant à la capacité de détection des défaillances (dangereuses ou non) de ces systèmes « critiques », leur assurant une disponibilité optimale, l'accroissement du taux de couverture (DC) augmentant considérablement le MTTF.

D'autre part, les normes IEC 61508 et IEC 61511, véritables outils normatifs de la « sécurité fonctionnelle », permettent, à partir du cycle de vie de tels systèmes (SIS), d'analyser et de réaliser toutes les phases indispensables à leur conception, leur réalisation et leur exploitation. Les Systèmes Instrumentés de Sécurité (SIS) relevant de ces normes doivent répondre aux divers niveaux de protection (de SIL1 à SIL4) définis dans un contexte de « risque tolérable », le facteur de réduction de risque (RRF) lié aux niveaux des SIL impliquant une parfaite adéquation entre les fonctions instrumentés de sécurité (SIF) et les spécifications requises (SRS). L'optimisation de la performance des SIS, qui reste un objectif majeur pour le concepteur comme pour l'utilisateur, s'effectue sous la contrainte des niveaux d'intégrité de Sécurité (SIL). Elle doit intégrer tous les éléments de la boucle de sécurité ainsi que les « incertitudes » des modèles de fiabilité des SIS, ceux-ci pouvant afficher certaines disparités selon les méthodes de calculs utilisées pour l'obtention des taux de défaillance (PFD), équations simplifiées, arbres de défaillances (FTA), réseaux de Markov.

Des méthodes nouvelles sur l'estimation des « imprécisions » des calculs des taux de défaillances par des approches floues (nombres flous/ réseaux de Markov flous, α-coupes, etc.) ont été également proposées, ce qui montrent que les problématiques liées à la performance de Systèmes Instrumentés de Sécurité restent nombreuses et complexes et méritent attention. Elles sont analysées dans un article à suivre qui explicitera toute l'importance de la tolérance aux fautes et des diagnostics dans la sûreté de fonctionnement de ces systèmes.