KAERI/TR-8697/2021

기술보고서

디지털 I&C 소프트웨어 신뢰도 평가 방법론 및 규제기준/사례 분석

Analysis on Digital I&C Software Reliability Assessment Methods and Regulation Standards/Cases

KAERI
Korea
Atomic Energy
Research Institute

한국원자력연구원
Korea Atomic Energy Research Institute

KAERI

제 출 문

한국원자력연구원장 귀하

이 보고서를 2021년도 “원전 디지털 I&C 소프트웨어 신뢰성 평가 규제 방법론 개발” 과제의 기술보고서로 제출합니다.

2021년 8월 31일

과제명 : 원전 디지털 I&C 소프트웨어 신뢰성 평가 규제 방법론 개발

주 저 자 이상훈

공 저 자 신성민

장승철

최종균

KAERI

요 약 문

Ⅰ. 제 목

디지털 I&C 소프트웨어 신뢰도 평가 방법론 및 규제기준/사례 분석

Ⅱ. 연구개발의 목적 및 필요성

- 최근 가동원전의 디지털 업그레이드 및 신규 원전의 디지털 장비 도입에 따라, 규제기관은 현 규제체제를 기반으로 디지털 I&C 계통 내 소프트웨어의 신뢰도 및 소프트웨어의 신뢰도에 따른 계통 안전성 영향을 체계적으로 평가할 수 있는 방법론의 개발이 필요함.
- 이에 따라, 원자력 분야에 적용된 정성적/정량적 소프트웨어 신뢰도 평가 방법론을 조사하여 현 규제체제에 활용가능성을 검토하고 국외 소프트웨어 규제기준 및 사례분석을 기반으로 국내 규제체제의 개선방향을 제안하고자 함.

Ⅲ. 연구개발의 내용 및 범위

- 디지털 I&C 소프트웨어 신뢰도 평가 방법론 현황 조사
  - 국내외 적용된 소프트웨어 정성적/정량적 신뢰도 평가 방법론들의 특징 및 한계점을 분석하고 현 규제체제에 활용 가능성 검토
    * 정성적 방법론 : SW HAZOP, SW FMEA, SW FTA, 정형 기법
    * 정량적 방법론 : SRGM, BBN, Metric-based Method, CSRM, Test-based Method
- 디지털 I&C 소프트웨어 신뢰도 규제기준 및 사례 분석
  - 국내 및 국외 (미국, 캐나다, 핀란드) 소프트웨어 신뢰도 관련 규제기준 및 사례를 분석하여 국내 규제체제의 개선방향 제안

Ⅳ. 연구개발결과

- 본 보고서는 당해연도 연구목표인 “국내외 디지털 I&C 소프트웨어 신뢰도 평가 방법론 분석”을 위해 소프트웨어 정성적/정량적 신뢰도 평가 방법론 조사 및 국내외 소프트웨어 신뢰도 관련 규제기준 및 사례들을 분석하고 국내 규제기술의 개선방향을 제안함.
- 국내외 여러 정성적/정량적 방법론들의 특징 및 한계점 분석 결과, 국내 소프트웨어 신뢰도 규제기준을 고려하여 시험 기반 기법이 가장 적합할 것으로 판단됨.

ㅇ 국내 규제기준 및 기술과 관련하여, 현재 한국원자력안전기술원 (KINS)은 소프트웨어 안전성 분석과 관련하여 소프트웨어 생명주기 품질 관리 등 미국 NRC의 정성적 평가 요건들을 규제지침으로 활용하고 있지만, 향후 미국 NRC의 APR-1400 NRC DC 사례, 캐나다 CNSC의 DNGS SDS 사례 등을 기반으로 정량적 평가 요건을 규제 지침에 추가할 것을 고려해야 함.

V. 연구개발결과의 활용계획

ㅇ 본 연구결과는 가동 원전의 디지털 I&C 설비 교체 및 업그레이드, 신규원전의 디지털 I&C 설비 도입 시, 원자력 규제기관의 소프트웨어 신뢰도 관련 규제지침 개발의 기초자료로 활용 가능함.

- 해당 연구결과는 차차기년도 “원전 디지털 I&C 소프트웨어 신뢰도 정량화(실패율) 방법론 개발” 업무에 활용되며, 도출된 방법론에 대해 사례분석을 통해 규제 측면의 적용가능성을 평가할 예정임.

KAERI

SUMMARY

Ⅰ. Project Title

Analysis on Digital I&C Software Reliability Assessment Methods and Regulation Standards/Cases

Ⅱ. Objective and Importance of the Project

- With the recent digital upgrade of operating nuclear power plants and the introduction of new digital equipment, regulators need to develop a methodology to systematically evaluate the software reliability in digital I&C systems.
- Accordingly, the qualitative/quantitative software reliability assessment methodology applied to nuclear field are investigated. The feasibility of each method's application to the current regulatory system are reviewed and the improvement direction of the domestic regulatory framework based on foreign regulatory standards and case analysis is proposed.

Ⅲ. Scope and Contents of Project

- Research on the current status of digital I&C software reliability assessment methodology
  - Analysis on the characteristics and limitations of the qualitative/quantitative reliability assessment methodologies and review of their applicability to the current regulatory framework
    * Qualitative method : SW HAZOP, SW FMEA, SW FTA, Formal method
    * Quantitative method : SRGM, BBN, Metric-based Method, DFM, Test-based Method
- Analysis on the digital I&C software reliability regulatory standards and cases
  - Suggestion for the improvement of domestic regulatory framework by analyzing regulatory standards and cases related to domestic and foreign (U.S., Canada, Finland) software reliability

Ⅳ. Result of Project

- This research investigates software qualitative and quantitative reliability assessment methodology and analyzes domestic and foreign software reliability-related regulatory standards and the cases for this year's research goal, "Analysis of domestic and foreign digital I&C software reliability assessment methodology"
- As a result of characteristics and limitation analysis of various domestic and foreign qualitative and quantitative methodologies, the test-based method is considered to be the most applicable to the current domestic software reliability regulatory framework.
- Regarding domestic regulatory standards and technologies, KINS currently uses qualitative assessment requirements adopted from the U.S. NRC, such as software lifecycle quality control, as regulatory guidance. Based on the APR-1400 NRC DC case and Canada's DNGS SDS case, adding the quantitative assessment requirements to current regulatory guidance should be considered.

Ⅴ. Proposal for Applications

- The result of this research can be used as a basic data for the development of regulatory guidelines related to the software reliability by regulators when installing digital I&C facilities of operating or new nuclear power plants.
  - The findings from this research will be used for the 3rd year's task "Development of Nuclear I&C Software Reliability Quantification (Failure Rate) Methodology" and will evaluate the applicability of regulatory aspects through case analysis.

CONTENTS

SUMMARY ····· 5

Chapter 1. Introduction ····· 15
Section 1. Research Background ····· 17
Section 2. Research Purpose ····· 17
Section 3. Research Scope ····· 18

Chapter 2. Software Failure Characteristics and Reliability Definition ····· 19
Section 1. Characteristics of Software Failure ····· 21
Section 2. Definition of Software Reliability ····· 22

Chapter 3. Survey on Digital I&C Software Reliability Assessment Methods · 23
Section 1. Qualitative Software Reliability Assessment Methods ····· 25
1. Software Hazard and Operability Studies ····· 25
2. Software Failure Mode and Effect Analysis ····· 28
3. Software Fault-tree Model ····· 30
4. Software Formal Method ····· 32
Section 2. Quantitative Software Reliability Assessment Methods ····· 40
1. Software Reliability Growth Model ····· 40
2. Bayesian Belief Network Model ····· 41
3. Metrics-based Method ····· 42
4. Context-based Software Risk Assessment Method ····· 44
5. Test-based Method ····· 46
Section 3. Comparative Analysis of Software Reliability Assessment Methods ····· 50

Chapter 4. Regulation Standards and Cases on Software Reliability ····· 51
Section 1. Domestic Regulation Standards and Case Study ····· 53
1. Republic of Korea KINS ····· 53
Section 2. Foreign Regulation Standards and Cases ····· 61
1. United States NRC ····· 61

2. Canada CNSC ····· 70
3. Finland STUK ····· 77

Chapter 5. Suggestion on Improvements for Software Reliability Regulation · 83

Chapter 6. Conclusion ····· 87

Reference ····· 91

BIBLIOGRAPHIC INFORMATION SHEET ····· 102

KAERI

목 차

요약문 ····· 3

제1장 서론 ····· 15
제1절 연구 배경 ····· 17
제2절 연구 목적 ····· 17
제3절 연구 범위 ····· 18

제2장 소프트웨어 고장 특성 및 신뢰도 정의 ····· 19
제1절 소프트웨어 고장 특성 ····· 21
제2절 소프트웨어 신뢰도 정의 ····· 22

제3장 디지털 I&C 소프트웨어 신뢰도 평가 방법론 현황 조사 ····· 23
제1절 정성적 소프트웨어 신뢰도 평가 방법론 ····· 25
1. 소프트웨어 위험요소 및 운전분석 방법 ····· 25
2. 소프트웨어 고장모드 및 영향 모델 ····· 28
3. 소프트웨어 고장수목 모델 ····· 30
4. 소프트웨어 정형 기법 ····· 32
제2절 정량적 소프트웨어 신뢰도 평가 방법론 ····· 40
1. 소프트웨어 신뢰도 성장 모형 ····· 40
2. 베이지안 네트워크 모델 ····· 41
3. 척도 기반 기법 ····· 42
4. 컨텍스트 기반 소프트웨어 리스크 평가 방법 ····· 44
5. 시험 기반 기법 ····· 46
제3절 소프트웨어 신뢰도 평가 방법론 비교 분석 ····· 50

제4장 소프트웨어 신뢰도 규제기준 및 사례 분석 ····· 51
제1절 국내 규제기준 및 사례 ····· 53
1. 한국 KINS ····· 53
제2절 국외 규제기준 및 사례 ····· 61
1. 미국 NRC ····· 61

2. 캐나다 CNSC ····· 70
3. 핀란드 STUK ····· 77

제5장 국내 소프트웨어 신뢰도 규제기술 개선방향 제안 ····· 83

제6장 결 론 ····· 87

참고문헌 ····· 91

서지정보양식 ····· 101

KAERI

표 목차

표 1. 정성적/정량적 소프트웨어 신뢰도 평가 방법론 비교 분석 ····· 50
표 2. 원전 계측제어계통 안전 등급 분류 ····· 54
표 3. 원전 계측제어계통별 소프트웨어 관련 규제지침 ····· 57

KAERI

그림 목차

그림 1. 소프트웨어 오류, 결함 및 고장의 관계 ····· 22
그림 2. 소프트웨어 HAZOP 수행절차 ····· 25
그림 3. 소프트웨어 HAZOP 가이드 워드 예제 ····· 26
그림 4. KNICS 소프트웨어 기능특성에 대한 위해도 분석결과 예시 ····· 27
그림 5. FMEA 워크시트 예제 ····· 28
그림 6. 디지털 원자로보호계통 ATIP 소프트웨어 FMEA 분석 사례 ····· 29
그림 7. 고장수목 분석모델 예시 ····· 30
그림 8. FBD 프로그램의 FTA 분석용 템플릿 ····· 31
그림 9. 원자로 트립 로직 소프트웨어 FTA 분석 예제 ····· 32
그림 10. 정형 기법 기반 소프트웨어 검증 절차 ····· 33
그림 11. 월성 SDS2의 FOD 분석 예시 ····· 34
그림 12. NuSCR Editor (NuSRS 2.0)을 활용한 정형명세 예시 ····· 35
그림 13. SMV 모델 체커를 활용한 정형검증 결과 예시 ····· 37
그림 14. KNICS BP 소프트웨어 SRS에 대한 정형검증 결과 예시 ····· 37
그림 15. FBD로부터 Verilog 코드 자동생성 및 SMV 분석 절차 ····· 38
그림 16. KNICS BP 소프트웨어 SDS에 대한 정형검증 결과 예시 ····· 39
그림 17. S-curve 모형에 근거한 원전 안전소프트웨어 결함 추정 예시 ····· 41
그림 18. 안전소프트웨어 결함 추정을 위한 BBN 모델 개발 예시 ····· 42
그림 19. TELLERFAST 소프트웨어의 상태천이도 및 천이확률 평가 예시 ····· 43
그림 20. PA-1 GN&C 시스템에 대한 DFM 모형 및 결과 예시 ····· 45
그림 21. LOCS 소프트웨어 시험용 CSFT-SS 시험환경 ····· 47
그림 22. 신한울1&2 RPS 소프트웨어 전수시험용 시뮬레이션 기반 시험 환경 ····· 48
그림 23. 원전 계측제어 계통 소프트웨어 관련 KINS 규제체계 ····· 56
그림 24. 안전등급 소프트웨어 생명주기 및 주기별 업무 ····· 57
그림 25. 원자력 안전계통 소프트웨어를 위한 NRC 규제요건 체계 ····· 63
그림 26. 소프트웨어 생명주기 업무 정의 ····· 66
그림 27. 디지털 계통 신뢰도 평가를 위한 NRC 연구 활동 ····· 67
그림 28. NRC DC 심사 중 소프트웨어 신뢰도 민감도 분석 결과 ····· 69
그림 29. 캐나다 CNSC의 원자력 안전 규제 체제 ····· 73
그림 30. 캐나다 DNGS 원자로 정지계통 구조도 ····· 75

그림 31. DNGS SDS1, SDS2 소프트웨어 시험 케이스 일부 ····· 76
그림 32. 원자력 관련 핀란드 규제기관 및 프로세스 ····· 77
그림 33. TXS PLC 플랫폼 및 응용 소프트웨어 로직 일부 ····· 81

KAERI

KAERI

제1장

서 론

제1절 연구 배경
제2절 연구 목적
제3절 연구 범위

KAERI

KAERI

제1장 서 론

제1절 연구 배경

원전 계측제어 (I&C; Instrumentation & Control) 계통은 원전 운전 상태를 감시하고 제어하며 비상시 안전 기능을 수행하는 계통으로 기존의 아날로그 I&C 계통의 부품 품귀 현상 및 높은 유지보수 비용 등으로 인해 디지털 I&C 계통을 적용하고 있다. 원전 디지털 I&C 계통은 하드웨어와 소프트웨어가 결합되어 주어진 기능을 수행하는데, 이중 소프트웨어 고장은 하드웨어 고장과 다른 특성 (설계 시 유입된 오류가 특정 입력에 의해 활성화되어 고장으로 발현)을 가진다. 따라서 소프트웨어의 신뢰도에 대해 기존 하드웨어와 별도의 분석 및 평가방법이 고려되어야 한다. 또한, 디지털 I&C 계통에서 동일한 소프트웨어를 사용하는 경우 공통원인고장 (Common Cause Failure; CCF)의 영향으로 해당 계통의 다중화 (Redundancy)를 무력화시킬 수 있으며, 이 경우 디지털 I&C 계통에 의한 제어신호가 올바로 발생되지 못함에 따라 안전 (Safety) 및 비안전 (Non-safety) 기능이 상실될 수 있다.

원전 운용에 있어서 안전성의 확인 및 보증이 무엇보다 중요한 사안임에 따라, 원자력 규제기관은 디지털 I&C 계통의 안전성 영향을 체계적으로 평가하고, 디지털 I&C 계통의 안전성을 보증할 것을 원전 사업자에게 요구하고 있다. 그러나 디지털 I&C 계통에 적용되는 원전 소프트웨어 신뢰도 평가 관련 규제 현안이 존재하여, 사업자 및 규제자 측면에서 원전 디지털 I&C 계통 인허가에 어려움을 겪고 있어 이를 해결할 수 있는 연구가 필요하다.

