Software Design Specification and Analysis (NuFDS) Approach for the Safety Critical Software based on Programmable Logic Controller (PLC)

Seo Ryong Koo and Poong Hyun Seong
Korea Advanced Institute of Science and Technology
Department of Nuclear and Quantum Engineering
373-1 Guseong-dong, Yuseong-gu, Daejeon, Korea 305-701

Jin-Yong Jung and Seong Soo Choi
Atomic Creative Technology Ltd.
1688-5 Sinil-dong Daedeok-gu, Daejon, Korea 306-230

Abstract

This paper introduces the software design specification and analysis technique for the safety-critical system based on Programmable Logic Controller (PLC). During software development phases, the design phase should perform an important role to connect between requirements phase and implementation phase as a process of translating problem requirements into software structures. In this work, the Nuclear FBD-style Design Specification and analysis (NuFDS) approach was proposed. The NuFDS approach for nuclear Instrumentation and Control (I&C) software are suggested in a straight forward manner. It consists of four major specifications as follows; Database, Software Architecture, System Behavior, and PLC Hardware Configuration. Additionally, correctness, completeness, consistency, and traceability check techniques are also suggested for the formal design analysis in NuFDS approach. In addition, for the tool supporting, we are developing NuSDS tool based on the NuFDS approach which is a tool, especially for the software design specification in nuclear fields.