

KNS 2025 Spring

Review of the Conventional Regulations Guideline for Digital Instrumentation and Control of Nuclear Power Plants focusing on Small Modular Reactors

Sujeong Lim¹, Jiyoung Song², Sejin Jung³, Yoona Heo⁴, Junbeom Yoo⁴, and Eunkyong Jee¹

1 KAIST, 2 Hannam Univ, 3 Chinju National Univ. of Education, 4 Konkuk Univ.

Contents

1. Introduction
2. FGPA 개발 절차
3. NUREG/CR-7006 핵심 고려사항
4. FPGA 특징 기반 기존 심사 지침 (GE-N001) 분석
5. Conclusion

Introduction

Background

- 기존 원전 디지털 계측제어 계통의 심사 및 규제 지침을 SMR에 적용할 때 발생하는 한계점 및 변경사항 파악 필요
- 국제 표준을 준수하기 위해, SMR 대상 국제 규제 지침 (DSRS 등)에 상응하는 국내 심사 지침 개발을 위한 고려사항 분석 필요

Goal

- 국내 SMR 핵심 변경 사항인 FPGA 도입에 집중하여, 기존 국내 심사 지침에서 변경 및 보완되어야 할 사항 제안
- NUREG/CR-7006^[1] (FPGA 심사지침)을 참고하여 국내 심사 지침의 변경 방향 분석

[1] Bobrek, M. (2010). Review guidelines for field-programmable gate arrays in nuclear power plant safety systems (NUREG/CR-7006). US Nuclear Regulatory Commission (US NRC).

FPGA 개발 절차

PLC 기반 개발 절차

*IEEE-1074, IEC-62566 기반



FPGA 기반 개발 절차

*NUREG/CR-7006 반영



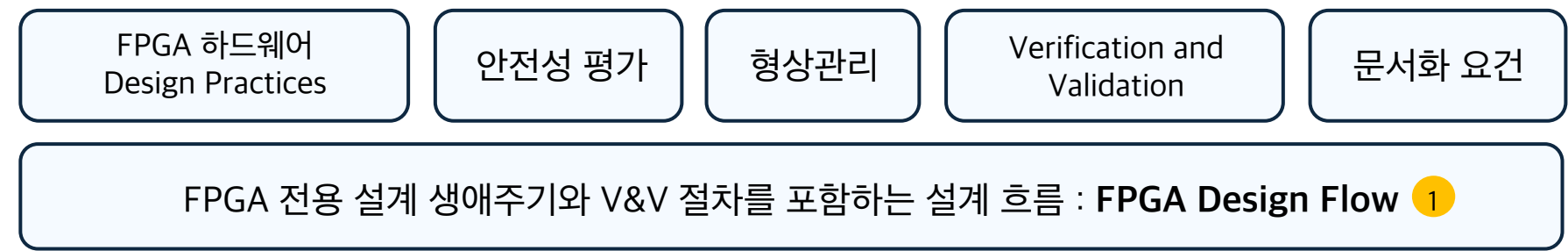
SW와 HW 특성을 모두 포함하는 FPGA 개발 절차 반영 필요

NUREG/CR-7006^[1]의 핵심 고려사항

NUREG/CR-7006

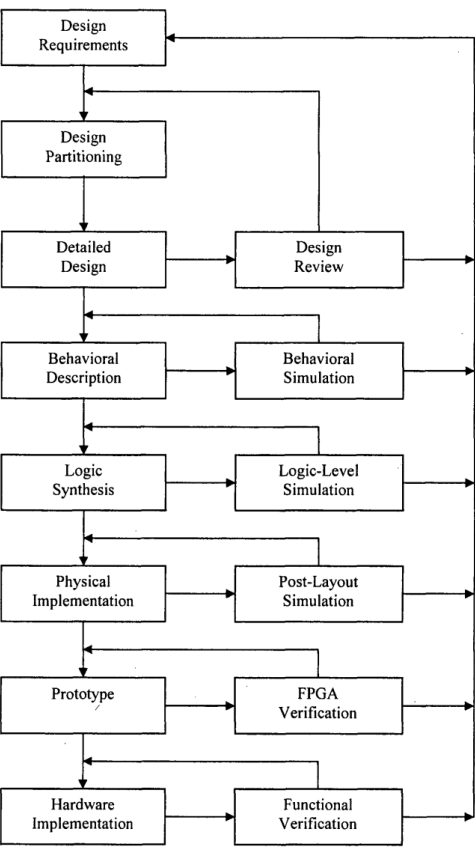
기존 원자력 발전소의 계측 및 제어(I&C) 계통 소프트웨어 관련 규제 지침이 **하드웨어와 소프트웨어의 특성을 모두 포함하는 FPGA의 특성**과 관련된 안전성 문제를 충분히 다루지 못하는 한계를 보완하기 위해 개발된 FPGA 전용 심사지침

NUREG/CR-7006 구성



CR-7006에서 제시하는 FPGA 특성과 FPGA 설계 흐름을 바탕으로
국내 심사 지침의 변경 방향을 분석하고자 함

1 FPGA Design Flow



[1] Bobrek, M. (2010). Review guidelines for field-programmable gate arrays in nuclear power plant safety systems (NUREG/CR-7006). US Nuclear Regulatory Commission (US NRC).