2014년 미국 Nuclear Regulatory Commission (NRC)에 신청한 설계 인증 (Design Certificate; DC) 심사과정에서는 프로그래머블 로직 컨트롤러 (Programmable Logic Controller; PLC) 플랫폼 기반으로 설계된 APR-1400 디지털 I&C 계통에 대한 첫 예비 질의에 '디지털 보호 계통의 소프트웨어와 하드웨어의 신뢰도를 각각 명확히 반영하라'는 항목이 있었다. 이러한 사례와 같이, 현재 원전 사업자 및 국내 규제기관은 원전 안전 소프트웨어의 신뢰도 정량화 및 규제방법론에 대한 명확한 대안을 제시할 것을 요구받고 있는 실정이다. 이에 따라, 가동원전의 디지털 업그레이드 시의 안전성 향상 및 신규 원전의 디지털 장비 도입 시의 계통 신뢰도 평가 등을 위하여 소프트웨어의 정량적 신뢰도 평가에 대한 규제입장의 정립이 필요하며, 이를 위한 소프트웨어의 정량화 방법론의 개발이 필요하다.

제2절 연구 목적

본 연구에서는 원전 디지털 I&C 소프트웨어 신뢰도의 정성적/정량적 평가 방법론 및 적용 사례들을 분석하고 국내 규제체계에 적용가능성을 검토하였다. 또한, 소프트웨어 신뢰도 관련

국내외 규제기준 및 적용 사례들을 분석하고 국내 규제기술의 개선방향을 제안하고자 한다.

제3절 연구 범위

본 보고서에서는 소프트웨어의 고장 특성 및 신뢰도 정의를 제2장에서 기술한다. 제3장에서는 정성적 및 정량적 소프트웨어 신뢰도 평가 방법론들의 특징 및 한계점에 대해 분석하며, 제4장에서는 소프트웨어 신뢰도 관련 국내외 규제기준 및 사례들을 기술한다. 제5장에서는 여러 기준 및 사례들을 바탕으로 소프트웨어 신뢰도 관련 국내 규제기준의 개선방향을 제안하며, 마지막으로 제6장에서 본 연구에 대한 결론과 시사점을 제시한다.

KAERI

제2장

소프트웨어 고장 특성 및 신뢰도 정의

제1절 소프트웨어 고장 특성
제2절 소프트웨어 신뢰도 정의

KAERI

KAERI

제2장 소프트웨어 고장 특성 및 신뢰도 정의

본 장에서는 원전 디지털 I&C 계통에 적용된 소프트웨어의 정성적 및 정량적 신뢰도 평가 방법론에 대한 선행 연구 및 기술 조사를 수행하였다. 아래 절에서 대표적인 소프트웨어 신뢰도 평가 방법론들에 대해 그 특성 및 한계점 등을 서술한다.

제1절 소프트웨어 고장 특성

ISO/IEC 표준 [ISO/IEC, 2015]에 따르면, 소프트웨어는 '정보 처리 시스템의 프로그램, 절차, 규칙 및 관련 문서화의 전부 또는 일부'로 정의하며, 실행 가능한 소프트웨어뿐만 아니라 펌웨어, 문서 (요구사항, 설계, 사용자 설명서 등) 및 데이터를 포함한다. 소프트웨어 실패와 관련하여, IAEA NP-T-1.5 [IAEA, 2009], IAEA NP-T-3.27 [IAEA, 2018]은 소프트웨어 결함(fault)과 소프트웨어 고장(failure)을 구분한다. 여기서 소프트웨어 결함은 '소프트웨어 오류(error)에 의해 야기되는 시스템이나 소프트웨어 상의 결점 상태 (Defective State)'로 정의하며, 소프트웨어 고장은 '촉발사건 (Triggering Event)에 의한 결함 (Fault)의 작동 결과'로 정의하였다. 소프트웨어 오류는 소프트웨어 생명주기 동안의 모든 개발 프로세스 및 운영 조건 중 발생한 실수 (인적 오류) 또는 결점 (설계 오류)들을 포함한다. IAEA NP-T-3.27에서는 소프트웨어 고장 원인에 대해 다음과 같이 기술한 바 있다.

- 소프트웨어는 요구된 대로 작동하지만, 특정 조건에서는 요구사항 정의 단계에서 잘못된 분석으로 인해 예상대로 작동하지 않는다.
- 소프트웨어는 요구된 대로 작동하지만, 발전소 장비나 운영 절차서의 개선 등에 기인하여 작동 환경이 변경될 수 있다.
- 소프트웨어는 부적절하게 설계되어 운영 서비스 이전에 수행된 V&V 등에 의해 검출되지 못한 잠재적 설계 오류로 남아있다면 이러한 오류는 소프트웨어 운영 수명 동안 소프트웨어 고장을 야기한다.

제조상의 결함, 노화 또는 환경적 영향으로 인해 무작위 고장의 대상이 되는 하드웨어 기기와 달리, 소프트웨어 고장은 그림 1과 같이 개발단계에서 내제된 오류 (검출되지 않은 잠재적 결함)가 소프트웨어 생명주기동안 무작위로 발생하는 촉발조건 (예: 임의의 하드웨어 기능 약화, 고장) 또는 메커니즘에 의해 활성화되어 나타난다. 여기서 소프트웨어 결함은 하나의 상태(State)이며, 소프트웨어 고장은 하나의 사건 (Event)이라는 차이가 있으며, 이는 결함촉발조건의 무작위 발생과 함께 소프트웨어 신뢰도를 확률적으로 다룰 수 있는 근거가 될 수 있다.

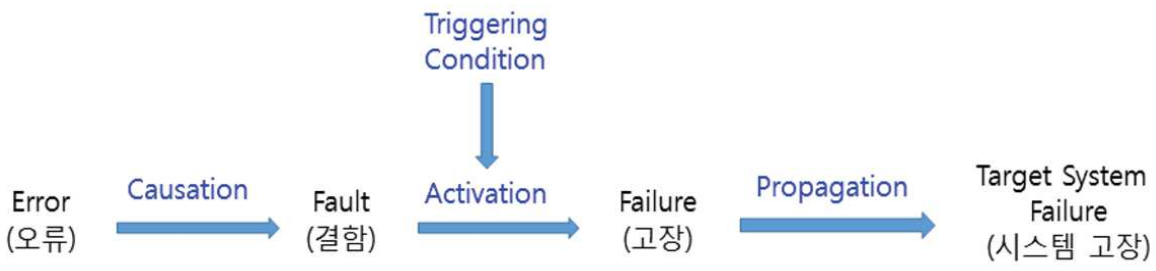


그림 1. 소프트웨어 오류, 결함 및 고장의 관계 [IAEA, 2018]

제2절 소프트웨어 신뢰도 정의

소프트웨어 신뢰도에 대한 관심 사항은 최종 목표 시스템의 고장을 발생시키는 소프트웨어 고장 확률을 평가하는데 있다 [장승철 외, 2019]. 일반적으로 소프트웨어 고장의 영향은 시스템 내부, 상호 연결 (Interconnected) 또는 종속적인 (Dependent) 시스템으로 파급되어 최종 목표 시스템의 고장으로 발현된다. 하지만 소프트웨어 기반 시스템은 구성 요소들로 쉽게 분해될 수 없고 구성 요소들의 상호 의존성은 쉽게 식별되거나 모델링될 수 없다. 이러한 복잡성 때문에 IAEA NP-T-3.27에서 식별한 3가지 소프트웨어 고장 메커니즘 중 어떤 것에 의해서도 영향이 없음을 완벽하게 증명할 수 없다. 따라서 소프트웨어 잔여 결함 (Residual Faults)에 대한 불확실성이 존재하며, 소프트웨어 신뢰도 모델링은 미해결된 문제로 남아있다. 다만, 소프트웨어 고장의 철학적 측면과 확률론적 모델을 사용하는 것에 대해서는 다음과 같이 전문가들의 공통된 의견 일치가 있었다 [Chu et al., 2009].

- 소프트웨어는 실패한다.
- 소프트웨어 실패의 발생은 확률적으로 처리될 수 있다.
- 소프트웨어 고장률과 확률을 사용하는 것은 의미가 있다.
- 소프트웨어 고장률과 확률은 디지털 시스템의 신뢰성 모델에 포함될 수 있다.

원전 확률론적 안전성 평가 (Probabilistic Safety Assessment; PSA) 모델에서 소프트웨어 고장을 고려하는 경우에는 일반적으로 소프트웨어 CCF만을 디지털 I&C 계통 고장수목에서 모델링하며, 공학적인 판단에 의해 소프트웨어 신뢰도 값을 가정하여 계통 신뢰도를 평가한다. 다만, 원전 산업계 및 규제기관에서 활용할 수 있는 소프트웨어 고장률 및 고장확률을 정량화하기 위해 다양한 소프트웨어 신뢰도 평가 방법론이 꾸준히 제안되어 왔으며, 여러 소프트웨어 기반 I&C 시스템들에 적용된 바 있다.

제3장

디지털 I&C 소프트웨어 신뢰도 평가 방법론 현황 조사

제1절 정성적 소프트웨어 신뢰도 평가 방법론

제2절 정량적 소프트웨어 신뢰도 평가 방법론

KAERI

KAERI

제3장 디지털 I&C 소프트웨어 신뢰도 평가 방법론 현황 조사

본 장에서는 원전 디지털 I&C 계통에 적용된 소프트웨어의 정성적 및 정량적 신뢰도 평가 방법론에 대한 선행 연구 및 기술 조사를 수행하였다. 아래 절에서 대표적인 소프트웨어 신뢰도 평가 방법론들에 대해 그 특성 및 한계점 등을 서술한다.

제1절 정성적 소프트웨어 신뢰도 평가 방법론

1. 소프트웨어 위험요소 및 운전분석 방법

위험요소 및 운전분석 방법 (Hazard and Operability Analysis; HAZOP)은 분석 대상 시스템의 위험을 찾아내고 분석하는 기법으로 발전소의 안전성을 평가하고 안전성 개선을 위한 설계 수정을 제안하는 데 사용되어 왔다. 특히, 시스템의 위험을 찾아내는 것뿐만 아니라 운영상에서의 문제들도 성공적으로 찾아내었기 때문에 발전소 위험 분석, 의학 진단 시스템, 도로 안전성 측정 등 여러 종류의 분야에 활용되고 있다 [Dunjo et al., 2010].

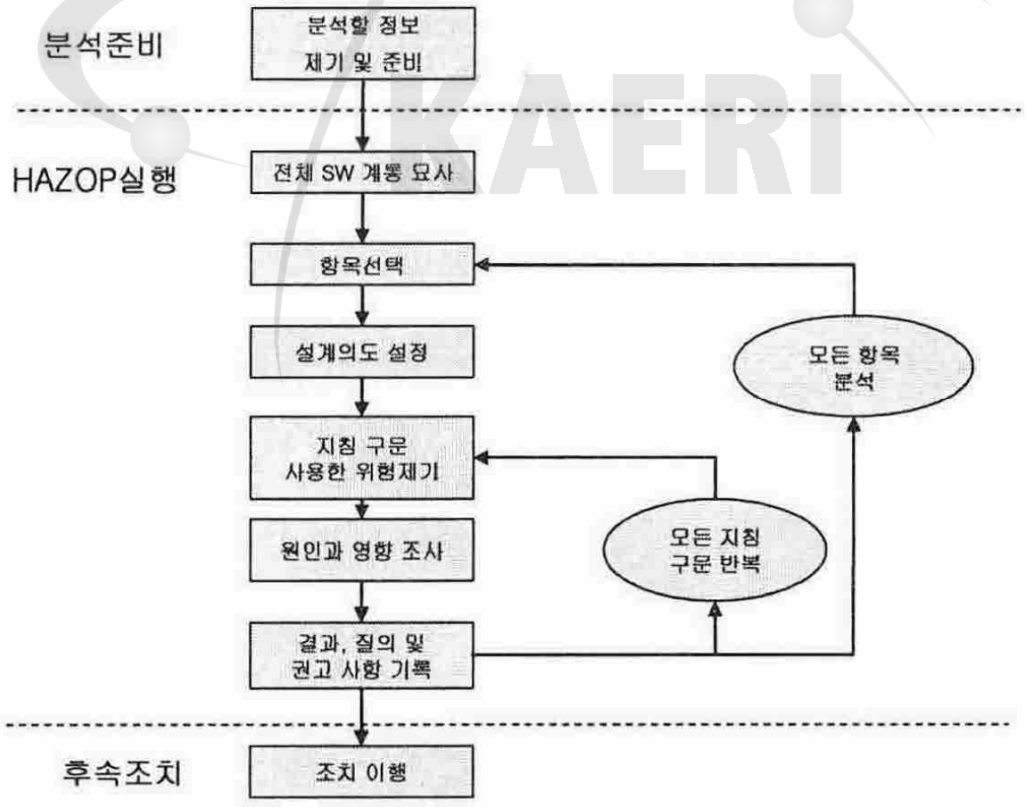


그림 2. 소프트웨어 HAZOP 수행절차 [이장수 외, 2003]

HAZOP은 시스템 기능이나 요건과 같은 매개변수와 HAZOP 가이드 워드 (Guide Word)를 조합하여 예상치 못한 시스템의 행위를 도출하고 도출된 시스템 행위가 시스템의 안전에 어떤 영향을 줄 수 있는지 분석한다. 소프트웨어 HAZOP은 'No', 'Less', 'More', 'Reverse', 'Also' 등의 소프트웨어 가이드 워드를 조합하여 소프트웨어의 예상치 못한 동작을 도출하며 소프트웨어 특징을 반영한 타이밍 가이드 워드가 추가된 워크시트를 활용한다 [Ericson, 2016]. HAZOP 워크시트 (Worksheet)는 일반적으로 분석 대상 시스템의 아이템, 기능/목적, 파라미터를 선정한 후 가이드 워드를 적용하여 위험성을 분석하는 단계로 진행된다.

미국 Lawrence Livermore National Laboratory (LLNL)는 소프트웨어 생명주기별 적용하는 위해도 분석에 사용하는 HAZOP 가이드 워드를 개발한 바 있다 [Lawrence, 1995]. 해당 가이드 워드는 IEEE Std. 379의 고장기준과 연관되도록 선정된 아이템에 대해서 표현 및 분석하기 위한 적합한 가이드 워드들을 선정하였다. 원자력 발전소의 HAZOP의 실제 적용 사례로는 Iranian Heavy Water Research Reactor (IHWRR)의 냉각시스템에 적용한 연구 [Mehdi et al., 2010]가 있으며, DICE (Detail ICE) 도출을 위해 기존에 수행된 원전 디지털 계측제어 시스템 FMEA 자료를 참고하였다. 캐나다 AECL (Atomic Energy of Canada Limited)은 소프트웨어 HAZOP 개발의 일환으로, Interim Defense Standard 00-58을 개발하였으며 해당 초안은 전통적인 HAZOP 단계를 따랐다 [AECL, 1993].

Quality	Aspect	Phase	Guide Phrases
Accuracy	Sensor	RADC	Stuck at all zeroes
		RADC	Stuck at all ones
		RADC	Stuck elsewhere
		RADC	Below minimum range
		RADC	Above maximum range
		RADC	Within range, but wrong
		RADC	Physical units are incorrect
		RADC	Wrong data type or data size
	Actuator	RADC	Stuck at all zeroes
		RADC	Stuck at all ones
		RADC	Stuck elsewhere
		RADC	Below minimum range
		RADC	Above maximum range
		RADC	Within range, but wrong
		RADC	Physical units are incorrect
		RADC	Wrong data type or data size

그림 3. 소프트웨어 HAZOP 가이드 워드 예제 [Lawrence, 1995]

국내에서는 한국원자력연구원이 디지털 계측제어 계통 소프트웨어 안전성 분석을 위해 소프트웨어 HAZOP을 수행하였으며, 그 결과를 요구사항 명세 안전성 분석 절차서 개발에 활용한 바 있다 [KAERI, 2008a]. 소프트웨어 HAZOP에 의한 안전성 분석은 NUREG/CR-6430 HAZOP 가이드 워드를 활용하여 소프트웨어가 의도된 동작에서 일탈이 일어났을 때 발생 가능한 시스템 위해도에 대하여 전문가 팀이 설계에 대한 의문을 제기하는 형식으로 수행되었다. 또한, 소프트웨어가 가질 수 있는 품질 특성, 성능, 기능성, 신뢰성, 강인성, 안전성, 보안성 등에 대한 가이드 워드를 개발하여 추가적인 체크리스트와 그 결과표를 개발하였다. 이를 위해 HAZOP 절차에 따라 위해 발생의 각 질문에 대한 원인, 공통원인을 기록하고, 이에 따라 초래될 수 있는 결과의 위험영향, 위험도 등을 파악하고 권고사항을 기록하였다.

