Abstract

Testing is one of the essential parts of software development. It provides guarantees in terms of system behaviour in specific scenarios, which are covered within the tests. That is why tests are a basis of a reliable system. Nevertheless, what if the system becomes increasingly large while the guarantees of its behaviour are the cornerstone of its existence? Such is the case for RTEMS, an open-source Real-Time Operating System (RTOS). RTEMS is commonly used in the embedded system in industries such as medicine, air and space. Many use cases in these industries require the system to have deterministic, predictable behaviour and guarantee to perform some tasks within time limit constraints. That makes writing tests a formidable task and makes it harder to verify whenever developed test suites are comprehensive enough.

This dissertation presents the framework that utilizes Promela/SPIN formal verification tools to model RTEMS behaviour and generate possible execution scenarios based on this model. These scenarios are then used together with templates to automatically generate the test suite for the modelled part of the system. Using SPIN/Promela allows the system to be formally verified through modelling while it also speeds up the development process of creating the test suites. Since the process is largely automated, it also decreases the chance of accidental human error and allows for better system scalability.

This work continues on previous research done as a part of the ESA RTEMS Qualification Project and is based on the framework used to model the Events Manager of RTEMS. The framework was overhauled, extended and applied to the RTEMS Barrier Manager to generate the test suite. The project resulted in a test suite with comprehensive code coverage and an improved framework that is cleaner and more extendable.