Sûreté et cybersécurité : comment concilier deux objectifs essentiels de la sécurité industrielle

Villeurbanne, mardi et mercredi 18 et 19 octobre 2016

Assurer sûreté et cybersécurité sur des logiciels industriels complexes à l'aide de technologies qualifiées

Jean-Louis Camus

ANSYS - Esterel Technologies Safety Manager

Tel : 06 08 17 11 47
9 rue Michel Labrousse, 31100 Toulouse

Email: jean-louis.camus@ansys.com

Mots clés : *Safety, security, real time, embedded, software*

Dans le domaine des logiciels industriels de type contrôle-commande-supervision, la sûreté de fonctionnement était jusqu'à une époque récente une problématique relativement isolée de la problématique sécuritaire. L'interconnexion des systèmes et surtout leur ouverture plus ou moins maîtrisée vers le monde extérieur ne permettent plus cette séparation.

Si des techniques spécifiques de développement/vérification de noyaux sécuritaires existent désormais, elles sont difficilement applicables à des parties applicatives de plusieurs dizaines de milliers de lignes. La présentation montrera comment il est possible de développer des logiciels industriels complexes par une structuration en couches. Elle développera plus particulièrement comment concevoir et développer des parties applicatives complexes par une approche qualifiée « basée modèle» grâce à la chaîne d'outils SCADE dédiée aux systèmes temps réels critiques. Celle-ci met en jeu :

- Une notation graphique à base sous-jacente formelle pour les logiciels réactifs temps réel ;
- Des outils d'édition, de vérification et de simulation de ces modèles ;
- Une chaîne de génération qualifiée pour les niveaux les plus exigeants des standards de sûreté (IEC 61508 SIL3, DO-178C DAL A, ISO 26262 ASIL D) ;
- Un outillage de test.

Le processus d'analyse et de développement de ce type de logiciel selon une approche « basée modèle » sera décrit et illustré par des exemples.