hitex
EMBEDDED TOOLS & SOLUTIONS

RogueWave SOFTWARE Klocwork	***Klocwork is a great static analysis tool producing very few false positives.*** Mark Kingston, Embedded Software Specialist, Hitex GmbH, Germany

The Product

The product is the firmware of a universal production programmer by Hitex called SPEED FLASH, used for end-of-line programming of microcontrollers and sensors. SPEED FLASH contains two XMC 4700 family microcontrollers from Infineon on which the firmware in question runs. The firmware is written in the C programming language, only a very small part is in assembler. In total, the firmware comprises of approx. 15.000 Lines-of-Code (LOC). The firmware is compiled using the MDK-ARM Version 5 development kit from ARM/Keil.

The Requirements

Although not being safety-critical in its strictest sense, the production programmer is intended to run around the clock (24/7), programming multiple microcontrollers or sensors in parallel. In consequence it is of high value that the programmer works permanently and reliable. Otherwise, production will stop unexpectedly, resulting in financial loss.

Usage of Klocwork

The development environment in which Klocwork is deployed uses Eclipse as editor. Klocwork comes with a plug-in for Eclipse enabling the direct use of Klocwork in Eclipse. Each time a source code file is saved, the analysis of Klocwork runs automatically. Klocwork is also integrated in a Continuous Integration system based on Jenkins. Klocwork looks primarily for violations of the MISRA-C:2012 rules and possible run-time errors (RTE). Except the rules for portability, almost all MISRA rules are enabled. This guarantees many positive effects in the source code: Avoidance of undefined or unspecified behavior, better understandability of the code, preventing misunderstandings of the effects of certain C constructs, etc. Overall, the MISRA rules intend to prevent the programmer from the dangers of the C programming language. In addition, Klocwork is on the lookout for run-time errors. Typical run-time errors are NULL pointer dereferencing, division by zero, out-of-bounds access, etc. Such errors usually cause the firmware to crash, which violates the goal of 24/7 availability. Therefore, it is paramount to produce code in a manner that prevents run-time errors.

Appraisal

“Klocwork is an essential tool that helps to reduce bugs in the firmware,” states Mark. “It helps a lot with complex logic; also, the capability to include multiple files in the analysis is invaluable. I like the fact that Klocwork produces very few false positives; and if it actually happens it is confirmed by the Klocwork support and usually remedied in the next release. Once Klocwork resolved a stability issue in a USB driver where an output parameter was not initialized correctly in all possible paths. Prior to the use of Klocwork this problem had caused tedious investigations. Therefore, I will continue to use Klocwork.”