Development of Software Safety Analysis Method for Nuclear Power Plant I&C Systems in Requirement Specification Based on Statechart and SCR

Jung Hwan Lee, Seo Ryong Koo, Han Seong Son, Poong Hyun Seong
Korea Advanced Institute of Science and Technology
373-1 Kusong-Dong, Yusong-Gu
Taejon Korea 305-701

Abstract

In recent years, Instrumentation and Control (I&C) system based on digital computer technology has been widely used throughout industries. These industries such as Nuclear Power Plant (NPP) have safety critical systems. Thus, safety critical system must have sufficient quality to assure a safe and reliable design. In this work, a formal requirement analysis method for Nuclear Power Plant (NPP) Instrumentation and Control (I&C) systems is proposed. This method use the Statechart diagram, Software Cost Reduction (SCR) formalism and ISO table newly suggested in this paper for checking the modeled systems formally. The combined method of utilizing Statechart, SCR and ISO table has the advantage of checking the system easily, visually and formally. This method is applied to the Water Level Monitoring System (WLMS). As a result of the formal check, one reachability error is detected.

원전 계측제어계통 소프트웨어 확인검증을 위한 지능형 통합환경 설계
An Intelligent & Integrated V&V Environment Design for NPP I&C Software Systems

구서룡, 손한성, 성풍현
한국과학기술원
대전광역시 유성구 구성동 373-1

요 약

원자력발전소는 그 특성상 안전성이 매우 강조되는 시스템이다. 원자로보호계통을 포함하는 계측제어계통은 원전에서 인간의 두뇌와 같은 역할을 담당하는 계통으로서 원전 전체의 안전성은 물론 운전에도 매우 중요한 영향을 미친다. 따라서, 안전이 중요한 원자력발전소의 보호계통에 소프트웨어 기반의 기기를 사용하려고 할 때 확인 및 검증은 필수적으로 수행되어야 하며, 이것은 인허가 문제와 직결되어 있기 때문에 기술적으로 매우 중요하다. 본 연구에서는 확인 및 검증을 자동화된 환경으로 구축할 수 있도록 지원하는 원전 계측제어계통 소프트웨어 확인검증을 위한 지능형 통합환경을 설계하였다. 지능형 통합환경의 주요 요소로는 지능형제어기부, 컴포넌트부, 인터페이스부, 그리고 GUI부가 있는데, 이 요소들은 각자의 독립적인 기능을 수행하기 위하여 유기적으로 결합되어 있다.