The 1st JAIST World Conference (JWC2018)
at JAIST, February 27-28, 2018

Vehicles need Formal Methods

TOSHIAKI AOKI

Graduate School of Advanced Science and Technology, Japan Advanced Institute of Science and Technology (JAIST), Nomi, Ishikawa, 923-1292, Japan
e-mail: toshiaki@jaist.ac.jp

Keywords: automotive systems, formal methods, model checking, testing

Recently, the safety and reliability of automotive systems are becoming a large concern in society. Although vehicles have been controlled by simple mechanics in the past, many of electronic parts are embedded in them at present according to the progress of electronic control technology and its performance. These electronic parts can actualize the complex control of the vehicles, and make it possible to provide high functionality to vehicles such as automatic speed controlling and braking. Furthermore, autonomous driving is accumulating interests all over the world. A complex electronic control is required in order to realize the autonomous driving and it must cause the drastic increase of the complexity of automotive systems. How we should ensure the safety and reliability of such super complex automotive systems is a big concern not only in industry but also academia.

In this background of industry and academia, our research group is working on the verification of automotive systems to ensure the safety and reliability of the automotive systems. We focus on applying scientific approaches such as formal methods and formal verification to practical automotive systems. We stick to practice. Our targets of the verification are real products. To target the real ones, we actively collaborate with industry. We succeeded in verifying real products so far including an automotive operating system which is developed by Renesas Electronics and safety requirements of an electronic steering system developed by Hitachi/Hitachi Automotive Systems. In addition, we are currently conducting several joint projects with automotive related companies in parallel. In this talk, I would like to briefly show the results and on-going status of three joint projects about the verification of the automotive operating system[1], the safety requirements[2] and Matlab/Simulink models[3].

References

1) Toshiaki Aoki, et.al: Combined Model Checking and Testing Create Confidence-A Case on Commercial Automotive Operating System, Chapter 5, pp.109-132, Cyber-Physical System Design from an Architecture Analysis Viewpoint, Springer, 2017.
2) Toshiaki Aoki, et.al: ISO 26262 using Goal Trees and Patterns, International Workshop on Formal Techniques for Safety-Critical Systems, Springer CCIS, pp.206-221, 2015.
3) Takashi Tomita, Daisuke Ishii, Toru Murakami, Shigeki Takeuchi and Toshiaki Aoki: Template-Based Monte-Carlo Test Generation for Models, Seventh Workshop on Design, Modeling and Evaluation of Cyber Physical Systems, 2017 (to appear).