이후, 해당 분석 결과는 한국원자력연구원이 개발한 KNICS 디지털 원전 안전계통 소프트웨어의 요구명세의 안전성 분석에 활용되었다. 소프트웨어 개발 단계별(요구사항 명세, 설계, 구현, 통합)로 NUREG/CR-6430을 참고하여 소프트웨어 대상의 HAZOP을 수행하였다 [KAERI, 2008a; 2008b; 2008c; 2008d]. 특히, 안전등급 PLC의 요구사항 공정특성에 대해 HAZOP 체크리스트를 이용하여 검토의견, 위험영향, 설계 권고사항 등을 포함한 종합적 안전성 검토를 실시하였으며 요구사항의 기능특성에 대해서도 상세 안전성 분석을 수행하였다.

품질 특성	적용 대상	Guide Phrases	Deviation Checklist	원인	공통 원인	위험영향 (결과)	위험도	권고사항	비고
성능	타이밍	Timer fail	타이머가 작동하지 않을 경우 어떠한 위험을 초래하는가?			WDT 작동불가	3		
		Interrupt latency occurs	인터럽트 지연이 발생하면 어떤 위험을 초래하는가?	스위칭 오류		Deadline 실패 가능성	4		
		Non-determ-inistic system behavior	타이밍이 비결정적일 때 어떤 위험을 초래하는가?	스케줄 에러		수행시간 예측불가	4		
	사이징	Memory chunk	메모리에서 mapping 되지 않은 ram chunk는 어떤 위험을 초래하는가?	단편화		메모리 낭비	3	static memory allocation 유도	
기능성		Function is not initialized properly before being executed	특정 기능이 각 동작 모드에 대해 명세 된 대로 수행하기 전에 적절히 초기화 되지 못할 때 어떤 위험을 초래하는가?	Reset 후 초기화 실패	연산, 변수 에러	데이터 무결성 침해	4	초기화후에만 기능이 수행될 수 있도록 함. 안전성 분석 추적 확인 필요함.	
보안성		Password system fail	비밀번호를 통한 시스템의 접근을 구현하지 못하면 어떠한 위험이 발생하는가?	어플리케이션 에러		보안 위협	4	초기화 부분에 사용자에 대한 인증도 고려	

그림 4. KNICS 소프트웨어 기능특성에 대한 위해도 분석결과 예시 [천세우 외, 2005]

이와 같이, HAZOP 방법론은 가이드 워드를 통해 다양한 관점에 대해 분석할 수 있고 잠재적으로 더 복잡한 타입의 위험한 사건과 원인을 알아낼 수 있지만 하나의 사건에만 초점을 두

고 있어 복합적인 사건에 대해서는 분석이 어렵다는 점과 가이드 워드와 관계없는 위해요소는 간과될 수 있다는 점이 있다. 또한, 분석자의 전문성과 충분한 교육이 필요하며 HAZOP 워크시트 작성에 많은 비용과 시간이 필요하다.

2. 소프트웨어 고장모드 및 영향 모델

고장모드 및 영향 분석 (Failure Modes and Effects Analysis; FMEA)는 서브시스템, 어셈블리, 컴포넌트의 잠재적인 고장 모드가 시스템에 미치는 영향을 상위 수준에서 분석하는 귀납적 분석 방법이며, FMEA 수행을 통해 시스템 위해 상태 등 의도하지 않은 시스템 상태에 대해 확인할 수 있다 [Ericson, 2016].

FMEA 수행에는 기능적 (Functional), 구조적 (Structural) 접근 방법이 존재한다. 구조적 접근 방법은 하드웨어와 하드웨어의 잠재적인 고장 모드에 대해 초점을 맞춘 접근 방법으로 시스템을 서브시스템, 유닛, 컴포넌트 단위로 모델링 하여 분석하는 방법이다. 기능적 접근 방법은 시스템, 서브시스템, 유닛 등이 의도한 기능을 수행하는가에 대해 분석하는 방법으로, 소프트웨어에 대해서는 기능적 접근을 취해 소프트웨어의 기능을 대상으로 하여 FMEA를 수행할 수 있다. FMEA 수행은 관련 데이터를 수집한 후, 워크시트 (Worksheet)를 작성하는 방향으로 수행한다. 그림 5는 FMEA 워크시트의 예제로, 대상 아이템 확인, 대상 아이템의 잠재적인 고장모드 확인, 확인한 대상의 잠재적인 고장모드로부터의 영향 등을 분석하게 된다. 최종적으로는 시스템의 잠재적인 고장모드 및 영향을 분석하여 시스템의 위험요소, 위해도 평가를 수행한다.

Failure Mode and Effects Analysis										
System:			Subsystem:				Mode/Phase			
Item	Failure Mode	Failure Rate	Causal Factors	Immediate 1. Effect	System Effect	Method of Detection	Current Controls	Hazard	Risk	Recomm Action

그림 5. FMEA 워크시트 예제

FMEA를 적용한 사례로 한국원자력연구원은 KNICS 원자로보호계통 자동시험 및 연계 프로세서 (Automated Test Interface Processor; ATIP) 소프트웨어를 대상으로 FMEA를 수행한 바 있다 [KAERI, 2008e]. 이후, 원전 소프트웨어 전용 FMEA 템플릿을 개발하여 안전 관련 소프트웨어를 분석하였다 [Park et al., 2014]. 대상 소프트웨어의 시스템은 디지털 원자로 보호 계통 내 ATIP 소프트웨어이며, 전체 시스템을 대상으로 위해도 분석을 수행 후 소프트웨어 FMEA를 각각의 소프트웨어에 적용하였다. 그림 6는 분석 대상 소프트웨어에 대해 수행된 FMEA 워크시트 결과의 일부이다.

Software FMEA analysis results for "Channel 3 Equipment Check" sub-module.

Sub-module	Failure mode	Failure cause	Failure effect	Failure detection/comments
Other Channel 3 Equipment Check	Omission	Omission in equipment diagnosis or heartbeat monitoring functions	Periodic automatic test is affected adversely	There is no update procedure for a variable AL_1_ATIP_ATIPD_PHBC.→ Channel A, B, and C cannot recognize when the channel D HB is malfunctioning
	Incorrect realization	There is an error in equipment diagnosis or heartbeat monitoring functions	Malfunction in Channel 3 equipment diagnosis	No failure detected
	Unintended addition	Additional functions in equipment diagnosis or heartbeat monitoring functions	There is no effect on equipment diagnosis	No failure detected
	Function interaction	Inappropriate location of implementation of a function	There is an degradation in this module	No failure detected
	Input definition	Wrong input definition, assignment, address, or type definition	Malfunction in Channel 3 equipment diagnosis	No failure detected
	Input value	Wrong min/max limits or initialization value in heartbeat coefficients	Malfunction in monitoring of channel D ATIP heartbeat signal	No failure detected
	Input timing	An input variable is used before updating	Delay in processing the input signal	No failure detected
	Input format	Omission/addition of an interver, wrong input number, or input disorder	Malfunction in Channel 3 equipment diagnosis	No failure detected
	Output definition	Wrong output definition, assignment, address, or type definition	Malfunction in Channel 3 equipment diagnosis	No failure detected
	Output value	Wrong assignment of an output value	Malfunction in Channel 3 equipment diagnosis	No failure detected
	Output timing	Wrong timing for generating an output value	Malfunction in Channel 3 equipment diagnosis	No failure detected. (Output from this submodule is correctly used in the next step.)
	Output format	Omission/addition of an interver, wrong output number, or input disorder	Malfunction in Channel 3 equipment diagnosis	No failure detected

그림 6. 디지털 원자로보호계통 ATIP 소프트웨어 FMEA 분석 사례 [Park et al., 2014]

항공분야는 오랜 기간 FMEA가 사용되어 온 분야로, 베이징대학교 Zhang 교수팀은 항공기 제어 컴퓨터 시스템 소프트웨어에 대해 소프트웨어 FMEA를 수행한 바 있다 [Xu et al., 2013]. 해당 분석에서는 소프트웨어의 모듈별 고장모드를 확인하고 그 원인을 확인하는 형태로 수행되었다.

이러한 예시들에서 확인할 수 있듯이, FMEA를 수행하면 고장모드로부터 인과관계를 체계적으로 규명함으로써 치명적 결함을 발생 시킬 수 있는 소프트웨어 고장모드에 대해 파악할 수 있다는 점과, 기법 자체가 이해하기 쉽고 적용하기 쉽다는 장점이 있다. 다만, 다른 분석기법처럼 구성 요소 간의 상세한 연관관계나 종속성에 대한 정보를 제공하지 않기 때문에 FMEA 수행을 위해서는 충분한 경험과 지식을 갖춘 전문가가 필요하다. 또한, FMEA 고장모드와 연관되지 않은 위해도 분석에 대한 내용이 부족하고, 인적오류 등 외부 영향에 대한 고려가 부족하다는 한계점이 있다.

3. 소프트웨어 고장수목 분석

고장수목 분석 (Fault Tree Analysis; FTA)은 전자, 전기, 원전 등의 분야에서 많이 사용되는 고장 해석 및 신뢰성 평가 기법으로 최상위 사건으로부터 탑-다운 (Top-down) 방식으로 기본 사건까지의 순차적 원인 분석을 통해 수목 (Tree) 형태의 모델을 작성하는 방법이다. 최상위 사건은 대상 시스템/소프트웨어의 고장 또는 사고가 해당된다. 고장수목 모델은 시스템의 고장을 정의하고, 고장을 발생시킨 원인을 연역적 방법을 통해 논리적으로 분석하는 형태로 수행되며 체크리스트, 공통모드고장 분석과 같은 기법으로 사용되기도 한다 [Ericson, 2016]. 고장수목 작성은 최상위 사건을 설정한 후에 순차적으로 상위 사건의 발생원인 분석, 상위 사건과 원인을 게이트로 연결, 원인이 분할될 수 없는 기본 사건이 될 때까지 반복 순으로 작성하며, 사건들 간에 연결은 이진 표현 (Boolean Expression)을 이용한다. 수목 작성 후 고장 수목의 최상위 사건 발생에 영향을 미치는 요소를 파악하기 위해 최상위 사건을 발생시키는 사건의 최소 집합인 최소절단집합 (Minimal Cut Set)을 분석한다.

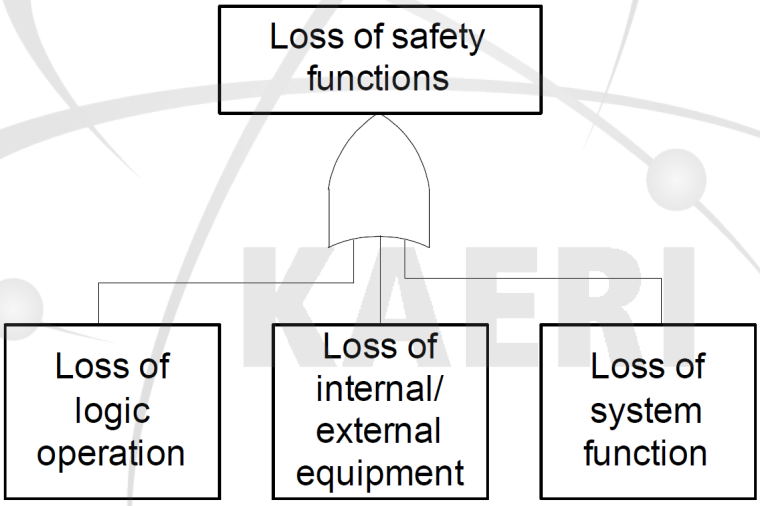


그림 7. 고장수목 분석모델 예시

FTA를 적용한 사례로 건국대학교 유준범 교수팀은 원전 계측제어 소프트웨어의 정형 요구사항과 설계 프로그램을 분석하였다 [Yun et al., 2010]. 해당 분석은 원자로 보호 계통 소프트웨어를 정의한 정형 요구사항 명세 언어를 대상으로 하여 고장수목을 자동 생성하였으며, 생성된 고장수목에 대한 FTA를 수행하였다. 또한 원전 안전등급 계측제어 시스템 소프트웨어 설계에 사용되는 Function Block Diagram (FBD) 언어를 고장수목으로 자동으로 변환하여 FTA 분석을 수행하였다. 그림 8은 FBD의 FTA분석을 위해 사용된 템플릿으로 FBD 작성 시 사용하는 각각의 Function Block에 대해 템플릿을 만들고, 템플릿을 이용하여 FBD로 작성된 소프트웨어를 분석하는 방식으로 수행하였다.

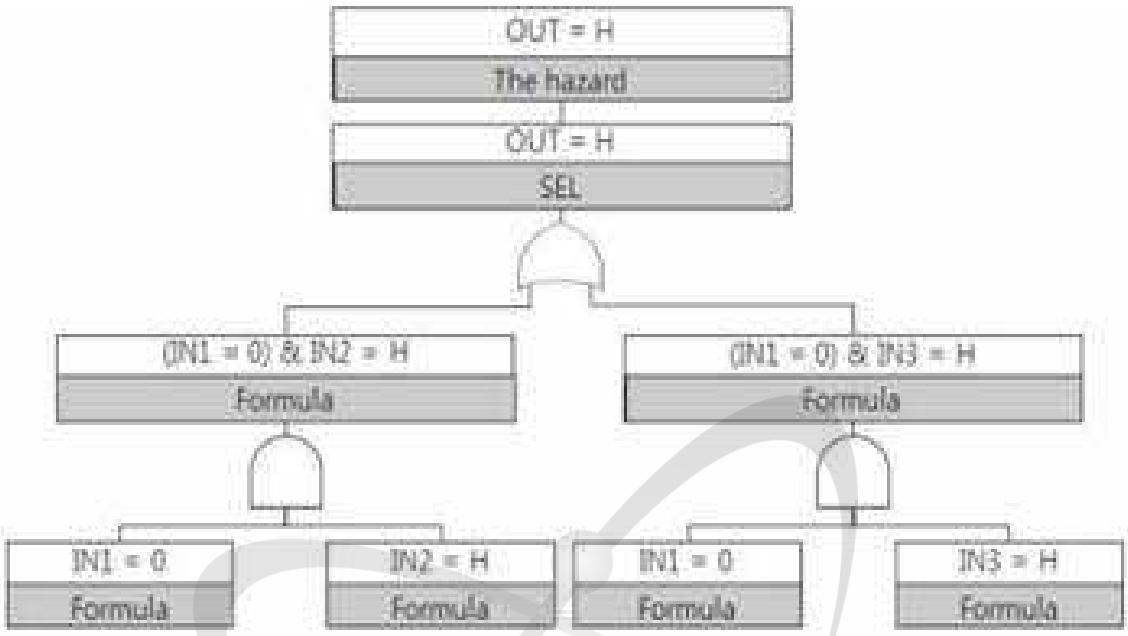


그림 8. FBD 프로그램의 FTA 분석용 템플릿

한국원자력연구원은 원자력 안전등급 소프트웨어 설계단계에서 FTA 분석을 적용하였으며 원자로 보호 계통 소프트웨어를 대상으로 사례연구를 수행하였다 [Park et al., 2008]. 해당 연구는 설계단계의 FBD를 이용하여 고장수목을 생성하였으며 기존의 FBD용 고장수목 템플릿을 바탕으로 오류 지향적 (Fault-oriented) 템플릿을 개발하였다. FBD 생성 시 복잡성과 크기가 커지는 문제점을 해결하고자 소프트웨어 HAZOP을 통해 주요 포인트를 우선적으로 식별하여 선별된 FBD를 대상으로 FTA를 수행하였다.

