A model-driven integrated approach for cyber physical systems hardware and software dependability testing

Supervisors

Dr. Mohamed KAÂNICHE, LAAS-CNRS, senior researcher "Directeur de Recherche", Head of "Dependable Computing and Fault Tolerance" team

Prof. Guillaume AURIOL, LAAS-CNRS, INSA Toulouse, Associate Professor

Subject

Our work is aimed at developing a methodology and a framework to support the validation of critical cyber-physical systems based on a testing approach.

The cyber-physical systems (CPS) paradigm refers to a new generation of systems with tight interactions and coordination between computational and physical resources. CPS research involves both scientific works on control systems and computer science. These two communities master the development of their own powerful system science and engineering methods and tools. CPS research aims at integrating knowledge and engineering principles across the computational and engineering disciplines to develop new CPS science and supporting technology.

Hardware and software components need to be developed beyond existing technologies. They must be highly dependable, reconfigurable, and, most of the time, certifiable, from components to fully integrated systems. Such complex systems must deliver services with a high level of trustworthiness that is lacking today in many cyber infrastructures. Overdesign is currently the only path to achieve safe and successful system certification and deployment. This approach is rapidly becoming intractable for complex designs and for systems where the product costs must be drastically reduced. New models, algorithms, methods and tools that will incorporate verification and validation at every design stage of software and systems, are needed. In particular, the validation of CPS requires the integration of heterogeneous and hybrid models and testing mechanisms at different system abstraction layers, including both the hardware and the software. The main challenge is to provide a flexible and automated approach that will enable the efficient integration of all these components together, while achieving an optimal trade-off between the dependability level achieved and the associated cost.

This low cost and multidisciplinary environment will be taken into consideration in the proposed thesis for which two aspects will be investigated. The first one will focus on a definition of a system engineering-based methodology to drive design through test specifications. This work aims at providing a practical guidance to head engineers who only have limited expertise in safety design and computer science. We will propose a methodology to manage high-level models understandable by non-expert system designers, and to integrate these models in the early first steps of design. The second aspect deals with the design and development of a testing platform and software tools to improve CPS reliability. We will focus on building a low-cost reusable testing platform with high-level flexibility to provide a comprehensive test coverage for all the sensitive components of the embedded software.

Our work aims at facilitating the software verification and dependability analysis of CPS under various conditions (e.g. real-time constraints) by means of well-known techniques like hardware-in-the-loop and software-in-the-loop. The approach will be based on efficient techniques such as fault-injection, system

monitoring, and software emulation. In some previous works carried out in our team, we have developed a simple platform designed to test nanosatellites. This platform will be used to assess and validate the testing approach that will be developed during the thesis. If the PhD student has not computer science skills some trainers could be supervised to develop this part.

Related references

R.S. Baheti and H. Gill, "Cyber-physical Systems", Part 3: Cross-Cutting Research Directions in "The Impact of Control Technology", T. Samad and A.M. Annaswamy (eds.), IEEE Control Systems Society, 2011.

F. Yang, H. Yue, G. Wang, Q. Tu, and W. Wang, "The design and analysis of picosatellite deployer with controllable release function", International Conference on Information and Automation (ICIA), Macau, China, July 2017.

D. Selva and D. Krejci, "A survey and assessment of the capabilities of CubeSats for Earth observation", Acta Astronautica, vol. 74, pp. 50–68, 2012

C. A. P. L. Conceicao, F. Attiello-Francisco, and C. L. G. Batista, "Dependability verification of nanosatellite embedded software supported by a reusable test system", Seventh Latin-American Symposium on Dependable Computing, 2016

N. K. Ure, Y. B. Kaya, and G. Inalhan, "The development of a Software and Hardware-in-the-Loop Test System for ITU-PSAT II nano satellite ADCS", 2011 IEEE Aerospace Conference, Big Sky, USA, pp. 1- 15, 5-12 March, 2011.

H. Waeselynck, Z. Micskei, N. Rivière, A. Hamvas, I. Nitu, "TERMOS: a formal language for scenarios in mobile computing systems", In: Sénac, P., Ott, M., Seneviratne, A. (eds.) MobiQuitous 2010. LNICSSITE, vol. 73, pp. 285–296. Springer, Heidelberg (2012).

About Toulouse

Toulouse is an affordable city, especially for students. Renting an accommodation in the private market is around €450, depending on where you live in Toulouse. Nonetheless, the transport cost is relatively cheap for people under 26. If you are under 26, you can have an unlimited annual access to bus, tramway and metro for €100. It is €10 for one month. If you do not use public transportation that much, you can buy a Pastel Card for €8 and fill it whenever you want. For 10 tickets, it will cost you only €4. Students aged between 26 and 35 are entitled to reduced prices: €9.8 for 10 tickets. Regarding food, students can enjoy a complete meal (entrance, main dish and dessert) for only €3.25, in every CROUS Restaurants (also called "Restaurant Universitaire" or RU). There are also cafeterias where student can buy sandwiches, quiches, hot meals, have a coffee break. Restaurants are opened every days, during dinner time as well. On the INSA campus, there is a restaurant and a cafeteria as well

About LAAS-CNRS

LAAS' research activities fall within the domain of Information Sciences and Technologies and address complex systems (artificial and sometimes natural) generally heterogeneous, and at different scales, to devise theories, methodologies and tools for modeling, designing and controlling them. Research, innovation and transfer are tied. The lab has a history of strong relationships with industry and works in a large number of collaborative projects with international, national and regional industries of all size. LAAS was one of the 20 first "Carnot Institutes" labeled in 2006. The systems considered in our research are of different kinds: integrated systems, embedded systems with real time and safety requirements, distributed systems, mobile

systems, autonomous and robotics systems, micro and nano systems, biological systems. They fall in various application domains such as aeronautics and space, telecommunications, transports, production, services, security and defense, energy management, healthcare, environment and sustainable development.

See https://www.laas.fr/public/en/tsf for more details on "Dependable Computing and Fault Tolerance" team.

About INSA

The school is located in Toulouse, more precisely in Rangueil, a large campus dedicated to scientific research and education. Toulouse is the second biggest student city in France. It only takes 15 minutes by metro to reach the main place of Toulouse, the Place du Capitole, which represents the very center of the "pink city". Enjoying a 20ha lively campus, INSA Toulouse is at the heart of a privileged environment thanks to its proximity with the Canal du Midi, which connects the Garonne river to the Mediterranean Sea, and provides a good place to study. Indeed, students can cycle along the Canal to reach the city center and enjoy a peaceful and natural environment in a vibrant city, in only half an hour. The campus also provides many facilities such as accommodation in safe small-rise buildings, restaurant services and sport and leisure facilities, adapted to high level athletes and musicians. Indeed, the school encourages its students to develop their gifts and talents that is why it offers an educational path adapted to high level musicians, dancers and athletes. Cultural initiative and responsible community projects are highly encouraged.

Expected collaboration

The "Centre Spatial Universitaire de Toulouse" is an organization to federate researches dealing with academic space systems. At the moment, 4 satellites are currently under development. For all parts of these systems, there is a great need to improve software reliability to pass all the European Space Agency (ESA) tests. As part of this thesis, it would be possible to assess the methodology during the design of new space projects and to test the platform on space systems. The PhD student could benefit from the experiences and expectations of all system researchers involved in the design of these satellites.