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

Villeurbanne, mardi et mercredi 18 et 19 octobre 2016

Intégrer les enjeux de la cybersécurité aux démarches existantes de sécurité fonctionnelle dans le domaine des véhicules connectés

Florian Stosse
Apprenti-ingénieur sécurité informatique
florian.stosse@fr.bureauveritas.com

Franck Sadmi
Chef de projet sûreté de fonctionnement
franck.sadmi@fr.bureauveritas.com

Bureau Veritas
60, Avenue du général De Gaulle
92046 Paris La Défense

Mots clés : *Automobile, cyber sécurité, sûreté de fonctionnement, ISO26262*

L'objectif de cette intervention est d'introduire le travail effectué conjointement depuis novembre 2015 par le service Sûreté de Fonctionnement de Bureau Veritas, groupe leader mondial dans l'évaluation de la conformité et la certification, et la société Devoteam, entreprise de services du numérique spécialisée en sécurité et conseil IT.

Ce partenariat ambitionne de rédiger sous la forme d'un guide une solution pratique et concrète d'intégration de la cyber sécurité dans le cycle de développement des véhicules, notamment en accompagnant les démarches existantes préconisées par la norme ISO26262 : 2011 («Véhicules routiers – Sécurité fonctionnelle»).

La méthodologie que nous proposons doit permettre une utilisation aisée et complémentaire aux bonnes pratiques actuelles. Le fondement de cette méthodologie est une approche par analyse de risques ainsi que le rapprochement entre safety (sécurité fonctionnelle) et cyber sécurité depuis les toutes premières étapes du développement système (conception des systèmes de détection des attaques, architecture robuste aux attaques logicielles) jusqu'aux phases de validation et de production (alertes en temps-réel).

Notre démarche trouve naturellement sa place au sein de la norme ISO 26262 :

1. Chapitre 3-7 et Chapitre 9 (analyse des risques) → intégration des cyber-risques dans la démarche ASIL (nouvelles menaces et vulnérabilités, impacts étendus, notion d'enchaînement de vulnérabilités).
2. Chapitres {4,5,6}-{6,7} : exigences de sécurité et design adaptés aux spécificités de ces risques.
3. Chapitres 4-8, 5-10, 6-9 et 6-10 → ne pas se limiter à des tests fonctionnels simulant un dysfonctionnement, mais simuler également des actes de malveillance ou leurs conséquences, ce qui implique la prise en charge d'une partie des tests par des experts en cybesécurité.
4. Chapitre 7 (production) → mise en place de dispositifs de détection, d'alerte et de remédiation en temps réel.