그림 9는 원자로 트립 컨디션이 만족되었음에도 불구하고 트립 로직이 False 인 경우에 대해 개발된 고장수목도이다. 이를 통해 해당 로직이 어떻게 의도하지 않은 경우에 도달하게 되는지 경로를 찾을 수 있고, 이를 바탕으로 추후에 시험 및 시뮬레이션을 위한 시험 케이스 작성에 도움을 줄 수 있다. 해당 연구를 바탕으로 KNICS 원자로보호계통 소프트웨어에 대해 소프트웨어 설계, 구현 단계에서 사용한 FBD을 대상으로 FTA를 수행하였다 [KAERI, 2008c; 2008d].

고장 수목을 이용한 위해도 분석의 장점은 사고 원인을 수목으로 분석하기 때문에 일반화시킬 수 있다는 장점이 있고, 간편화 할 수 있다. 또한 나아가 정량화 데이터를 FTA에 입력함으로서 정점 사건에 대한 확률 계산을 통해 사고를 예측 할 수 있다. 도출된 최소절단집합은 향후 소프트웨어 개발 및 확인 및 검증 (Verification and Validation; V&V)을 위한 체크리스트로도 사용 할 수 있으며, 사고 발생에 기여하는 기본 사건을 파악함으로써 사고 예방

을 위한 비용을 줄일 수 있다는 장점이 있다. 하지만 고장수목은 전문가에 의해 작성해야 하며 분석 자체에 많은 비용이 소모될 수 있다. 또한, 정점사건의 확률 계산을 위해서는 각각의 기본 사건의 발생 확률을 계산해야 하며 고장수목 모델링에 활용되는 AND와 OR 논리 게이트만으로 소프트웨어 논리를 표현하기 어렵다는 단점이 있다.

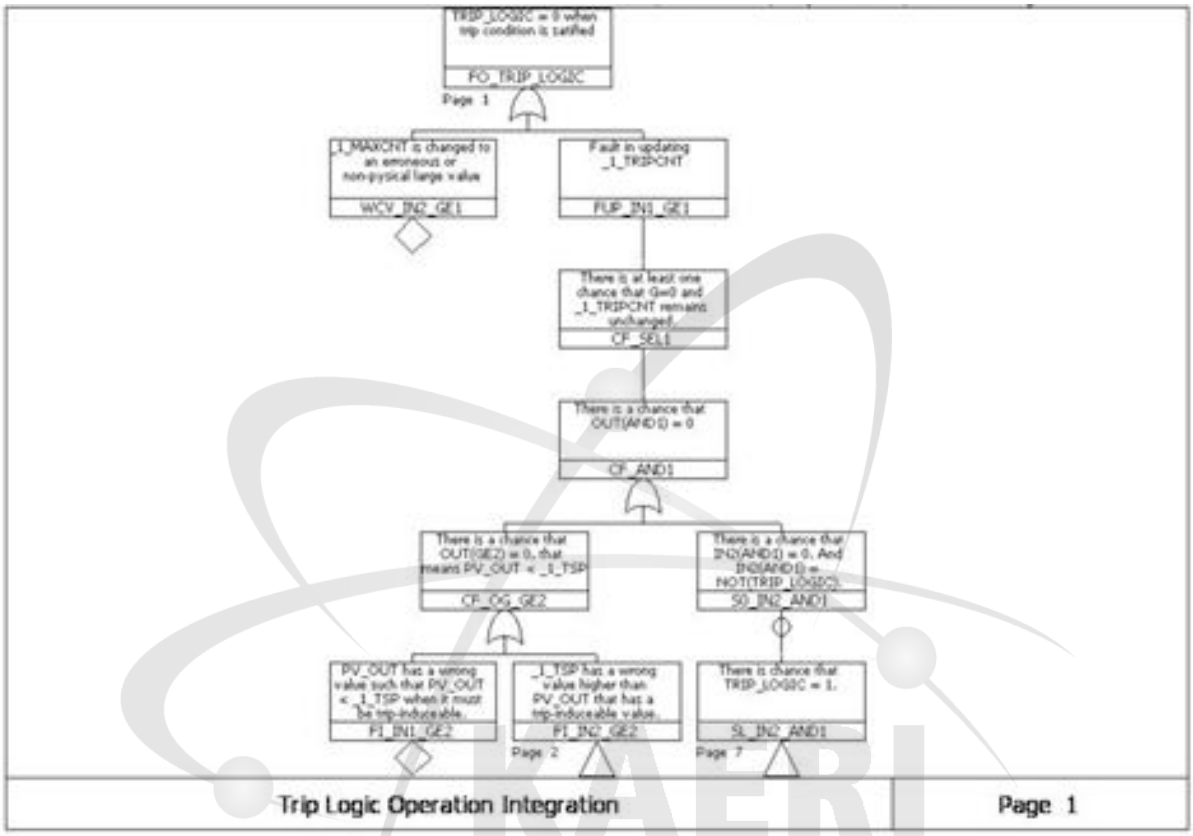


그림 9. 원자로 트립 로직 소프트웨어 FTA 분석 예제

4. 소프트웨어 정형 기법

일반적으로 소프트웨어는 요구사항 분석, 설계, 구현, 시험, 유지보수 등의 주기에 따라 개발된다. 이 중, 요구사항 분석단계는 소프트웨어의 품질과 안전성에 가장 중요한 역할을 하며 자연어로 되어있는 요구사항 명세는 많은 모호성을 가져 검증을 수행하기 힘들다는 단점이 있다. 소프트웨어로 인한 많은 사고들이 소프트웨어 요구사항 오류에 기인하고 있으며, 요구사항 단계에서 생기는 오류는 구현 등의 단계에서 생기는 오류보다 매우 큰 수정 비용을 필요로 한다. 이러한 문제점의 해결을 위해 요구사항에 대한 엄격한 명세와 검증을 위해 모호성을 제거하고, 검증을 수행하기에 용이하게 할 수 있는 정형 기법이 소프트웨어에 대한 안전성, 신뢰성, 확실성, 무결성 등이 중요하게 요구되고 있는 항공우주 및 원전 분야 등에 활용되고 있다.

정형 기법이란 소프트웨어 공학의 일종으로 오류가 없는 시스템을 설계하여 시스템의 신뢰

성을 높이려는데 목적이 있다 [Kotonya et al., 1998]. 이러한 정형 기법은 수학적 기호를 사용함으로 설계된 사용자의 요구조건과 동일한지 수학적인 성질을 이용하여 증명할 수 있는데, 크게 정형 명세와 정형 검증으로 나눌 수 있다. 정형 명세는 시스템이 달성해야 하는 요구 사항과 그러한 요구 사항을 만족시키는 설계를 묘사하는데 그 목적이 있고, 정형 검증은 그 설계가 요구사항을 만족하는지를 검사하는 일련의 과정을 의미한다.

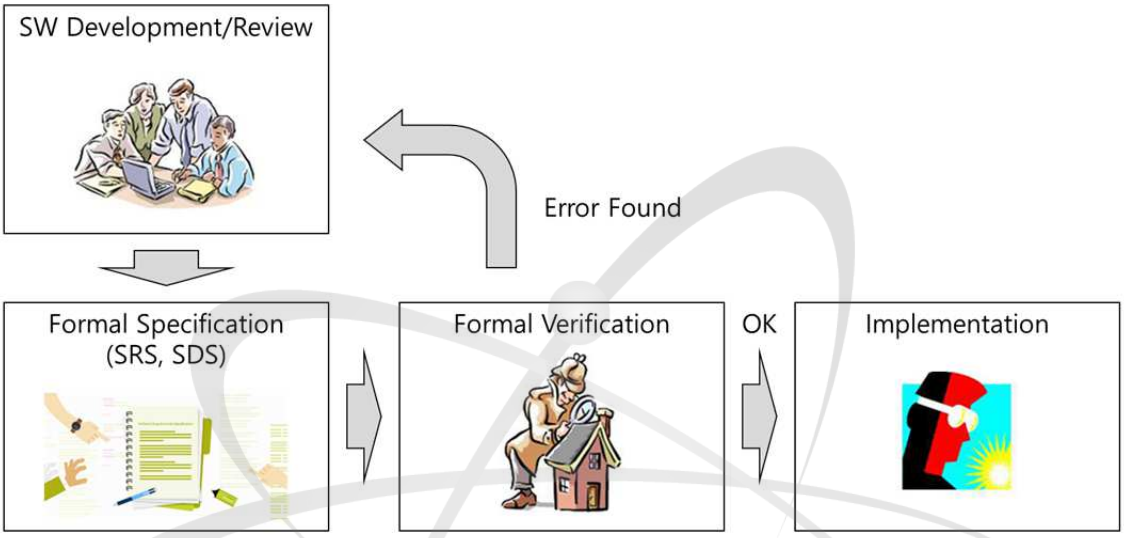


그림 10. 정형 기법 기반 소프트웨어 검증 절차

정형 명세는 수학적 논리 기호식이나 의미가 명확한 다이어그램 등을 그래픽 표현을 사용해서 명세를 작성하는 기법을 말한다. 명세는 시스템이 무엇을 만족해야 하는가를 정의하고, 시스템이 어떻게 이루어져 있는가를 나타냄으로서 시스템의 동작 환경, 요구사항, 설계 등을 기술하는 것이다. 정형 명세는 소프트웨어 개발 초기단계에서 개발자가 모든 요구 사항들을 생략하지 않고 명확하게 명세하도록 유도함으로써 소프트웨어의 안전성을 향상시킬 수 있는 기법이다. 정형 명세 언어로서는 크게 State-diagram과 같은 도식적인 명세 언어와 논리식이나 프로세스 대수 (Process Algebra)와 같은 수학적 기호와 문자를 사용하는 언어가 사용되며 널리 쓰이는 방법으로는 Statecharts, Software Cost Reduced (SCR), Esterel, Z 등이 있다.

특히, SCR은 안전성이 중요한 시스템의 소프트웨어 요구사항을 기술하기 위한 테이블 기반 정형 명세기법이다 [Heitmeyer et al., 1998]. SCR에서 하드웨어 인터페이스는 입력과 출력 데이터 아이템과 소프트웨어 기능으로 기술되며, 소프트웨어 기능은 조건 테이블, 이벤트 테이블, 모드 전이 테이블의 세 가지 테이블 (수학적 함수를 정의)의 집합으로 이루어져 있다. SCR이 시스템이나 소프트웨어를 표현할 때 유한상태 기계 (Finite State Machine)를 사용한

다. SCR 명세는 Monitored Variable과 Controlled Variable이라는 두 환경 변수를 정의하는데 Controlled Variables는 시스템을 제어하거나 시스템에 영향을 주는 물리적 양을 나타내는 환경 변수이고, Monitored Variables는 단지 시스템을 측정하고 감시하는 환경 변수이다. 작성된 SCR 명세는 변수들의 값을 가지고 시뮬레이션도 할 수 있으며 SCR tool을 통해 검증을 할 수도 있다.

정형 명세의 적용사례로는 캐나다 AECL (Atomic Energy of Canada Limited)이 SCR을 활용하여 Darlington 발전소 소프트웨어에 대한 명세 및 검증을 수행한 바 있다 [Parnas et al., 1993]. 해당 방법론은 자연어로 기술되어있는 기능 요구 명세 (Functional Requirement Specification; FRS)를 SCR 언어 표기법을 이용하여 정형화된 언어로 나타내었다. 이는 원전안전계통 소프트웨어에 적용된 최초의 정형 명세 기법이며 한국 월성 2, 3, 4호기 안전계통인 정지계통-2에도 해당 기법이 적용되었다 [WNPP, 1993]. 다만, 해당 연구에서는 정형 기법을 요구사항 명세 단계만 적용하였으며, V&V 절차에는 적용하지 못하였다 [WNPP, 1994].

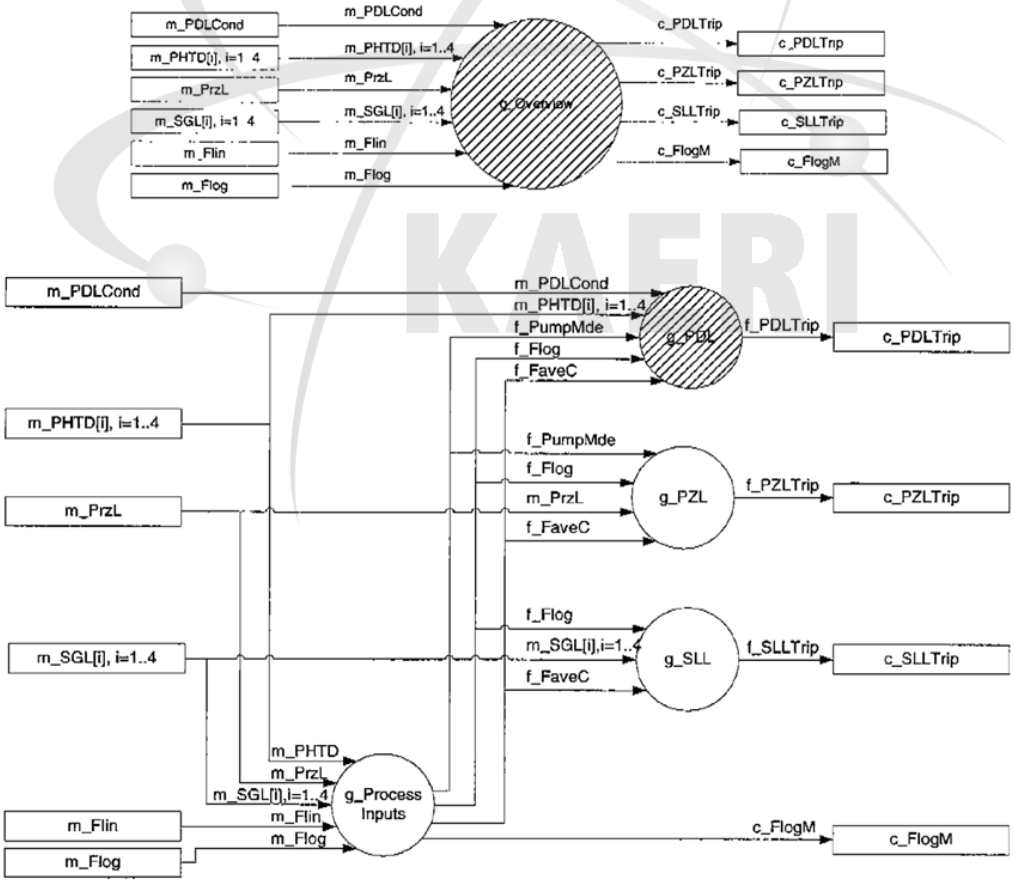


그림 11. 월성 SDS2의 FOD 분석 예시 [김태호 외, 2002]

국내에서는 한국원자력연구원이 기존의 AECL의 SCR에 기반하는 방법론을 수정, 보완하여 원전 디지털 계측제어 계통 내 소프트웨어를 명세하는 데 보다 유용하게 사용될 수 있는 NuSCR을 개발하였다 [Yoo et al., 2005]. 해당 방법론은 NuSCR과 마찬가지로 Parnas' Four-Variable Model [Parnas et al., 1991]에 기초하며 모델에서 정의되는 관계를 보다 명확하게 명세하기 위해서 세 가지의 추가적인 변수 모델 (Function Variable, History Variable, Timed-history Variable)을 사용했으며, 이는 Structured Decision Table (SDT), Finite State Machine (FSM), Timed Transition System (TTS)를 이용해서 표현되었다.

NuSCR은 각각 다른 특징을 가지는 변수들을 혼용함으로써 소프트웨어를 보다 명확하게 명세할 수 있으며 이를 위하여 Function Overview Diagram (FOD)을 이용하여 데이터 흐름을 나타낸다. 각 변수들은 그림 12과 같이 실행 순서에 의한 상관관계를 지니는 노드로 표현되며 각 노드들은 입력, 출력을 가진다. NuSCR로 작성된 정형 요구사항 명세서는 기존의 자연어 명세에서 발생되었던 모호성, 불일치성 등의 문제를 해결 할 수 있을 뿐만 아니라, 추가적으로 요구사항명세에 대한 수학적인 정형 검증을 가능하게 해준다.

