원자력발전소용 FPGA 기반 디지털 I&C 시스템 개발에 사용된 COTS 소프트웨어의 안전 카테고리 분류

정세진 O1 김의섭 1 유준범 1 최종균 2 김장열 2

1 건국대학교 컴퓨터-정보통신 공학부, 2 한국 원자력 연구원

{jsjj0728, atang34, jbyoo}@konkuk.ac.kr, {choijg,jykim}@kaeri.or.kr

Safety Category Classification of COTS software for developing Digital I&C System of Nuclear Power Plants

Sejin Jung O1 Eu-Sub Kim1 Junbeom Yoo1 Jong-Gyun Choi2 JangYeol Kim2

1School of Computing, Konkuk University, 2Korea Atomic Energy Research Institute

요 약

원자력 발전소의 디지털 계측제어 시스템은 안전성과 신뢰성이 보장 되어야 하는 안전필수시스템이다. 이러한 시스템 개발에 COTS 소프트웨어를 사용하기 위해서는 엄격한 적용 기준에 따라 사용 되어야 하고 이에 따른 표준들이 있다. 본 논문에서는 FPGA 기반의 원자력발전소 디지털 I&C 개발환경에 사용되는 COTS 소프트웨어를 대상으로 COTS 인증 프로세스(COTS dedication)의 첫 과정인 안전성 등급 분류를 수행 하였다.

1. 서 론

원자력발전소의 디지털 계측제어 시스템 (I&C: Instrumentation and Controller)은 안전성과 신뢰성이 중요한 안전필수시스템(Safety Critical System)이다. 신규 I&C 시스템을 개발하기 위해서는 검증된 인증 프로세스(COTS dedication)를 거쳐 안전성과 신뢰성이 충분히 보장된 COTS 소프트웨어를 사용 해야 한다[1][2].

미국 원자력규제위원회(NRC)와 전력연구원(EPRI) 에서는 원자력발전소의 I&C 시스템 개발 혹은 유지보수에 사용하기 위한 COTS 소프트웨어의 인증과정에 대해 가이드라인(NUREG/CR-6421[1], NP-5652[2])을 제시 하고 있다. 가이드라인에 따르면 먼저 COTS 소프트웨어가 수행하게 될 안전 기능(safety function)을 식별하여 안전 카테고리(safety category)를 분류한 뒤 카테고리에 맞는 인증 프로세스를 진행할 것을 제시하고 있다. 각 카테고리마다 수행해야 할 프로세스의 수준과 정도가 다르기 때문에 카테고리 분류 과정이 필수적이다.

우리는 이전 연구를 통해 PLC 기반의 소프트웨어 개발 환경을 이용해 FPGA를 이용한 디지털 I&C 개발을 지원하는 개발 환경을 제안 하였다[3][4][5]. 개발 환경에는 일반적으로 FPGA를 개발하기 위해 사용되는 합성(synthesis) 도구나 배선 및 배치(P&R: Place and Route) 도구와 같은 다양한 COTS 소프트웨어가 포함되어 있고, 안전성 분석 및 검증을 위해 개발한 다양한 소프트웨어 또한 포함되어 있다. 이전 연구에서 사용한 COTS 소프트웨어 및 개발한 소프트웨어들을 디지털 I&C 시스템 개발에 이용하기 위해서는 해당 소프트웨어들에 대해 인증 프로세스를 거쳐 안전성과 신뢰성을 입증할 필요가 있다. 이에 본 논문에서는 해당 소프트웨어 들의 인증 프로세스 진행을 위한 첫 단계인 안전 카테고리 분류를 수행하였다.

2. 배경지식

IEC 1226[6]은 원자력발전소에 사용되는 소프트웨어의 안전성 중요도에 따라 카테고리의 분류를 제시한 표준이다. 소프트웨어의 안전성 중요도에 따라 소프트웨어를 4개의 카테고리로 분류하고 있으며 각 카테고리는 A, B, C, unclassified 가 있다. 순서대로 중요성에 따라 분류하며 카테고리 A로 분류되는 소프트웨어가 가장 안전성이 중요한 소프트웨어가 된다. 표 1은 IEC 1226 에서 분류하고 있는 안전 카테고리 및 예시이다.

