Toward Better Integration of Functional and Dysfunctional Models: Safety Architect.

Frédérique Vallée [1], Anne-Catherine Vié [1], Jonathan Dumont [1], Nataliya Yakymets [2], Yupanqui Munoz Julho [2] and Agnès Lanusse [2]

Abstract As systems are becoming more complex, their safety assessment dramatically needs powerful tools. Most of the existing tools are poorly connected to the system design process and cannot be associated at early stages of development cycle. We introduce a model-based safety analysis (MBSA) methodology and its supporting tool: Safety Architect that permits better interactivity between design and safety assessment activities. A dysfunctional model is built from the system model described in SysML. It is used to specify possible failure-modes, mitigation barriers and propagation behavior at components level. From the specification of feared events (expressed in safety requirements), it can automatically produce propagation paths and highlight which components are potentially critical. Such critical paths related to feared events can be displayed on the system model for better understanding of failure sources. This cooperative safety analysis framework relies on the Papyrus modeling tool exploiting both its system modeling and advanced customization facilities.

[1] ALL4TEC, 2-12 rue du chemin des Femmes, Odyssée E, 91300 Massy, France
frederique.vallee@all4tec.net,anne-catherine.vie@all4tec.net, jonathan.dumont@all4tec.net

[2] CEA Saclay Nano-INNOV, Institut CARNOT CEA LIST, DILS,PC174 and CEA, LIST, Laboratory of Model Driven Engineering for Embedded Systems, 91 191 Gif sur Yvette CEDEX, Saclay, France - nataliya.yakymets@cea.fr, yupanqui.munozjulho@cea.fr, agnes.lanusse@cea.fr