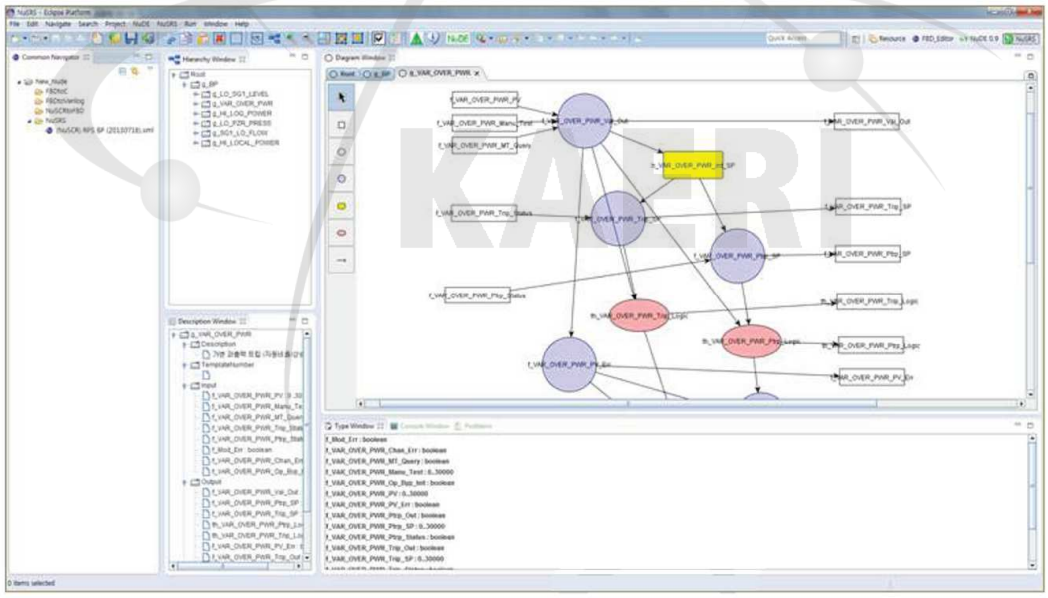


그림 12. NuSCR Editor (NuSRS 2.0)을 활용한 정형명세 예시

정형 검증은 정형 논리 또는 수학 논리 등에서 제공하는 증명 방법을 이용하여 정형 명세를 분석하여 시스템 설계 및 요구사항의 만족여부를 검사하는 것을 말한다. 일반적인 코드 조사 (Inspection) 및 소프트웨어 시험은 프로그램이 입력 값의 모든 가능한 조합을 통해 올바르게 동작하는 것을 보여주기 위한 기술들의 모음으로 구성한다. 하지만 시험 데이터의 모든 가능

한 조합을 통해 프로그램을 시험하는 것은 물리적으로 불가능한 경우가 많으므로, 정형 검증은 프로그램의 전체적인 정확성을 설명하려 하며 자동적인 정리 증명과 그래프 이론에 근간한다. 정형 검증 기법에는 크게 두 가지가 있는데, 하나는 모델 체킹 (Model Checking) 방법 [Emerson et al., 1986]이며 다른 하나는 정리증명법 (Theorem Proving) [Dalem, 1994]이다. 모델 체킹은 유한 상태의 병렬 시스템을 자동으로 검증해 주고 항상 원하는 결과가 나옴을 수학적으로 증명해 주는 기법으로 SMV (Symbolic Model Verifier), VIS (Verification Interacting with Synthesis), SPIN (Simple Promela INterpreter) 등의 방법이 여기에 속한다. 정리증명법은 논리수학식을 사용해서 수학적으로 증명하는 기법으로 PVS (Prototype Verification System) 방법을 들 수 있다.

모델 체킹 방법론은 기존의 모의실험, 시험 및 연역적 추리를 기반으로 시스템을 검사하는 방법보다 뛰어난 검증 방법으로 평가되며, 유한 상태 동시 시스템을 검증하기 위한 오토마타 기반의 기술이다. 상태 전이 시스템 (State Transition System)과 특성이 주어지면, 모델 체킹 알고리즘은 시스템이 원하는 특성을 만족하는지를 알아보기 위해서 전체 상태 공간 (State Space)을 검사한다.

가장 대표적인 모델 체킹 도구로서 SMV는 유한 상태 시스템이 Computational Tree Logic (CTL)로 표현된 요구 명세를 만족하는 지를 자동으로 검증하며 상태들의 집합과 이들 간의 전이 관계를 Binary Decision Diagram (BDD)로 표현한다 [McMillan, 1993]. 주로 하드웨어 디자인의 정형 검증을 위해 사용되며 SMV 언어로 모델링된 시스템이 시제 논리 (Temporal Logic)으로 기술된 특정 속성을 만족하는지 분석할 수 있다. 다만, SMV 언어가 유한 상태 시스템을 위해 만들어진 것이기 때문에 언어가 제공하는 자료 구조도 유한한 형태 (Boolean, Scalar, Fixed Array 등)만을 제공하여 요구명세를 CTL로 명세해야만 하므로 표현력이 제한될 수 있다는 단점이 존재한다. 후속 연구들에서 NuSCR로 작성된 정형 명세 및 FSM, TTS, FOD를 SMV를 이용하여 정형 검증을 수행할 수 있는 템플릿이 개발된 바 있다 [조재명, 2003].

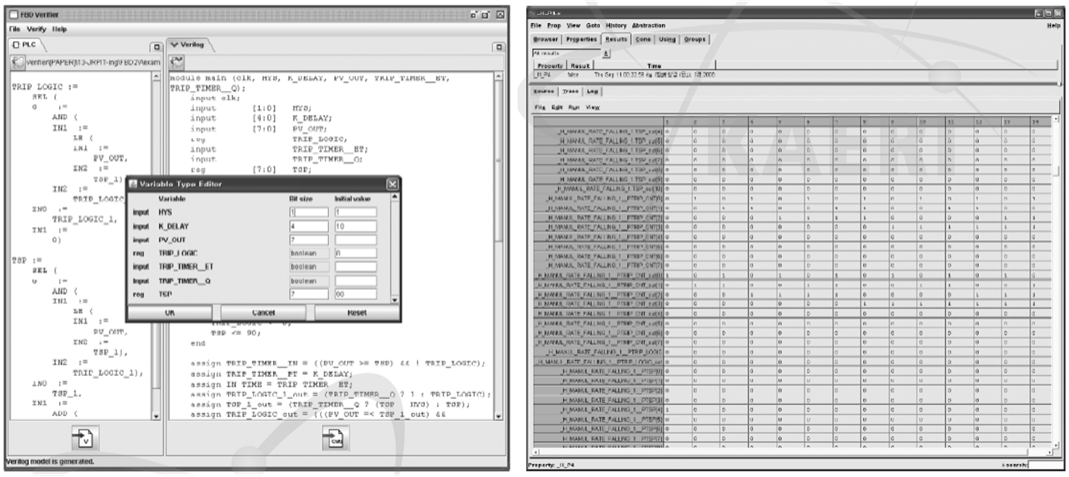


그림 13. SMV 모델 체커를 활용한 정형검증 결과 예시 [지은경 외, 2011]

정형 검증의 적용사례로는 한국원자력연구원이 원전 계측제어 시스템 소프트웨어 요구사항 명세에 특화된 NuSCR 명세를 모델체킹하기 위해 NuSCR 명세를 SMV로 변환하는 알고리즘 및 도구 (NuSRS)를 개발하여 디지털 보호논리 소프트웨어 요구사항 명세 (SRS)에 대한 정형 검증을 수행한 바 있다 [지은경 외, 2011]. 해당 연구는 비교논리프로세서, 동시논리프로세서, 자동시험연계프로세서에 대한 NuSCR 명세에 문법적 및 의미적 오류를 검토하고 수정하였으며 정형 검증을 수행하기 위해서 전문가와 상의하여 소프트웨어 안전성에 필수적인 검증속성들 (명세의 완전성 검증, 트립 조건 시 트립이 발생해야 함 등)을 추출하였으며 이들을 SMV 모델 체커의 입력이 되는 CTL 시제논리 형태로 기술하였다. 이후 각 점증마다 검증 대상, 검증속성, 검증결과를 기록하여 모델체킹 속성이 만족되지 않은 경우에는 SRS 상의 어떤 부분에서 어느 이유 때문에 오류가 발생하였는지 분석하였다.

대상	검증속성	검증속성 의미	검증결과	분석결과
f_HI_LOG_POWER_Op_Byp_Init	AG !(FROM-_init_-TO-s0-taken & FROM-_init_-TO-s1-taken))	초기상태에서 운전우회개시신호가 발생되는 조건과 발생되지 않는 조건이 동시에 만족되는 경우는 없다.	true	f_HI_LOG_POWER_Op_Byp_Init SDT 명세의 일관성을 확인함
	AG (in-_init_ -> AX ! in-_init_)	초기상태에서는 반드시 다음 상태로 전이가 되어 출력변수 값이 결정된다.	true	f_HI_LOG_POWER_Op_Byp_Init SDT 명세의 완전성을 확인함
	AG (f_HI_LOG_POWER_Opb_Perm_In = true & (f_HI_LOG_POWER_Opb_Rqst_MCR = true | f_HI_LOG_POWER_Opb_Rqst_RSR = true) -> AF f_HI_LOG_POWER_Op_Byp_Init = true)	운전우회 허용신호가 들어오고, 주제어반 운전우회 요청 또는 원격정지반 운전우회 요청이 들어오면 운전우회 개시 신호가 발생된다.	true	검증속성이 만족됨을 확인함
f_HI_LOG_POWER_OB_Err	AG !(FROM-_init_-TO-s0-taken & FROM-_init_-TO-s1-taken)	초기상태에서 운전우회오류가 발생되는 조건과 발생되지 않는 조건이 동시에 만족되는 경우는 없다.	true	f_HI_LOG_POWER_OB_Err SDT 명세의 일관성을 확인함
	AG (in-_init_ -> AX ! in-_init_)	초기상태에서는 반드시 다음 상태로 전이가 되어 출력변수 값이 결정된다.	true	f_HI_LOG_POWER_OB_Err SDT 명세의 완전성을 확인함
	AG (f_HI_LOG_POWER_Opb_Perm_In = false & (f_HI_LOG_POWER_Opb_Rqst_MCR = true | f_HI_LOG_POWER_Opb_Rqst_RSR = true) -> AF (f_HI_LOG_POWER_OB_Err = true))	운전우회 허용신호가 들어오지 않은 상태에서, 주제어반 운전우회 요청 또는 원격정지반 운전우회 요청이 들어오면 운전우회 오류 신호가 발생된다.	true	검증속성이 만족됨을 확인함

그림 14. KNICS BP 소프트웨어 SRS에 대한 정형검증 결과 예시

해당 연구는 추가적으로 원자로 보호 계통 소프트웨어 설계 명세 (Software Design Specification; SDS)에 대해 모델 체킹 기법을 이용하여 정형 검증을 수행한 바 있다. 소프트웨어 요구 명세와는 다르게 설계 명세는 PLC 프로그래밍 언어인 FBD로 기술되어 있기 때문에 FBD를 PLCVerifier 도구를 사용하여 Verilog로 변환하고 변환된 코드에 검증할 속성을 삽입하고 Cadence SMV 모델 체커를 이용하여 검증을 수행하였다. 검증 수행에 필요한 주요 검증 속성은 전문가와 상의하여 추출되었으며 추출된 속성들은 각각의 공정 변수들에 대하여 적용되었다. 요구 명세와 마찬가지로, 설계 명세도 각 검증마다 검증대상, 검증속성, 검증결과를 기록하였으며 모델 체킹 속성이 만족되지 않은 경우에는 FBD와 자연어로 작성된 설계 명세 상의 어느 부분에서 어떤 이유 때문에 오류가 발생하였는지 분석하였다. 해당 연구의 결과, 원자로 보호 계통 요구 명세의 경우 비교논리프로세서, 동시논리프로세서, 자동시험연계프로세서 각각 130개, 87개, 136개의 오류를 발견하였으며 설계 명세의 경우 각각 46개, 13개, 46개의 오류를 발견하였으며, 소프트웨어 수정의 입력으로 활용하였다.

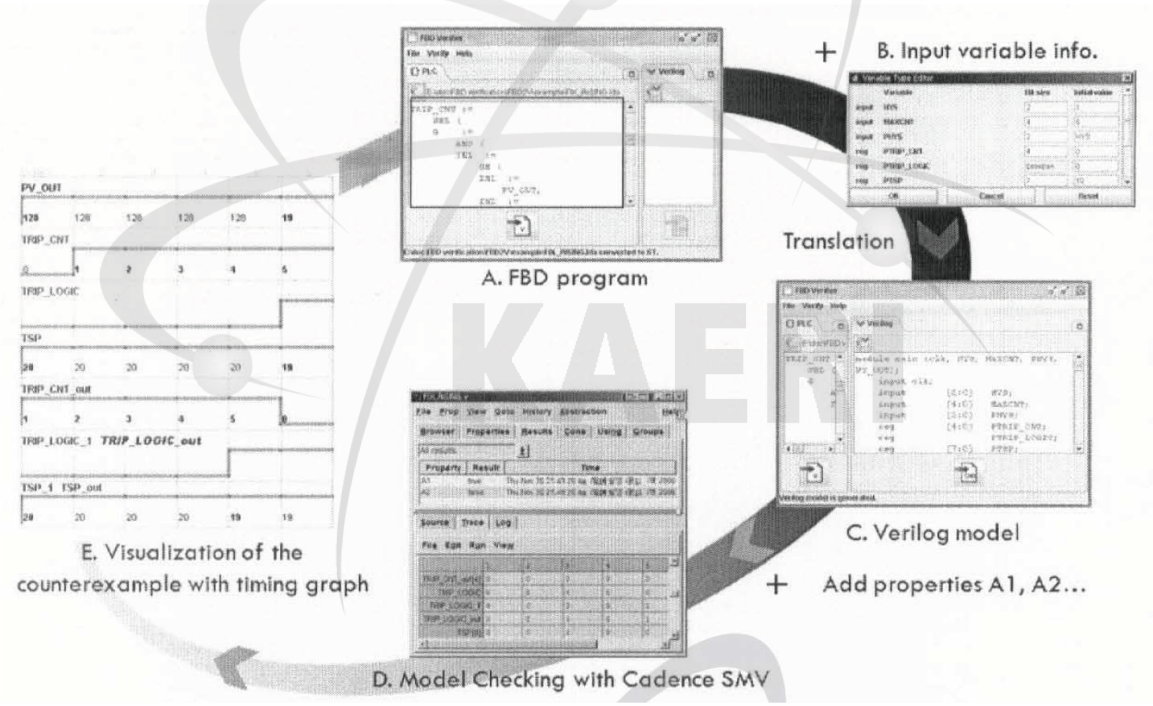


그림 15. FBD로부터 Verilog 코드 자동생성 및 SMV 분석 절차

3.4 트립논리 모듈(7.2.4) > 가압기 고압력 트립 모듈(7.2.4.1) 모델체킹 결과

- 고정설정치 상승트립
- SDS 검토사항 (p. 51~54)
  - p.53, 7.2.4.1 가압기 고압력-고정형 설정치 상승 비교논리 블록의 <블럭논리> (3)에서 주석 및 논리에는 (공정값 <= TSP)로 기술되어 있으나, FBD 상에는(FIX_RISING 사용자 정의 블록) 같은 부분이 < (LT: less than)으로 기술되어 있다. 트립 해제 조건이 미만인지 불분명하다. ➔ 일관성 있게 수정 필요((3)논리에서 주석과 논리를 모두 < 로 수정)
  - p.53, 7.2.4.1 가압기 고압력 - 고정형 설정치 상승 비교논리 블록의 <블록논리> (4)에서 주석문에는 공정값 <= PTSP로 되어 있고, 아래 논리 기술은 < 로 되어 있다. FBD 상에는 < (LT: less than)로 되어 있다. 불일치 ➔ 일관성 있게 수정 필요 (주석문에서 <로 수정)