표 1. 안전 카테고리 및 예시(Safety category)

IEC 1226 안전 카테고리	예시
A	원자로 보호 계통 시스템(RPS) / 공학 안전 설비(ESFAS) 등
B	발전소 자동 제어 시스템 / 연료 재충전 시스템 등
C	알람 / 모니터링 시스템 등

NuREG/CR-6421[1] 은 미국 원자력규제위원회 (NRC)에서 제안한 표준 가이드라인으로 원자력발전소의 I&C 개발을 위해 사용되는 COTS 소프트웨어 인증 프로세스를 설명하고 있다. 인증 프로세스는 크게 전체 시스템 위험성 분석을 통한 COTS 소프트웨어 카테고리 분류와 카테고리 별로 인증 프로세스를 진행하는 두 부분으로 되어있다. COTS

소프트웨어 카테고리 구성은 IEC 1226 표준의 안전성 카테고리를 따라 4 가지로 구성되어 있으며 분류한 카테고리에 따라 채택 과정에서 검증 강도가 달라진다. 카테고리 A 의 채택 과정에서는 높은 수준의 소프트웨어 품질 관리와 검증 및 확인이 요구되며 사용 경험과 지속적인 에러 확인 및 버그 추적 또한 필요하다. 카테고리 B의 경우는 A에 비해 다소 낮은 수준의 소프트웨어 품질 관리 와 검증 및 확인 작업이 요구된다.

3. 디지털 I&C 시스템의 개발을 지원하는 COTS 소프트웨어의 안전 카테고리 분류 및 과정

COTS 소프트웨어의 dedication을 위해 NuREG/CR-6421에 따라 안전 카테고리 결정 과정을 수행 하였다. 그림 1은 NuREG/CR-6421에 따라 수행한 안전 카테고리 결정 과정에 대한 그림이다.

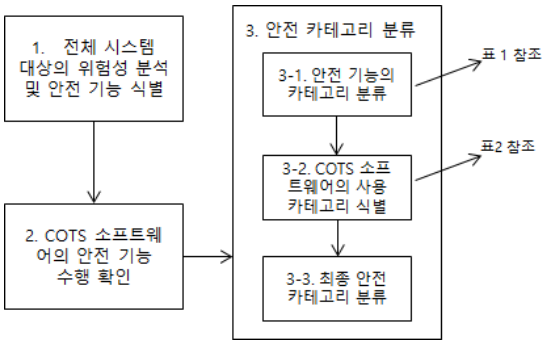

그림 1. COTS 소프트웨어의 안전 카테고리 결정 과정

3.1 위험성 분석 수행 및 안전 기능 식별

보호계통 또는 제어 계통의 시스템 등이 있다. 전체 시스템을 대상으로 위험성 분석(hazard analysis)을 수행 하여 시스템의 안전 기능(safety function)을 파악해야 한다. 안전 기능이란 원자로의 정상 동작을 위협하는 요소(위험, 에러)에 의한 사고로부터 원자로를 보호하기 위한 기능이다. 예를 들어 I&C 시스템의

3.2 COTS 소프트웨어의 안전 기능 수행 확인

본 논문에서 분류하고자 하는 소프트웨어 들은 I&C 시스템의 보호계통 중 하나인 RPS(Reactor Protection System) 시스템 개발에 사용되는 소프트웨어들 이다. RPS는 원자로발전소의 안전관련 공정 변수들이 정해진 제한 값을 위반하는지 확인하여 위반 시 원자로를 안전하게 정지시키고 관련 안전설비를 작동시켜 원자로를 위험으로부터 보호하는 기능을 수행하는 시스템이기 때문에 안전 기능을 수행하는 시스템이라 판단할 수 있고, 인증 프로세스를 진행할 필요가 있다.

3.3 안전 카테고리 결정

식별된 안전 기능에 따라 COTS 소프트웨어에 적용할 안전 카테고리를 결정한다. COTS 소프트웨어의 안전 카테고리는 수행하는 안전 기능과 소프트웨어의 사용 방식 및 목적에 따라 달라진다. 안전 카테고리 분류과정을 3 단계로 세분화 하여 살펴보면 안전 기능의 카테고리 분류, COTS 소프트웨어의 사용 카테고리 식별과 두 카테고리를 이용해 최종 안전 카테고리를 분류하는 3 단계로 구성 되어 있다.

