Robustness testing of embedded systems by controlled disturbance simulation from virtual platforms

Contact

Yves LHUILLIER: yves.lhuillier@cea.fr desk phone: +33 (0)1 69 08 23 07

Daniel CHILLET: daniel.chillet@irisa.fr desk phone: +33 (0)2 96 46 90 69

Context

CEA is a public multidisciplinary research organization whose research fields range from nuclear industry to biosciences and fundamental physics. It is made of several research centers located in France. CEA represents 15024 employees, 2.7 B Euros budget, 1689 patents registered or active, and 1300 contracts signed with industry. More than 80 new companies have been created since 1984 in high technologies sectors and 9 research centers (http://www.cea.fr/english). In HORIZON 2020, the EU Framework Programme for Research and Innovation, CEA is already involved in more than 100 projects.
The CEA LIST (Laboratory for Integration of Systems and Technology) institute is part of CEA TECH, the CEA Technological Research Division. CEA LIST combines basic research and industrial R&D and is primarily concerned with the development of technologies that combine software and hardware to form highly integrated complex systems. The research activities are structured into three major themes: embedded systems, interactive systems and sensors, and signal processing. CEA LIST focuses on methods and tools for the design of embedded systems with appropriate architectures, software, and an optimal level of safety.

In the context of embedded system, the design Systems-on-Chip (SoCs) is subject to large integration issues where more and more cores are included in each chips to form complex computing systems. However, this high integration leads the designer to consider the sensitivity of the circuit to faults. Furthermore, these systems are difficult to test due to their complexity, and they represent real risk in terms of vulnerability and security. In conclusion, these problems must be taken into account as soon as possible in the design flow, and the need of tools to simulate faulty systems is more and more critical.

Problematic

The development of embedded systems is subject to the ever-growing impact of hardware and software faults. The consequent failures gain importance due to (1) the massive use of digital system in our everyday life, (2) the increasing complexity of hardware and software designs and (3) the stress of cyber attacker.
Classical development methods show their limits with respect to these threats because most of development tools tend to restrict the model of environmental running conditions. In almost all cases, the software is developed under the assumption of a stable and secure hardware, this being generally ensured by mechanisms of redundancies more and more expensive. To reduce these risks, the use of virtual platforms makes it possible to understand where software can diverge from nominal execution and to develop software that is less sensitive to potential errors.

Subject

The objective of this thesis is to develop a virtual platform based environment for simulation of complex embedded system with rich and flexible fault/disturbance injection mechanisms. Using this environment, the software developer will be able to see how an embedded system may misbehave. Heavy faults may be easy to detect using watchdog timers or other similar mechanisms, yet some more malicious faults may leave the system in such a state that it appears to work correctly whereas the consequences may be dramatic.
Because the platform intends to inject any kind of errors and not only necessarily realistic hardware faults, the more general disturbance term is used. For this, we propose to setup to disturbance injections in the virtual platform. The first is a low-level disturbance injector capable of directly altering values manipulated by machine instructions in the CPUs. The second disturbance injector will act at software

boundaries by affecting values corresponding to identify source code values (e.g. parameter or return values of functions).
Finally, to understand and monitor precisely how software diverges during disturbed execution, a difference tool will be developed with the aim of producing the most concise and comprehensive difference log of two analyzed traces. This tool will allow understanding how some errors may be almost invisible for several cycles of computations and how to detect them as early as possible.

Organization

The PhD is in the framework of a DGA/CEA PhD thesis. The PhD takes place in a collaborative environment between Leading French Public Research Institutes (CEA, DGA and INRIA). Candidate will be mainly located in CEA Nano-INNOV (Paris Saclay campus). Within CEA, the candidate will leverage the virtual platform expertise and tools provided by the UNISIM-VP team with whom the student will work.
UNISIM-VP (http://unisim-vp.org [6]) stands for "UNISIM Virtual Platforms", a full-system simulation environment that is cross-platform Open source software based on industry standard SystemC. UNISIM-VP provides several Virtual platforms at transaction level of modeling and a framework to ease the development of new virtual platforms.

Application deadline: 1/06/2019

References

[1] G. Foucard, 《 Taux d'erreurs dues aux radiations pour des applications implémentées dans des FPGAs à base de mémoire SRAM : prédiction versus mesures 》. Thèse de doctorat en micro et nano électronique, Laboratoire TIMA, Université de Grenoble, Juin 2010

[2] P. Hazucha and C. Svensson, 《 Impact of CMOS Technology Scaling on the Atmospheric neutron Soft error Rate". IEEE TRANSACTIONS ON NUCLEAR SCIENCE, VOL. 47, NO. 6, DECEMBER 2000

[3] H. Amrouch, P. Krishnamurthy, N. Patel, J. Henkel, R. Karri, and F. Khorrami, "Special Session: Emerging (Un-)Reliability Based Security Threats and Mitigations for Embedded Systems". In Proceedings of CASES, Seoul, Republic of Korea, October 15-20, 2017 (CASES'17), 10 pages. DOI: https://doi.org/10.1145/3125501.3125529

[4] A. Dessiatniko, 《 Analyse de vulnérabilisées de systèmes avioniques embarquées : classification et expérimentation 》, Thèse de doctorat, Laboratoire d'Analyse et d'Architecture des Systèmes, Université de Toulouse, Juillet 2014

[5] M. Kooli, G. Di Natale, 《 A Survey on Simulation-Based Fault Injection Tools for Complex Systems", 2014 9th IEEE International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS), 6-8 May 2014

[6] David I. August, Jonathan Chang, Sylvain Girbal, Daniel Gracia-Perez, Gilles Mouchard, David A. Penry, Olivier Temam, and Neil Vachhara-Jani. UNISIM: An open simulation environment and library for complex architecture design and collaborative development. Computer Architecture Letters, 6(2):45-48, 2007.