속성 Label	검증속성	검증속성 의미	검증 결과	분석결과
_5_P1	if (PV_OUT_out >= _5_TSP_out && _5_TRIP_CNT_out >= _5_MAXCNT) assert _5_P1: _5_TRIP_LOGIC_out == 1	공정값이 트립설정치보다 크거나 같고 TRIP_CNT가 MAXCNT보다 같거나 커지면 즉, 지정된 시간이 지나면 트립이 발생한다.	true	
_5_P2	if(PV_OUT_out >= _5_PTSP_out && _5_PTRIP_CNT_out >= _5_MAXCNT) assert _5_P2: _5_PTRIP_LOGIC_out == 1	공정값이 예비트립설정치보다 크거나 같고 PTRIP_CNT가 MAXCNT보다 같거나 커지면 즉, 지정된 시간이 지나면 예비트립이 발생한다.	true	
_5_P3	if (_5_TRIP_LOGIC == 1 && PV_OUT_out < _5_TSP_out) assert _5_P3: _5_TRIP_LOGIC_out == 0	트립이 난 상태에서 공정값이 트립설정치 미만으로 내려가면 트립이 해제된다.	true	
_5_P4	if (_5_TRIP_LOGIC == 1 && PV_OUT_out =< _5_TSP_out) assert _5_P4: _5_TRIP_LOGIC_out == 0	트립이 난 상태에서 공정값이 트립설정치 이하로 내려가면 트립이 해제된다.	false	➢ 반례) 공정값과 트립설정치값이 같은 경우, 트립이 해제되지 않는다. ➢ 원인) p.53 7.2.4.1 가압기 고압력-고정형 설정치 상승 비교논리 블록의 <블럭논리> (3)에서 주석 및 논리에는 (공정값 <= TSP)로 기술되어 있으나, FBD 상에는(FIX_RISING 사용자 정의 블록) 같은 부분이 LT(less than, <)으로 기술되어 있다. 트립 해제 조건이 미만인지 이하인지 불분명하다. ➔ 미만으로 일관성 있게 수정 필요
_5_P5	if (_5_PTRIP_LOGIC == 1 &&	예비트립이 난 상태에서 공정값이 예비	true	

그림 16. KNICS BP 소프트웨어 SDS에 대한 정형검증 결과 예시

국외에서는 CTL과 HyTech 도구 등을 이용하여 래더로직 (Ladder Diagram; LD) 및 FBD을 모델체킹이 가능한 오토마타 모델로 변환하여 검증하는 자동화된 정형 검증 기법들을 개발하였다 [Hassapis et al., 1998]. 특히 카네기멜론대학교 연구팀은 LD를 Transition System으로 변환하여 SMV 모델체커를 활용하여 검증을 수행하였다 [Moon, 1994]. Lawford 연구팀은 Darlington 원전의 정지 계통에 대해 소프트웨어 요구 명세 및 설계 명세에 대한 4-Variable Model을 개발하였으며 PVS 모델체커를 활용하여 소프트웨어의 기능적 요구사항에 대한 정형 검증을 수행하였다 [Lawford et al., 2012].

위의 예시에서 볼 수 있듯이, 소프트웨어 정형 검증을 수행할 시, 소프트웨어 구현 단계 이후 나온 코드를 바탕으로 요구 명세 및 설계 명세에서 정의된 요구사항들을 수학적으로 만족하는지 증명할 수 있으며 PLC 기반 보호계통 소프트웨어에 특화된 다양한 툴들이 개발되어 적용하기 쉽다는 장점이 있다. 정형 검증 방법론이 소프트웨어 개발 과정에서의 안전성과 신뢰성을 높이는 데 중요한 역할을 하지만 소프트웨어의 운전 중 신뢰성은 소프트웨어의 입력 및 동작 환경에 따라 결정되는 점을 고려하여 비정상적인 입력 및 환경 변수 하에 소프트웨어의 정량적인 신뢰도를 평가할 수 없으며, 더 나아가 확률론적 안전성 평가의 관점에서 소프트웨어 실패가 원전의 신뢰성에 미치는 영향을 정량적으로 평가할 수 없어 원전 내 소프트웨어 적용에 대한 규제의 한계점이 존재한다.

제2절 정량적 소프트웨어 신뢰도 평가 방법론

현재까지 원전 디지털 I&C 계통에 사용되는 소프트웨어의 정량적 신뢰도 평가 방법론의 경우, 원전 소프트웨어의 고장률 및 요구 시 실패확률 (Probability of Failure on Demand; PFD)에 대한 정량적 평가가 가능한 다양한 방법론들이 개발 및 제안된 바 있으며, 대표적인 방법론들로는 소프트웨어 신뢰성 성장 모델, 베이지안 네트워크, 척도 기반 기법, 컨텍스트 기반 소프트웨어 리스크 평가 방법, 시험 기반 기법들을 포함한다.

1. 소프트웨어 신뢰도 성장 모형

소프트웨어 신뢰도 성장 모형 (Software Reliability Growth Model; SRGM)은 소프트웨어 개발 단계에서 소프트웨어의 잠재된 결함의 수가 줄어드는 것을 모델링하는 방법이다. 따라서 각 모델마다 적용된 가정 및 필요한 데이터가 주어져야 하며, 가용한 데이터를 사용할 수 있는 적절한 모델을 선택하여 소프트웨어 신뢰도 평가에 적용한다 [Stringfellow et al., 2002]. 예를 들어, 원자로 정지를 위한 안전 필수 소프트웨어의 경우 PFD에 관한 데이터를 수집하기에 적절하므로 이러한 데이터를 활용할 수 있는 모델을 선택해야 한다. 대표적인 SRGM 모델로는 Duane Model, Musa Model, Littlewood Model, Musa-Okumoto Model 등이 존재한다 [Lawrence, 1993].

SRGM은 소프트웨어 신뢰도를 평가하기 위한 기법 중 매우 성숙된 것으로 원전 분야뿐만 아니라 산업 분야 등에 폭넓게 연구되어 왔지만 원전의 안전 필수 소프트웨어에 적용하기에는 평가 결과에 대한 불확실성과 안전소프트웨어 실패 데이터의 부족 등의 현실적인 한계로 인해 현재까지는 규제요건으로 활용되지 않고 있다. 특히 원전 소프트웨어에 SRGM 방법론을 적용한 기존 국내 연구 [Kim et al., 2007, Park et al., 2004]에 따르면 매우 엄격한 소프트웨어 생명 주기를 따르는 원전 안전 소프트웨어는 실패 데이터가 매우 드문 이유로 SRGM 방법론을 활용하여 분석된 신뢰도 결과의 불확실성이 매우 높다고 평가한 바 있다. 또한, 평가된 결함 개수는 해당 고장수명 데이터에 매우 민감하므로 매우 낮은 실패 확률을 가지는 원전 안전 소프트웨어의 신뢰도를 평가하기에는 한계점이 있다고 분석한 바 있다. 안전 소프트웨어의 개발 과정 특징 상 소프트웨어 고장의 수가 매우 적어 소프트웨어의 신뢰도를 평가하기 위한 고장 데이터를 얻기 위해서는 많은 수의 테스트나 운영 경험 자료가 필요하다. 예를 들어, 10^{-9} 수준의 신뢰도를 얻기 위해서는 대략 10억 시간 가량의 소프트웨어 운전이력이 필요하며 그 시간 동안 안전 기능에 위해가 되는 소프트웨어의 고장이 없이 운영되어야 한다. IEEE Std. 1633에서는 SRGM 기법을 통해 추정할 수 있는 적절한 소프트웨어의 고장률 수준을 10^{-3} ~ 10^{-4} 정도로 제시한 바 있다 [IEEE, 2016].

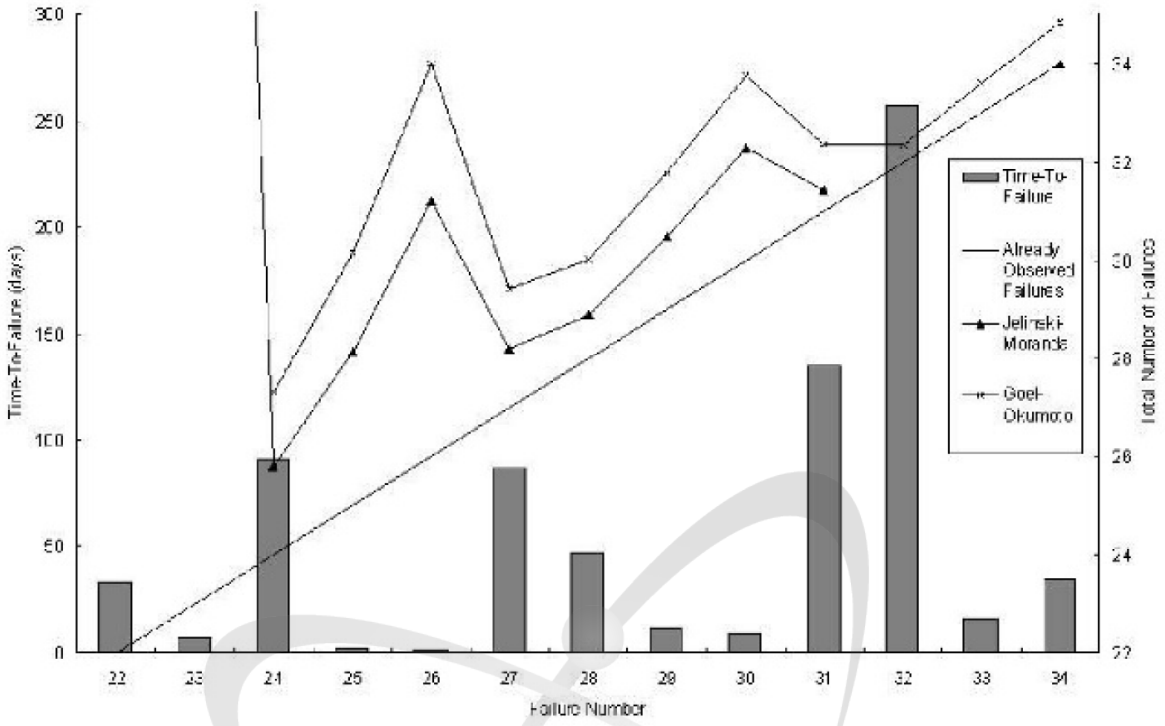


그림 17. S-curve 모형에 근거한 원전 안전소프트웨어 결함 추정 예시 [Park et al., 2014]

2. 베이지안 네트워크 모델

베이지안 네트워크 (Bayesian Belief Network; BBN) 방법론은 소프트웨어 고장 데이터와 소프트웨어 개발 수명 주기 (Software Development Lifecycle; SDLC) 활동 등의 다양한 개발 및 V&V 관련 정보들을 통합하여 신뢰도를 평가하는 방법론이다. 국내에서는 한국원자력연구소에서 BBN 방법론을 이용하여 원전 안전 소프트웨어의 결함 수 추정에 응용한 바가 있다 [Eom et al., 2009; 2013; 엄흥섭 외, 2010]. 해당 연구에서는 원전계측제어시스템개발(KNICS)사업에서 개발된 원자로 보호계통 소프트웨어에 대한 V&V 체계를 기반으로 각 소프트웨어 개발 및 V&V 과정을 개별적인 노드로 구현하여 BBN 그래프를 개발하였다. BBN 모델 평가 과정에서는 V&V 전문가의 지식을 반영하여 BBN 모델 내 각 노드의 노드 확률 테이블 (Node Probability Table; NPT)을 작성하고, 소프트웨어 결함 수 및 신뢰도를 정량적으로 평가하였다. 국외에서도 BBN 모델을 활용하여 원전 안전소프트웨어의 신뢰도를 평가한 바 있다 [Fenton et al., 2008; Chu et al., 2018].

앞선 선행 연구들에서 볼 수 있듯이, BBN 방법론은 모델 입력으로 사용되는 V&V 결과물은 규제지침으로 제출되어야 하므로 BBN 모델에 필요한 자료의 확보가 용이한 장점이 있다. 하지만 BBN 방법론은 BBN 모델 내 노드 간의 의존성에 대한 표현과 전문가 의견에 의해 생성된 NPT을 이용하여 소프트웨어 신뢰도를 추정함에서 오는 높은 불확실성에 그 한계점이 있

다. 특히 BBN 노드들의 개발과 각 노드간의 NPT 정량화 과정은 분석가의 주관적 판단과 지식에 기초하여 이루어지는데, 다수의 전문가 의견을 통합적으로 반영하여 그 오류를 줄일 수는 있지만 그 완결성을 입증하는 것은 어렵다. 또한, 정보가 불충분한 경우 전문가마다 정량화 과정에서의 결과가 다를 수 있어 BBN 모델을 이용한 소프트웨어 신뢰도 추정치 및 결과 값에 불확실성이 커질 수 있다. 이에 따라, BBN 방법론을 활용하기 위해서는 BBN 모델 및 변수들의 정량화에 많은 자료와 개발 노력이 필요할 것으로 평가되며, BBN 개발 전문가의 확보 가능성 및 전문가의 자질 검증 등의 관련 문제들이 해결되어야 한다.

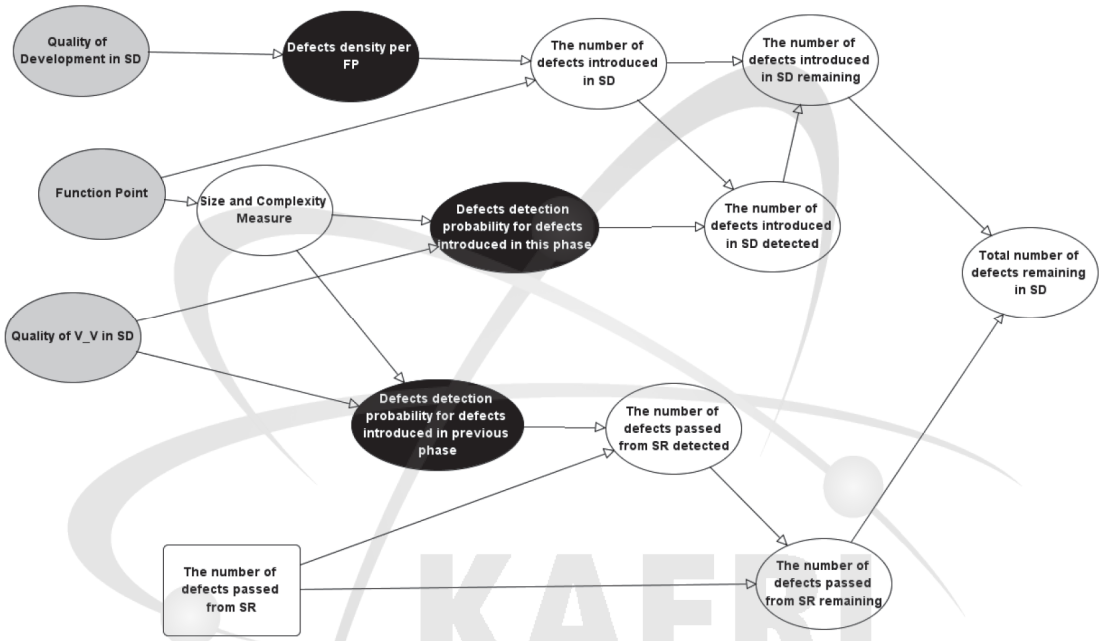


그림 18. 안전소프트웨어 결함 추정을 위한 BBN 모델 개발 예시 [Chu et al., 2018]

3. 척도 기반 기법

척도 기반 기법 (Metric-based Method)은 소프트웨어 신뢰성 및 질 (Quality)과 관련된 척도들을 선정하고 정성적으로 평가하여 결함 밀도 (Defect Density)나 평균 무고장 시간 (Mean Time to Failure; MTTF)와 같은 정량적인 신뢰도 도출에 활용하는 방법이다. 미국 Ohio State University (OSU) 연구진은 원전 디지털 계측제어 계통에 사용되는 안전 필수 소프트웨어의 신뢰도를 평가하기 위해 척도-기반 소프트웨어 신뢰도 평가 방법인 RePS (Reliability Prediction Systems)를 제안하고 소프트웨어 신뢰도 관련 30가지의 소프트웨어 공학 척도들을 선정하여 이들에 대한 우선순위를 평가한 바 있다 [Smidts et al., 2000; Li et al., 2003]. 도출된 소프트웨어 공학 척도들의 검증을 위하여, 이들 중 6개의 척도를 이용하여 실제 디지털 시스템인 PACS (Personnel Entry/Exit Access System)에 적용한 바 있

다 [Smidts et al., 2004]. 해당 적용 사례는 RePS의 여러 분석 방법 중 상태천이도를 모형화하고 천이확률들을 분석하는 방식으로 수행되었다. 이를 위해, 소프트웨어 개발 문서들을 기반으로 소프트웨어 동작에 대한 상태천이도를 개발한 뒤 운전이력을 기반으로 상태천이 확률을 결정한다. 이후, Wiegers, Pressman, Ebenau and Strauss 점검표 등을 활용하여 요구사항명세서, 설계기술서, 코드설명서 등과 같은 소프트웨어 개발 문서들에 대한 점검을 수행하며 소프트웨어 점검을 통하여 발견된 소프트웨어 결함을 상태천이도에 반영함으로써 발견된 결함이 일으킬 수 있는 소프트웨어 고장 확률을 정량적으로 평가한다.

