

PLC-기반 디지털 원자로안전계통 시제품을 위한 운영체제 소프트웨어의
요구사항 확인검증

Requirements Verification and Validation of Operating System Software
for a PLC-based Plant Protection System Prototype

차경호, 이영준, 천세우, 손한성, 김장열, 이장수, 권기춘
한국원자력연구소
대전광역시 유성구 덕진동 150

요약

본 논문은 원전계측제어시스템(Korea Nuclear Instrumentation and Control System: KNICS) 사업단에서 개발중인 안전등급 제어기기(Programmable Logic Controller: PLC)-기반 디지털 원자로안전계통 시제품의 운영체제 소프트웨어에 대한 요구사항 확인 및 검증(Requirements Verification and Validation)을 기술한다. 운영체제 소프트웨어는 신개발 소프트웨어(Newly Developing Software: NDS)로써 생명주기 확인검증(Lifecycle Phases V&V)이 적용되며, NUREG-0800의 Software Review Plan(SRP)/BTP-14와 IEEE Std. 7-4.3.2이 요구하는 소프트웨어 확인검증 기준들과 IEEE Std. 1012와 IEEE Std. 1028의 소프트웨어 확인검증 요구들이 생명주기 각 단계마다 엄격하고 체계적으로 적용된다. 요구사항 확인검증은 체크리스트-기반 Fagan 인스펙션이 주로 적용되었으며, 그리고 모델체킹에 의한 정형검증과 HAZOP(HAZards and OPerability) 방법에 의한 안전 요구사항의 확인이 수행되어 왔다. 체크리스트로 구성된 검증절차가 체계적인 요구사항 검증에 매우 효과적인 방법이었으며, 요구사항 확인검증에 사용된 검증기법과 도구들은 체계적인 설계 확인검증에도 적용될 수 있다.