Ongoing Work on Domain-Specific Modeling for Early Design Evaluation with the Help of Formal Methods for Correctness and Completeness Guarantees

Gurvan Le Guernic*†[1], Hubert Godfroy[2], Pierre Kimmel[2], Abdelghani Alidra[3], and Antoine Beugnard[3,4]

[1]DGA Maîtrise de l'information Université de Rennes (DGA.MI) – Direction générale de l'Armement (DGA) – Route de Laillé. La Roche Marguerite - 35170 - Bruz, France

[2]Capgemini – Capgemini – France

[3]Département Informatique (IMT Atlantique - INFO) – IMT Atlantique – IMT Atlantique - Campus de Brest - Technopôle Brest-Iroise CS 8381829238 BREST Cedex 3, France

[4]Lab-STICC – Lab-STICC UMR CNRS 6285, Brest – France

Résumé

The DGA is involved in the development of sensitive devices that may require the evaluation by the contracting authority (MOA) of early design decisions made by the prime contractor (MOE). The exchange of information for this evaluation is traditionally based on documents (bearing resemblance to Common Criteria documentation) and face-to-face meetings. DGA experiments on using Model-Based System Engineering and Formal Methods to improve the correctness and completeness of information exchanged at this stage, in order to improve the efficiency and quality of this early design evaluation. This talk will first quickly introduce the audience to the Network Pump of the NRL, a realistic use case representative of the type of sensitive devices dealt with by the DGA, and for which a large amount of information is openly accessible. It will then present the objectives and current state of an ongoing project by the DGA to develop a dedicated (domain specific) modeling environment for this task of early design evaluation. The current prototype allows modeling different "views" of the early design for which the tooling provides various algorithms providing guarantees regarding the completeness and correctness of those views. The talk will conclude by presenting the limitations and open questions in the current state of this work.

*Intervenant

†Auteur correspondant: gurvan.le_guernic@inria.fr