국내에서는 한국원자력연구원이 오하이오주립대학교와의 국제공동연구로서 현금자동지급기 소프트웨어 (TELLERFAST)에 해당 방법론을 적용하고 안전 필수 소프트웨어에 대한 적용가능성을 평가한 바 있다 [김만철 외, 2008]. 해당 연구에서는 Wiegers 점검표를 활용해 TELLERFAST 코드 점검을 수행한 결과, 오타와 같은 단순 오류를 제외한 39개의 결함을 발견하였으며 해당 점검결과를 상태천이도에 반영하여 소프트웨어 오류 발생확률을 평가하였다. 하지만 척도 기반 방법의 경우, 상태천이도를 활용하여 이미 발견된 소프트웨어 결함에 따른 오류확률을 평가하여 이후 소프트웨어 디버깅을 통해서 발견된 결함을 제거할 경우에는 도출된 소프트웨어 신뢰도가 큰 의미를 가지지 못할 것으로 예상된다. 또한 천이확률을 나타내는 운전이력이 척도 기반 방법론의 핵심적인 부분이라고 할 수 있는데 평가된 신뢰도 값에 불확실성을 제거하기 위해 원전 안전 소프트웨어의 운전이력을 정확하게 측정하는 것에 많은 노력이 필요할 것으로 예상된다.

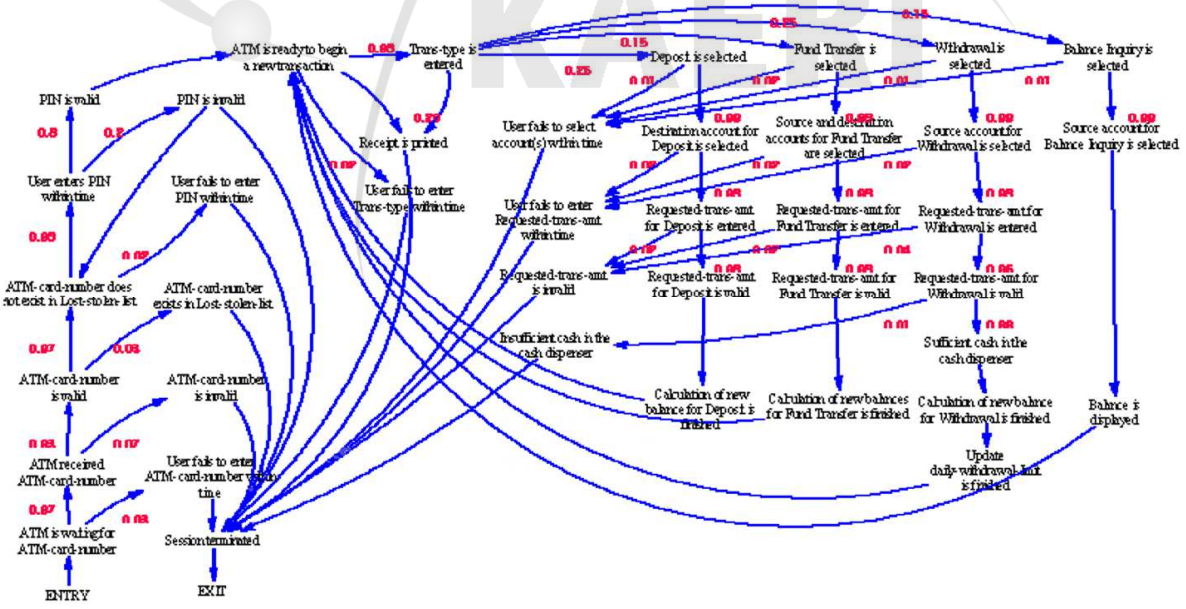


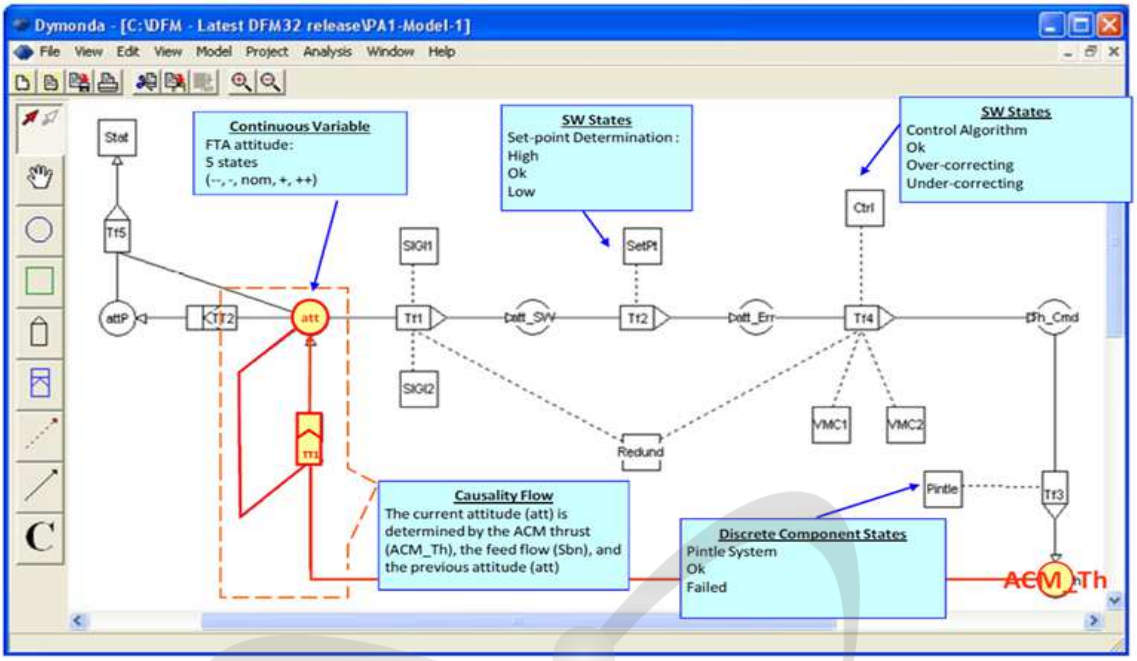
그림 19. TELLERFAST 소프트웨어의 상태천이도 및 천이확률 평가 예시 [김만철 외, 2008]

4. 컨텍스트 기반 소프트웨어 리스크 평가 방법

컨텍스트 기반 소프트웨어 리스크 평가 방법 (Context-based Software Risk Assessment Method; CSRM) 의 대표적인 기법인 동적 흐름도 기법 (Dynamic Flowgraph Method; DFM)은 소프트웨어가 내재된 시스템 신뢰도 분석에 활용되는 기법이다 [Garrett et al., 1999]. 디지털 계측제어 계통은 향상된 성능과 고장 검출 기능 등을 제공하지만 내재된 소프트웨어로 인한 새로운 고장모드가 발생할 가능성이 있다. DFM은 이러한 디지털 시스템의 특성을 반영하기 위해 소프트웨어, 하드웨어 및 운전환경을 통합하여 하나의 모형으로 구현하여 분석하는 digraph-기반 기법이며 시간-전이망, 인과망, 조건화망 등 시스템의 논리적, 물리적, 시간적 속성을 표현하는 모형을 활용한다. DFM 모델 내 각 노드의 관계는 전환 상자 (Transition Box)에 의해 설명되는데 각각의 전환 상자에는 의사결정 표 (Decision Table)가 연결되며 입력 및 출력 프로세스 변수 노드간의 관계를 정량화하는데 사용된다. 사용되는 의사결정 표는 시스템을 구성하는 하드웨어, 소프트웨어, 운전환경에 대한 경험적 지식에 의해 구축되며, 여기에는 시스템의 상태를 결정하는 물리적 수식이나 소프트웨어 코드나 규격 등이 포함된다.

DFM 분석은 일반적으로 영향에서 원인으로 향하는 모형을 기반으로 기본 컴포넌트 상태의 조합 및 순서를 식별하여 시스템 상태를 연역적, 귀납적 알고리즘으로 평가한다. 즉, 관심이 있는 시스템의 상태에 이르는 하드웨어 및 소프트웨어 조건들의 조합 경로 및 순서를 식별하여 소프트웨어를 포함한 시스템의 실패 확률을 평가한다. 또한, DFM은 시스템의 상태를 위험도에 따라 여러 수준으로 분류할 수 있으며, 상태 간 전이를 통하여 시스템의 동적인 특성을 나타낼 수 있다.

미국 National Aeronautics and Space Administration (NASA)은 DFM 기법을 활용하여 PA-1 고도 제어 시스템의 소프트웨어 신뢰도 분석을 수행한 바 있다 [Stamatelatos et al., 2011]. 해당 연구에서는 소프트웨어 로직 및 메모리, 중앙처리장치와 같은 하드웨어 기기들을 포함한 소프트웨어 기반 시스템에 대한 DFM 모형을 개발하여 소프트웨어 신뢰도를 평가할 수 있는 체계를 제안하였다. 해당 분석에서는 소프트웨어 실패로만 발생되는 시스템 실패, 소프트웨어 및 하드웨어 실패의 조합으로 발생되는 시스템 실패, 하드웨어 실패로만 발생되는 시스템 실패로 구분하여 신뢰도를 평가하였으며, 각 노드 간 의사결정 표에 정의된 전이 확률에 대한 불확실성을 고려하여 소프트웨어 신뢰도를 평가하였다. 특히, 하드웨어 실패가 발생된 후 소프트웨어 실패로 인해 발생하는 조건부 실패 확률을 추가적으로 분석하여 소프트웨어의 운전 환경을 반영하여 신뢰도를 평가하다는 점에 의의가 있다.



#	Prime Implicant	Probability
1	Pintle system failure	xxx
2	GN&C set-point high AND Control algorithm normal	xxx
3	GN&C set-point low AND Control algorithm normal	xxx
4	SIGI1 biased high	xxx
5	SIGI1 biased low	xxx
6	GN&C set-point high AND Control algorithm over-correcting	xxx
7	GN&C set-point low AND Control algorithm over-correcting	xxx

SW function cut-sets

HW cut-sets

그림 20. PA-1 GN&C 시스템에 대한 DFM 모형 및 결과 예시 [Stamatelatos et al., 2011]

미국 Ohio State University는 DFM 기법을 소프트웨어를 포함한 디지털 I&C 시스템이 적용된 가스 저장 시스템과 압력 제어시스템의 실패확률을 평가하는데 활용한 바 있다 [Aldemir et al., 2009]. 시스템의 실패 상태로 가스 압력을 적절히 제어하지 못하는 상태로 정의하였고, 시스템의 실패를 야기하는 소프트웨어와 하드웨어의 실패 조합을 도출하고 기존 원전의 확률론적 안전성 평가 모델에 해당 결과를 통합할 수 있는 체계를 제안하였다. 원전 안전 소프트웨어에 대한 DFM 기법의 적용가능성에 대해서는, 노드 간 의사결정 표에 정의된 전이확률이 전문가 의견에 의해 결정되므로 DFM 기법으로 평가된 소프트웨어 실패 확률에 대한 불확실성을 최소화할 수 있는 방안이 필요할 것으로 예상된다.

5. 시험 기반 기법

시험 기반 기법 (Test-based Method)은 원전 안전 필수 소프트웨어에 대한 시험 결과를 바탕으로 통계적 방법에 근거해 소프트웨어 신뢰도를 평가하는 방법이다. 여기서 시험 결과는 소프트웨어의 실제 운전 이력 데이터를 바탕으로 하드웨어 기반 시험 환경 또는 시뮬레이션 시험 환경에서 소프트웨어를 시험하여 생성된 결과를 의미한다. 소프트웨어 시험 기반 방법론은 블랙박스 시험 (Black-box Testing) 과 화이트박스 시험 (White-box Testing) 방법론으로 나뉜다.

소프트웨어 블랙박스 시험은 시험의 대상이 되는 소프트웨어를 내부 구조나 작동 원리를 모르는 블랙박스로 취급하며 특정 소프트웨어 시험 케이스에 대한 소프트웨어의 시험 결과를 바탕으로 소프트웨어의 신뢰도를 입증하는 방법론이다 [Chu et al., 2013]. 해당 방법론에서 소프트웨어 시험 입력은 소프트웨어의 실제 운전 이력 (Operational Profile)을 바탕으로 개발된다. 블랙박스 시험 방법론에서는 매우 높은 소프트웨어 신뢰도를 입증할 수 있는 시험 케이스 (95% 신뢰도에서 10^{-5}의 소프트웨어 신뢰도를 입증하기 위해서는 $3*10^{5}$개의 시험 케이스가 필요함)의 개수를 도출한다. 개발된 시험 입력들은 소프트웨어가 설치되어 있는 하드웨어 기반 시험 환경에서 검사되어 주어진 소프트웨어 입력에 대해 소프트웨어가 올바른 출력을 생성하는지 확인하고 이러한 시험 결과를 바탕으로 소프트웨어 신뢰도를 정량화한다. 블랙박스 시험 방법론은 시험 대상이 되는 소프트웨어의 자세한 개발 정보가 필요하지 않다는 장점이 있지만, 시험 대상이 되는 소프트웨어의 코드 및 내부 구조에 대한 정보 없이 시험이 수행되므로 개발된 시험 입력이 소프트웨어 운전 이력을 잘 반영하는지에 대한 검증이 어렵다는 한계점을 가지고 있다.

국내에서 이루어진 시험 기반 소프트웨어 신뢰도 평가는 2005년 울진 3/4호기 발전소제어계통 (Plant Control System) 소프트웨어에 대해 수행된 바 있다 [김효정 외, 2005]. 해당 시험은 2차에 걸쳐 실시되었다. 1차 시험은 현장상황 하에서 실제 제작사의 시험모듈을 이용하여 하드웨어적으로 검증받을 수 있는 40년간의 운전이력에 대해서 시험을 실시되었으며, 2차 시험은 별도의 시험모듈을 이용하여 연구실 환경에서 더 오랜 기간의 소프트웨어의 신뢰도를 검증하고자 3000-10000년간의 운전이력에 대해 시험이 실시되어 운전이력 시험에서 소프트웨어가 정상적으로 동작하는 것을 확인하였다. 또한, 2008년 월성 2, 3, 4호기의 디지털 제어용 전산기 (Digital Computer Controller)에 대하여 수행된 바 있으나, 시간이력을 고려한 입력 시험 (Trajectory Input Testing)을 이용하였기 때문에 시험에 매우 장시간이 소요된 바 있다. 두 연구는 소프트웨어 운전이력을 활용하여 소프트웨어를 시험하여 신뢰도를 평가하였다는 점에서 의의가 있으나, 원전 안전 등급 소프트웨어의 고신뢰성을 입증할 수 있는 시험 수에 미치지 못하는 결과가 도출되었다. 국외에서는 미국 Idaho National Laboratory (INL)이 Advanced test reactor (ATR) Loop Operating Control System (LOCS)의 소프트웨어

신뢰도 평가에 열수력 분석 코드와 연동한 Control Software Failure Test Signal Simulator (CSFT-SS)라는 소프트웨어 시험 환경을 개발하였으며 10,000개의 서로 다른 시험 입력을 이용해 소프트웨어 시험을 수행한 바 있다 [Chu et al., 2016; 2017].

