The KNICS Approach for Verification and Validation of Safety Software

Kyung Ho Cha, Han Seong Sohn, Jang Soo Lee, Jang Yeol Kim,
Se Woo Cheon, Lee Young Joon, In Koo Hwang,
and Kee Choon Kwon

Korea Atomic Energy Research Institute
150 Dukjin-Dong, Yusong-Gu,
Daejon, 305-353, Korea

Abstract

This paper presents verification and validation (VV) to be approached for safety software of POSAFE-Q Programmable Logic Controller (PLC) prototype and Plant Protection System (PPS) prototype, which consists of Reactor Protection System (RPS) and Engineered Safety Features-Component Control System (ESF-CCS) in development of Korea Nuclear Instrumentation and Control System (KNICS). The SVV criteria and requirements are selected from IEEE Std. 7-4.3.2, IEEE Std. 1012, IEEE Std. 1028 and BTP-14, and they have been considered for acceptance framework to be provided within SVV procedures. SVV techniques, including Review and Inspection (R&I), Formal Verification and Theorem Proving, and Automated Testing, are applied for safety software and automated SVV tools supports SVV tasks. Software Inspection Support and Requirement Traceability (SIS-RT) supports R&I and traceability analysis, a New Symbolic Model Verifier (NuSMV), Statemate MAGNUM (STM) Model Certifier, and Prototype Verification System (PVS) are used for formal verification, and McCabe and Cantata++ are utilized for static and dynamic software testing. In addition, dedication of Commercial-Off-The-Shelf (COTS) software and firmware, Software Safety Analysis (SSA) and evaluation of Software Configuration Management (SCM) are being performed for the PPS prototype in the software requirements phase.