ISA France Section

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

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

Villeurbanne, mardi et mercredi 18 et 19 octobre 2016

Three tentative criteria for the successful industrialisation of safety and security engineering tools

Synthèse du projet ITEA "Merge"

Letitia Li (doctorante Telecom Paristech)

Email: letitia.li@telecom-paristech.fr

Mots clés : *Safety, Security, Co-engineering, Tools*

Safety and security co-engineering is emerging as an industrial need for the development of most safety-critical systems, throughout many domains (avionics, rail, nuclear, etc.) To support this, new methods and tools are needed, and are effectively emerging. After performing an extensive state of the art of the domain, we propose three criteria that we believe such methods and tools should respect to be successfully accepted within legacy and industrial engineering frameworks:

- (i) Intermediate safety and security work products can be shared between the two engineering specialties as long as the vernacular is maintained for each specialty;
- (ii) Work on common safety and security work products should be transparent for each specialty, except in case of conflict / inconsistencies
- (iii) New tooled-up approaches should be implemented as add-ons to existing (standard) processes, with added-value related to formal analyses, and without significant negative side-effects, incl. extra workload.

We illustrate our case on two tools: an ad-hoc safety and security engineering academic prototype, and the extension of an existing industrial tool, which was initially dedicated only to safety-engineering.