Verification and Testing of the RTOS for safety-critical embedded systems

Na Young Lee
Seoul National University, 56-1, Shillim, Kwanak, 151-742, Seoul, Korea

Jin Hyun Kim and Jin Young Choi
Korea University, 5-1, Anam, Seongbuk, 136-701, Seoul, Korea

Ah Young Sung and Byung Ju Choi
Ewha Womans University, 11-1, Daehyun, Seodaemoon, 120-750, Seoul, Korea

Jang Soo Lee
Korea Atomic Energy Research Institute, Daejon, Korea

Abstract

Development in Instrumentation and Control (I&C) technology provides more convenience and better performance, thus, adopted in many fields. To adopt newly developed technology, nuclear industry requires rigorous V&V procedure and tests to assure reliable operation. Adoption of digital system requires verification and testing of the OS for licensing. Commercial real-time operating system (RTOS) is targeted to apply to various, unpredictable needs, which makes it difficult to verify. For this reason, simple, application-oriented real-time OS is developed for the nuclear application. In this work, we show how to verify the developed RTOS at each development life cycle. Commercial formal tool is used in specification and verification of the system. Based on the developed model, software in C language is automatically generated. Tests are performed for two purposes; one is to identify consistency between the verified model and the generated code, the other is to find errors in the generated code. The former assumes that the verified model is correct, and the latter incorrect. Test data are generated separately to satisfy each purpose. After we test the RTOS software, we implement the test board embedded with the developed RTOS and the application software, which simulates the safety critical plant protection function.

Testing to identify whether the reliability criteria is satisfied or not is also designed in this work. It results in that the developed RTOS software works well when it is embedded in the system.