FPGA 특징 기반 기존 심사 지침 (GE-N001) 분석

1. FPGA의 HW와 SW적 특성을 반영한 심사 지침

- 심사 지침 내 적용 범위를 '소프트웨어'로 한정하는 부분
- 소프트웨어 관점만 다루는 부분
- → FPGA와 같은 프로그래머블 복합 논리 장치를 포함한다는 점을 명시

심사 지침 부분

- 제7.7절 (제어계통): 제어 계통에 대한 검토 절차
- 제7.9절 (데이터 통신계통): 데이터 통신 계통에 대한 검토 절차 및 평가 계획
- 부록 7.1-4 (KEPIC ENB-6370 “안전계통 디지털 컴퓨터”준수에 관한 평가 지침)
- 부록 7-17 (디지털 컴퓨터 실시간 성능에 관한 평가지침)

변경 방향 참고용 국제 표준 레퍼런스

maintenance, and retirement. This standard applies to the system, software, and hardware being acquired, developed, maintained, or reused. The term *software* also includes firmware and microcode (e.g., Field Programmable Gate Arrays and Programmable Logic Devices). Each of the terms *system*, *software*, and *hardware* includes its associated documentation.

IEEE 1012-2016

This guidance applies to microprocessor-based technology, as well as other forms of complex logic, such as programmable logic devices (e.g., field programmable gate arrays (FPGAs)). This DSRS uses the term *software* to refer to such technology and complex logic. In developing these systems, an applicant should follow a well-defined and documented system development approach that is consistent with the guidance in this section.

DSRS

FPGA 특징 기반 기존 심사 지침 (GE-N001) 분석

2. FPGA의 개발 절차 반영

기존

부록 7-13 (디지털 컴퓨터 기반 계측제어 시스템의 소프트웨어 검토 지침)

- 안전 계통에 사용되는 소프트웨어 승인에 필요한 규제 요건
- 소프트웨어 생애주기 프로세스 평가를 위한 지침 제공
- 소프트웨어 생애주기의 각 단계별 설계 산출물에 대한 규제 지침 제공
- 디지털 컴퓨터 구현과 관련하여 HDL은 포함하지 않는 개발 언어만 명시



변경 방향

- FPGA 전용 개발 생애주기 및 하드웨어 개발 언어 반영
- SW와 HW 문서화 요건 모두 포함
 - IEEE 1012 (SW 문서화 요건) + DO-254^[2] (HW 문서화 요건)
 - IEEE 1012-2016^[3] (SW & HW)

[2] Do, R. T. C. A. (2000). Design Assurance Guidance for Airborne Electronic Hardware (DO-254). Design Assurance Guidance for Airborne Electronic Hardware, RTCA Inc., Washington, DC.

[3] "IEEE Standard for System, Software, and Hardware Verification and Validation," in *IEEE Std 1012-2016 (Revision of IEEE Std 1012-2012/ Incorporates IEEE Std 1012-2016/Cor1-2017)*, vol., no., pp.1-260.

FPGA 특징 기반 기존 심사 지침 (GE-N001) 분석

3. PLC 지침에 상응하는 FPGA 사용 지침 마련

기존

부록 7-15 PLC 사용에 대한 심사지침

- PLC 관련 규제 지침
- PLC 정의
- PLC 특성
- 프로그래밍 언어
- 심사 대상 주요 문서



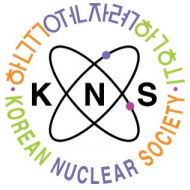
변경 방향

부록 7-xx FPGA 사용에 대한 심사지침

- FPGA 관련 규제 지침
- FPGA 정의
- FPGA 특성
- 프로그래밍 언어
- 심사 대상 주요 문서

Conclusion

- SMR은 계측 및 제어(I&C) 계통의 기존 규제 요건을 충족하는 데 어려움 예상
- FPGA의 사용에 따른 국내 심사 지침 마련 필요
- NUREG/CR-7006 (FPGA 심사 지침)을 기반으로 FPGA 도입에 따른 변경 방향 분석
 - 기존 SW 중심 규제 지침에 HW와 SW적 특징을 모두 포함하는 FPGA 특성 반영 필요
 - FPGA 사용에 대한 지침 추가 필요



감사합니다.

