

Villeurbanne, mardi 20 octobre 2015

Comment concevoir et valider un applicatif dédié à la sécurité d'un process ?

Philippe Primard

Responsable Systèmes de Sécurité

Yokogawa France, 17, rue Paul Dautier 78147 Vélizy Villacoublay

Mots clés : *système de gestion de la sécurité fonctionnelle, normes, qualité logicielle*

La gestion de la sécurité fonctionnelle couvre toutes les activités qui garantissent le niveau de sécurité fonctionnelle attendue. Les entreprises qui réalisent des systèmes de sécurité doivent répondre à des spécifications techniques mais également à des contraintes de gestion et d'organisation.

Si la partie matérielle est relativement simple (essentiellement liée aux composants utilisés et leur association), la partie logicielle (applicatif) est plus délicate. La solution pour garantir que toutes les activités sont exécutées correctement consiste en l'application d'un *Système de Gestion de la Sécurité Fonctionnelle (Functional Safety Management System - FSM)*, qui décrit toutes ces activités en conformité avec la normalisation.

Le *Système de Gestion de la Sécurité Fonctionnelle* est un aspect important des normes. Cela revient à appliquer un système qualité spécifique à la réalisation de projets dédiés à la sécurité et ce en faisant appel à du personnel spécifiquement compétent dans ce domaine.

Le FSM couvre à minima :

- Les concepts d'exécution pour garantir le niveau SIL requis basés essentiellement sur le plan de validation de la sécurité fonctionnelle : Safety Validation Plan (SVP),
- Les responsabilités des personnes impliquées,
- Les compétences et la formation de l'équipe d'ingénierie,
- La gestion des développements logiciels applicatifs,
- La gestion des tests et validation des logiciels applicatifs,
- Les moyens et techniques utilisés pour pallier aux erreurs,
- La gestion des informations et de la documentation,
- La gestion des vérifications, validations and évaluations de la sécurité fonctionnelle.

YOKOGAWA présentera son FSM et ses méthodes, outils et procédures qui garantissent la bonne exécution des projets de sécurité fonctionnelle. Une attention particulière sera portée sur le groupe d'experts sécurité indépendant "*Safety Assurance and Consultancy*" (SA&C), créé en 2001, pour assurer les services tels que la vérification des niveaux de SIL, les audits d'exécution de projet, les évaluations de la sécurité fonctionnelle, ... et ce en total indépendance de l'équipe de réalisation.

Key words : *Functional Safety Management System, standards, software quality*

Management of functional safety includes all activities to achieve the required functional safety. When companies have to deliver safety systems, they have to fulfill technical requirements, but also management and organizational requirements.

If the hardware part is easier to manage (essentially depending on used components and their combination), the software part (application) is more difficult. The solution, to guaranty that all necessary activities are executed correctly, is to apply a Functional Safety Management System (FSM), which describes all activities as defined in safety standards.

Functional Safety Management is a significant aspect of standards. It means that you apply a specific quality management system on the safety projects execution and that you employ safety competent engineers.

SFM covers at minimum:

- Description of safety concept to achieve required SIL level of functional safety mainly by a Safety Validation Plan (SVP)
- Responsibility of involved persons
- Competence and training of safety engineering team
- Software development management
- Software tests and validation management
- Measures and techniques used to prevent and correct mistakes
- Information management and documentation
- Verification, validation and assessments management

YOKOGAWA will present its FSM and applied methods, tools and procedures to guaranty good project execution in accordance with the safety standards. A specific independent safety expertise group "Safety Assurance and Consultancy" (SA&C), created in 2001 provides safety consultancy services like SIL verification studies, audit, assessments, site validations, etc. independently from the project execution team.