Feature-based software architecture analysis to identify safety and security interactions

Oum El Kheir Aktouf*[1]

[1]LCIS – Institut National Polytechnique de Grenoble - INPG – France

Résumé

In the automotive domain, feature-based software architecture is a widely used software design method to produce cost efficient and reusable software. With increasing complexity of automotive systems and the shift towards automated driving, safety and security measures become even more crucial for these systems. However, safety and security functionalities can undermine each other if they interact in unintended ways. We propose the novel method FIISS for automatic identification of interactions between safety and security features in UML models. We evaluate our implementation of the method by applying it to a real-world component for autonomous driving. We show that the method is able to identify unintended interactions while providing only few false positive findings. Thus, we see that our method can be applied to real-world UML system designs without modifying the underlying models and without applying specialized UML profiles.

*Intervenant