Review of the Conventional Regulations Guideline for Digital Instrumentation and Control of Nuclear Power Plants focusing on Small Modular Reactors

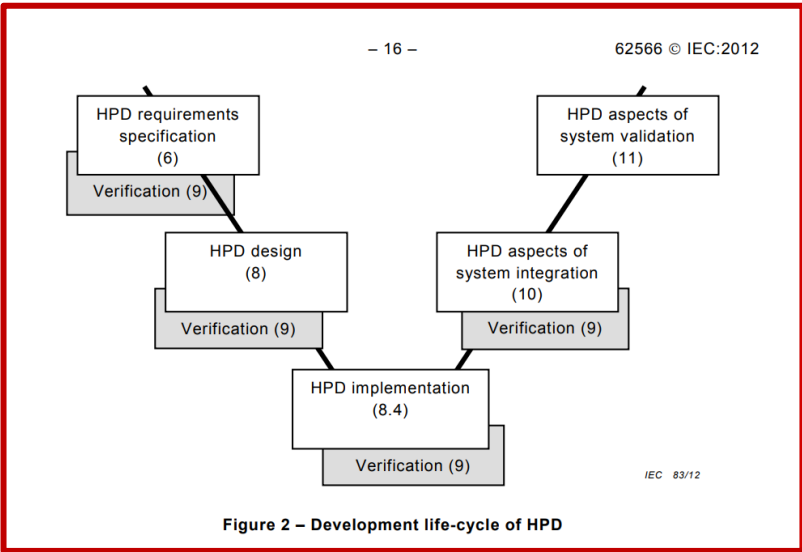
Sujeong Lim¹, Jiyoung Song², Sejin Jung³, Yoona Heo⁴, Junbeom Yoo⁴, and Eunkyong Jee¹

1 KAIST, 2 Hannam Univ, 3 Chinju National Univ. of Education, 4 Konkuk Univ.

Contact (Sujeong Lim)

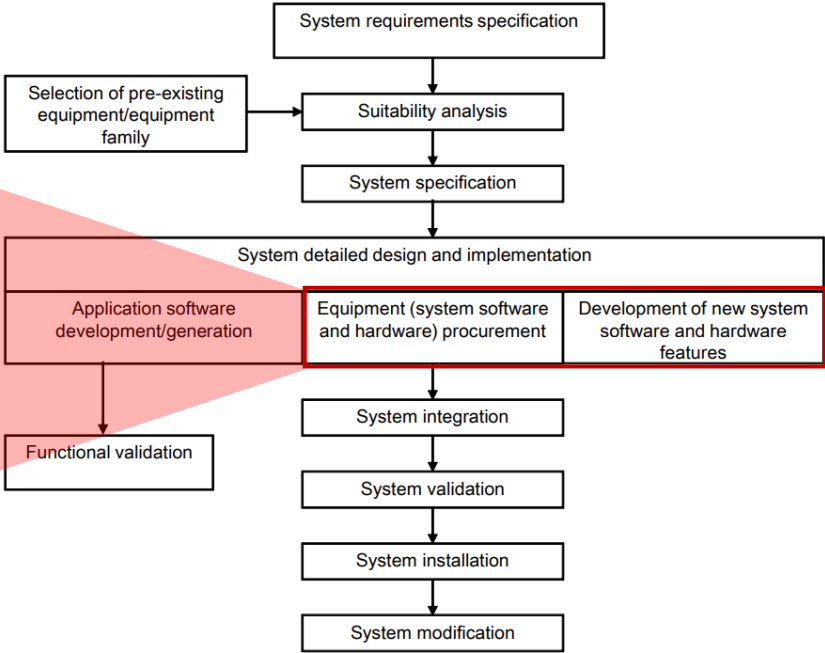
sjlim@webeng.kaist.ac.kr

Appendix



62566 © IEC:2012

– 15 –



Appendix

- 라. 제어계통 고장의 영향 : 검토담당부서는 어떠한 제어계통 부품이나 제어계통을 지원하는 보조지원계통의 고장이 발전소 상태를 안전성분석보고서 15장의 예상 운전과도에 대한 분석에서 기술된 발전소 상태보다 악화시키지 않음을 확인해야 한다. 이러한 평가는 하드웨어 무작위적인 고장뿐만 아니라 **소프트웨어** 설계 오류와 같은 디지털 시스템과 관련될 수 있는 고장모드에 대해 다루어야 한다.(다중 독립적인 고장에 대한 평가를 의도하는 것은 아님)
- 마. 사고에 의해 유발되는 제어계통 고장의 영향 : 제어계통 검토담당부서는 예상 운전과도사건/사고의 결과가 안전성분석보고서 15장에 기술된 것 보다 더 심각한 결과를 야기할 수 있는 제어계통의 고장을 유발하지 않는지를 확인해야 한다.
- 바. 환경제어계통 : 검토담당부서는 계측제어계통이 극한 환경으로부터 기기를 보호하기 위해 필요한 환경제어를 포함하는지를 확인해야 한다. 예를 들면, 이러한 환경제어기에는 안전계통의 안전성 계측기 및 계측 감지관의 보온(RG 1.151 참조), 캐비닛의 냉각팬 등이 있다.
- 사. 디지털 계통의 사용 : 안전계통에 영향을 미칠 수 있는 제어계통의 고장 잠재성을 최소화하기 위하여, 제어계통의 **소프트웨어**는 안전계통에 적용된 **소프트웨어**와 유사하게 체계적인 과정을 통해서 개발되어야 한다. 제어계통 **소프트웨어**가 안전계통보다 비교적 낮은 안전 중요도를 갖고 있음을 감안하여 개발과정중의 일부 과정은 생략될 수 있다.(부록 7.0-1 및 7.1-4의 디지털 계통에 대한 지침 참

7.7절 제어계통