Modeling Correct Safety Requirements Using KAOS and Event-B

Kriangkrai Traichaiyaporn (1110203)

School of Information Science,
Japan Advanced Institute of Science and Technology

August 8, 2013

Keywords: Formal methods, Event-B, KAOS, Safety requirements specification, Correctness.

Safety-critical systems are the systems whose failures can cause significant damage to life, property, and environment in which the systems are working on. One major causes of the system failures is the incorrectness of the safety requirements specifications described for developing the systems. Thus, the correctness of the safety requirements specification is crucial. Event-B is a famous formal specification language, which provides a refinement mechanism and a set of proof obligations for modeling and verifying the specifications. Event-B has a good potential for dealing with the correctness. However, Event-B lacks of the semantics of the correctness, and the mechanism to perform requirements analysis and elaboration. The semantics and the mechanism are necessary to ensure the correctness. In addition, there is no guideline for using the refinement mechanism. These shortcomings are hindrances for applying Event-B to the practical development of the safety-critical systems.

This thesis aims to propose an approach to overcome the shortcomings of Event-B. Firstly, the semantics of the properties preserved by the proof obligations are analyzed based on the semantics of the correctness defined in an evolutionary framework. This analysis claims that Event-B can preserve the correctness as defined in the evolutionary framework. Secondly, a new model is proposed to assist structuring and understanding Event-B.

The model is named ORDER model. Thirdly, a set of refinement patterns for the ORDER model are created based on the patterns of the KAOS method, which is a goal-oriented requirements engineering method. The KAOS method has the capabilities for requirements analysis and elaboration by the use of goals of systems and the notions of goal refinement. Through the usage of the KAOS-based patterns, the ORDER model can inherit the capabilities of the KAOS method, and the refinement in Event-B can be used in the similar way as the goal refinement. By applying the evolutionary framework and the KAOS method to Event-B, the shortcoming of Event-B can be overcome.

Evaluation of the approach is described through case studies. The case studies shows that the KAOS-based patterns are capable to analyze and elaborate safety requirements. Then, the requirements can be easily modeled in Event-B for verifying the correctness. In summary, through the usage of KAOS and Event-B, a formal model, representing correct safety requirements specification, can be obtained.