3.3.1 안전 기능의 카테고리 분류

이전 단계 에서 확인한 안전 기능의 중요도에 따라 안전 기능의 안전 카테고리를 분류한다. 본 논문에서 적용하고자 하는 RPS 시스템은 최상위 등급의 안전 기능을 수행하는 시스템으로서 IEC 1226의 안전 카테고리에서 A 카테고리에 해당한다.

3.3.2 COTS 소프트웨어의 사용 카테고리 분류

다음 단계로 COTS 소프트웨어가 사용되는 방식을 분석하여 COTS 소프트웨어의 사용 카테고리를 분류한다. 표 2는 NuREG/CR-6421에서 사용 방식 및 목적에 따라 사용 카테고리를 분류하는 표이다.

표 2. COTS 사용 방식에 따른 카테고리 분류 방식

COTS 사용 카테고리	상세 설명	IEC 1226 카테고리
직접 사용 (Direct)	A, B, C 안전 카테고리의 안전 기능에 직접적으로 사용	A, B, C
간접 사용 (Indirect)	A, B, C 카테고리의 모듈을 생성 (예, 컴파일러, 링커 등)	A, B, C, unclassified
지원 용도 (Support)	지원 시스템, 간접 사용이 아닌 다른 방식으로 A, B, C 카테고리 시스템 개발을 지원	unclassified
미 연관 (Unrelated)	A, B, C 카테고리에 영향을 미치지 않음	unclassified

표 3. 디지털 I&C 시스템 개발에 사용되는 COTS 소프트웨어

용도	사용 단계	
	디자인	구현
안전성 분석	FBDFTA	
개발	FBD Editor	FBDtoVerilog FBDtoVHDL Synthesis Tool P&R Tool
검증	FBD Checker Scenario Generator FBD Simulator	ModelSim Co-Simulator FBD-Verilog Comparator

본 논문에서 분류하고자 하는 COTS 소프트웨어들은 표 3과 같다. 개발을 위한 도구로 *FBDtoVerilog*, *FBDtoVHDL*, *Synthesis Tool, FBD Editor, P&R 도구* 가 있고, 검증을 위한 도구로 *FBD Checker, Scenario Generator, FBD Simulator, FBD-Verilog Comparator, ModelSim, Co-Simulator*가 있다. 또한 안전성 분석을 위한 도구로 *FBD FTA*도 존재 한다.

표 4. COTS 소프트웨어 사용 카테고리 분류

COTS 사용 카테고리	FPGA 기반 디지털 계측제어 I&C 개발환경의 COTS 소프트웨어	용도
간접 사용	FBDtoVerilog / FBDtoVHDL / Synthesis Tool / P&R Tool	개발
지원	FBD Editor	개발
미 연관	FBD FTA	안전성 분석
	FBD Checker Scenario Generator / FBD Simulator / FBD-Verilog Comparator / ModelSim / Co-Simulator	검증

표 3 의 도구들을 사용 카테고리 별로 분류하면 표 4와 같다. 안전성 분석에 사용되는 도구들은 미연관 카테고리에 속하고 개발에 사용되는 도구 중 디자인에 사용되는 FBD Editor는 에디터로서 지원 카테고리에 속한다. 그 외 구현에 사용되는 4 가지 개발 도구들은 안전 기능의 모듈을 직접 생성하고 변환하는 도구이기 때문에 간접 사용 카테고리에 속한다. 검증에 사용되는 디자인과 구현 단계의 도구들은 FPGA 개발에 직접 사용되지 않기 때문에 미 연관 카테고리로 분류된다.

3.3.3 최종 안전 카테고리 분류

최종 안전 카테고리 분류는 3.3.1, 3.3.2 에서 수행했던 분류 결과를 이용한다. 표 5는 FPGA 개발 과정에 사용되는 소프트웨어들의 안전 카테고리 분류 결과이다. 3.1 에서 분류한 대상 시스템의 카테고리는 A 이고 3.2에서 분류한 소프트웨어들의 카테고리는 간접 사용과 지원용도 및 미 관련 카테고리가 있다. 지원 용도 및 미 관련 카테고리의 소프트웨어 들은 NuREG/CR-6421 표준에 따라 대상 시스템의 안전 카테고리에 구분 없이 unclassified로 분류된다.

표 5. COTS 소프트웨어 안전 카테고리 분류표

안전 카테고리	FPGA 기반 디지털 계측제어 I&C 개발환경의 COTS 소프트웨어
A	N/A
B	FBDtoVerilog / FBDtoVHDL / Synthesis Tool / P&R Tool
C	N/A
Unclassified	FBD Editor / FBD FTA / FBD Checker Scenario Generator / FBD Simulator / FBD-Verilog Comparator / ModelSim / Co-Simulator

간접 사용 카테고리에 속하는 소프트웨어들의 경우 결과물의 다른 검증 방법이 없다면 대상 모듈과 같은 수준의 카테고리로 분류되지만 결과물에 대해 다른 검증 방법이 존재한다면 한 단계 낮은 수준의 카테고리로 분류 할 수 있다.

간접 사용 카테고리 소프트웨어들의 분류 결과를 자세히 확인해보면 FBDtoVerilog 와 FBDtoVHDL 은 각각 FPGA 개발에 사용되는 Verilog와 VHDL이라는 하드웨어 상세 언어(HDL)를 FBD로부터 변환하는 도구이다. VHDL로 작성된 모듈은 시뮬레이션(ModelSim)을 통한 검증이 가능하고 Verilog 또한 시뮬레이션(ModelSim)을 통한 검증과 정형 검증 방법(VIS, smv)을 통한 검증도 가능하기 때문에 A 카테고리의 모듈을 생성하는 B 카테고리의 COTS 소프트웨어로 분류된다.

Verilog 나 VHDL 같은 HDL 언어를 gate-level의 Netlist로 변환해 주는 synthesis 도구의 결과물인 Netlist와 Netlist를 layout 형태로 변환해 주는 P&R 도구의 결과물인 JEDEC 또한 시뮬레이션(ModelSim)을 통한 검증이 가능하기 때문에 B 카테고리의 COTS 소프트웨어로 분류 된다.

4. 결론 및 향후 연구

본 논문에서는 FPGA 기반 RPS 개발에 사용된 COTS 소프트웨어의 인증을 진행하기 위한 안전 카테고리 분류를 수행하였다. 우리는 RPS 시스템의 안전성 카테고리를 IEC 1226 표준에 맞추어 분류 하였고, 각 COTS 소프트웨어의 사용 카테고리를 분류 하였다. 분류된 안전 카테고리와 사용 카테고리를 이용하여 각 COTS 소프트웨어에 대해 적절한 안전 카테고리를 분류할 수 있었다. 앞으로 우리는 분류한 안전 카테고리를 이용하여 다음 과정의 인증 프로세스를 진행할 계획을 가지고 있다.

사 사

본 연구는 한국원자력연구원의 “FPGA-기반 제어기 통합개발환경을 위한 핵심 소프트웨어 기술 개발” 의 지원으로 연구한 결과입니다.

참 고 문 헌

[1] Nuclear Regulatory Commission, NuREG/CR-6421 “A Proposed Acceptance Process for Commercial Off-the-Self (COTS) Software in Reactor Applications”, 1996.

[2] Electric Power Research Institute, “Plant Engineering : Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications”, 2013.

[3] Junbeom Yoo, Eui-Sub Kim, Dong-Ah Lee, Jong-Gyun Choi, Young Jun Lee and Jang Soo Lee, “NuDE 2.0 : A Model-based Software Development Environment for the PLC & FPGA based Digital Systems in Nuclear Power Plants”, International Symposium on Integrated Circuit, pp 604-608, 2014.

[4] Junbeom Yoo, Eui-Sub Kim, Dong-Ah Lee and Jong-Gyun Choi, “An Integrated Software Development Framework for PLC & FPGA based Digital I & Cs”, International Symposium on Future I & C for Nuclear Power Plants, 2014.

[5] 이동아, 유준범, 최종균, “원자력 발전소의 FPGA 기반 계측제어 시스템을 위한 통합 소프트웨어 개발 환경”, 정보과학회지 제 32권 제 12호, p36-43, 2014.

[6] International Electrotechnical Commission, IEC 1226 “Nuclear Power Plants - Instrumentation And Control Systems Important For Safety - Classification”, 1994.