이러한 선행 연구들의 예시에서 볼 수 있듯이 원전 소프트웨어 신뢰도 평가에 활용된 소프트웨어 블랙박스 시험 방법론의 단점으로는 시험 대상이 되는 소프트웨어가 설치된 하드웨어 기반 환경에서 입출력을 확인하기 때문에 시험 입력 당 시험 시간이 길며, 시험 입력이 소프트웨어 입력 공간에서 추출되므로 해당 입력들로 소프트웨어 기능에 대한 완결성을 증명하기 어렵다는 한계점을 가지고 있다.

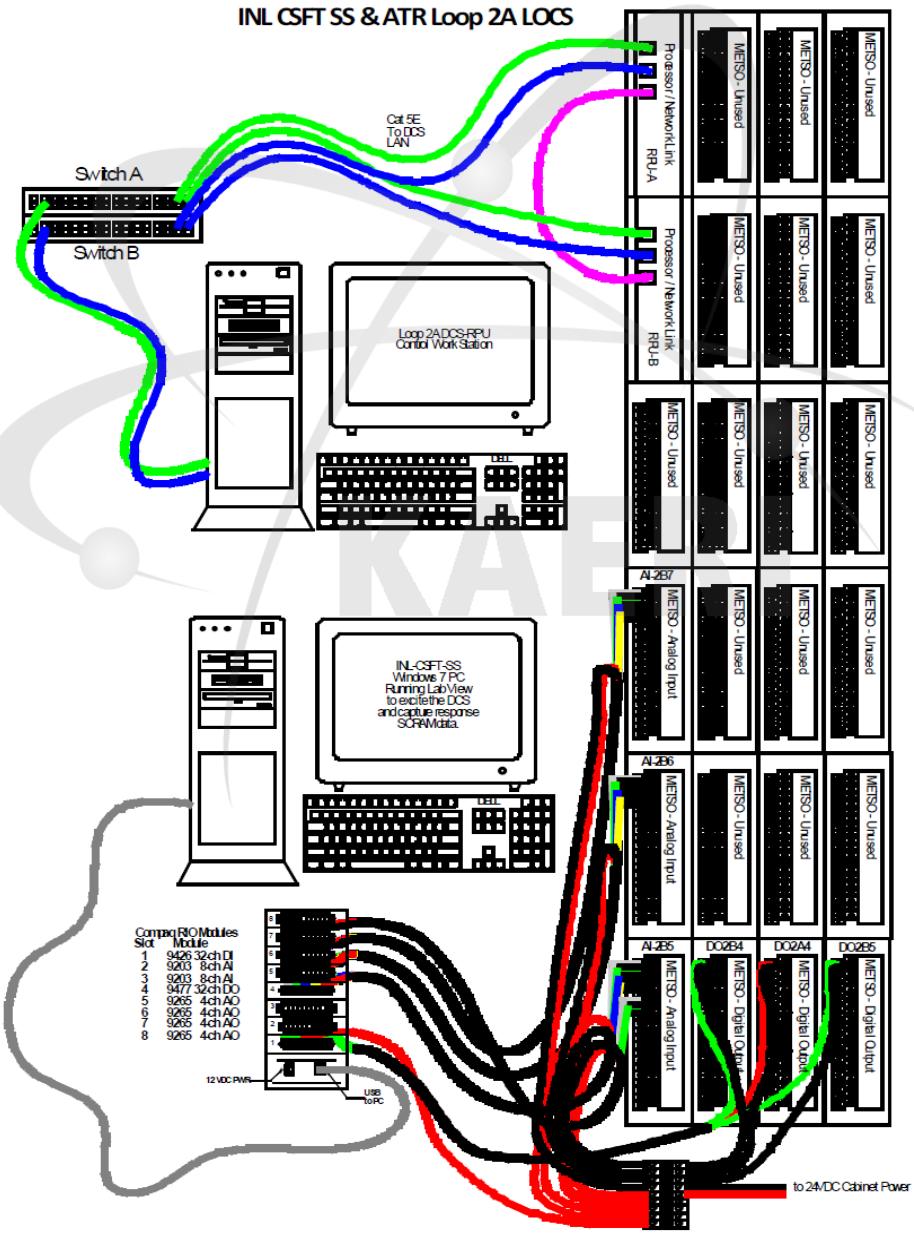


그림 21. LOCS 소프트웨어 시험용 CSFT-SS 시험환경 [Chu et al., 2017]

소프트웨어 화이트박스 시험 기법은 소프트웨어의 내부 구조를 고려함으로서 소프트웨어 코드가 어떤 경로로 실행되며 소프트웨어 동작의 유효성을 살펴볼 수 있을 뿐만 아니라 불필요한 코드 혹은 테스트되지 못한 코드 부분이 있는지 확인할 수 있어 소프트웨어 시험 입력에 대한 커버리지 (Coverage) 분석도 가능하다는 장점이 있다.

국내에서는 KNICS 원자로 보호 계통 비교논리프로세서 (Bistable Processor)의 트립 로직에 대한 부분적인 전수 조사 시험 입력을 개발한 바 있다 [Kang et al., 2009; Shin et al., 2017; Cho et al., 2019]. 여기서 부분적인 전수 조사 시험 입력이란 트립 로직을 결정하는 안전소프트웨어의 모든 입력 및 내부 변수를 고려하여 전수 조사 시험 입력을 개발하지 않고, 트립 결정에 기여하는 몇 가지 중요 변수들에 대해서 우선적으로 시험 입력을 개발했음을 의미한다. 한국원자력연구원은 고장주입 시뮬레이터를 활용하여 KNICS 원자로 보호 계통 가압기 저압력 트립 로직에 대해 도출된 512,820개의 부분 전수시험 입력을 생성하고 시험한 바 있다 [Shin et al., 2017]. 한국수력원자력 중앙연구원은 APR-1400 노형인 신한울 1, 2호기 발전소보호계통 비교논리프로세서 내 총 20개 및 동시논리프로세서 내 총 35개의 트립 및 공학적 안전설비 개시 논리에 대해 트립 및 공학적 안전설비 개시 발생에 관련된 소프트웨어 변수들의 전수 시험 입력을 개발하고 전수 시험을 수행하기 위한 안전소프트웨어 시뮬레이션 환경을 구축하고 시험을 수행한 바 있다 [오해철 외, 2019; Lee et al., 2020].

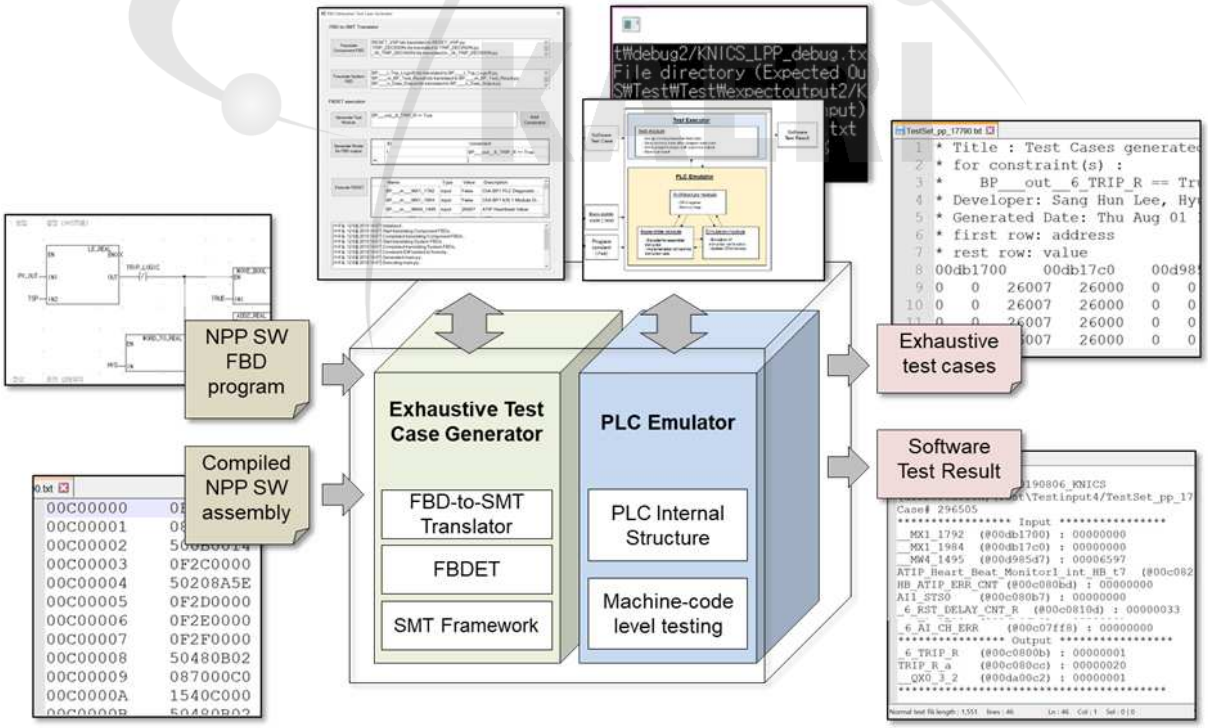


그림 22. 신한울1&2 RPS 소프트웨어 전수시험용 시뮬레이션 기반 시험 환경 [Lee et al., 2020]

국외에서는 베이지안 방법에 기반하여 소프트웨어 시험 입력들을 분류하고 화이트박스 시험 기법으로 소프트웨어를 시험함으로서 소프트웨어 실패 확률을 평가하는 방법론을 처음으로 제시한 바 있으며 [Miller et al., 1992], 이후 State-based Model, Path-based Model, Additive Approach 등의 다양한 화이트박스 시험 기반 방법론들이 제안된 바 있다 [Goševa-Popstojanova et al., 2001].

선행 연구들의 예시에서 볼 수 있듯이 원전 소프트웨어 신뢰도 평가에 적용된 화이트박스 시험 방법론의 단점으로는 소프트웨어의 원시 코드 혹은 유사한 수준의 설계 정보를 활용하여 시험 입력이 개발되기 때문에, 블랙박스 시험보다 많은 수의 케이스를 시험하게 되므로 실제 구동환경과 유사하면서도 소프트웨어 시험을 빠른 시간 안에 수행할 수 있는 시험환경의 구축 및 시험수행이 필요하다.

KAERI

제3절 소프트웨어 신뢰도 평가 방법론 비교 분석

본 연구에서는 현재 규제요건에 대한 적용가능성을 포함한 9가지 평가 기준을 바탕으로 각 소프트웨어 신뢰도 평가 방법론의 특성을 비교 분석하였다. 각 방법론이 각 평가 기준에 부합하는지에 따라 전문가 판단에 의해 정성적으로 평가되었으며, 평가 결과는 아래 기준에 따라 총점으로 환산되었다.

표 1. 정성적/정량적 소프트웨어 신뢰도 평가 방법론 비교 분석

평가 기준 / 방법론	1	2	3	4	5	6	7	8	9	총점
SW HAZOP	△	X	X	△	X	△	X	△	△	5
SW FMEA	△	X	X	△	X	△	X	△	△	5
SW FTA	△	X	X	X	X	△	X	△	△	4
Formal Method	○	△	△	X	X	○	X	○	○	10
SRGM	△	X	X	X	△	X	X	△	X	3
BBN	○	X	○	△	△	○	△	○	△	12
Metric-based Method	△	△	X	X	X	X	X	△	X	3
CSRM	△	○	X	△	X	△	X	△	△	7
Test-based Method	○	○	X	○	△	○	○	○	○	15

- 평가 점수 : 예 (○, 2점), 아마도 (△, 1점), 아니오 (X, 0점)
- 평가 기준
  - 방법론에 사용되는 가정은 합리적인 근거를 기반으로 함.
  - 방법론은 소프트웨어의 특정 동작 환경을 고려함.
  - 방법론은 소프트웨어 생명주기 공정의 품질을 고려함.
  - 방법론은 소프트웨어 운전 이력을 고려함.
  - 방법론은 불확실성을 고려함.
  - 방법론은 기존 적용사례를 통해 검증됨.
  - 방법론은 고신뢰도 소프트웨어(10-4~10-5)의 신뢰성 평가에 활용 가능함.
  - 방법론에 필요한 데이터 및 정보가 존재하며 수집 가능함.
  - 방법론은 기존 규제 요건에 부합함.

제4장

소프트웨어 신뢰도 규제기준 및 사례 분석

제1절 국내 규제기준 및 사례

제2절 국외 규제기준 및 사례

KAERI

KAERI

제4장 소프트웨어 신뢰도 규제기준 및 사례 분석

제1절 국내 규제기준 및 사례

1. 한국 KINS

가. 규제기준

원자력발전소의 건설 및 운영에 대한 인허가 단계에서 건설 및 운영허가 신청자(이하 허가신청자)는 원자력발전소가 종사자 및 일반 공중의 보건과 안전 및 환경에 대한 위험을 초래하지 않고 건설·운영될 수 있음을 입증하여야 한다. 이를 위해 허가신청자는 원자력발전소를 상세하게 설계 및 분석하고 원자력안전법 제10조 및 제20조, 그리고 동법 시행령 제7조, 시행규칙 제4조 및 제16조의 규정에 따라 각각 예비(최종)안전성분석보고서에 수록될 사항을 모두 포함하여 제출하여야 한다. 검토자는 허가신청자가 작성·제출한 안전성분석보고서에 기술된 내용이 원자력안전법 제11조 및 제21조의 허가기준을 충족하는지 여부를 평가하여 원자력발전소의 안전성을 심사한다. 허가신청자가 제출한 안전성분석보고서를 검토함에 있어 검토자는 원전 안전심사지침 외에 한국원자력안전기술원의 규제기준과 규제지침을 동시에 참고하여야 하며, 규제기준과 규제지침은 안전심사지침보다 우선하는 지위를 갖는다. 따라서 규제기준과 규제지침이 안전심사지침과 상충되는 경우에는 규제기준과 규제지침을 우선하여 적용하되, 규제기준과 규제지침의 기술적 근거가 불명확한 경우에는 안전심사지침을 적용할 수 있다.

본 연구에서는 디지털 안전계통 개발을 위해 필요한 규제법규, 규제지침, 기술기준, 참고문서 등을 소프트웨어 측면에서 분석하여 체계적으로 정리하였다. 규제요건의 최상위 요건인 규제 법규인 원자력법, 원자력법 시행령, 과기부령(규칙)과 과기부고시(기준), 디지털 계측제어계통에 대한 안전규제 일반 원칙 및 규제지침(안), KEPIC, 그리고 한국원자력안전기술원이 발간한 각종 보고서를 분석 범위로 설정하였다. 디지털 I&C 계통 및 소프트웨어와 관련된 KINS 규제기준으로는 KINS/RS-N08.00, KINS/RG-N08.01, KINS/RG-N08.15 ~ 08.20, 08.27 등이 있다. 계측제어 안전등급 분류는 디지털 계측제어계통 설계 및 인허가를 위해 필수적으로 수행되어야 한다. 안전등급 분류기준과 체계에 대한 자료를 수집하여 디지털 계측제어계통에 적용할 수 있는 안전등급 분류기준과 요건을 설정 또는 선정하고, 소프트웨어 안전등급 분류기준과 체계도 분석범위에 포함하였다.

KINS/RG-N08.01에서는 다양한 I&C 계통 소프트웨어의 신뢰도 및 품질보증에 관한 규제기준을 기술하는데, 여기에서는 원자력발전소의 계측제어계통은 안전성 계측제어계통과 비안전성 계측제어 계통으로 분류하며, 안전성 계측제어계통은 다시 안전관련 계측제어계통과 비안

전관련 계측제어계통으로 분류한다. 안전관련 계측제어계통의 안전등급을 3등급으로 나누어 안전등급 IC-1, 안전등급 IC-2, 안전등급 IC-3으로 분류한다.

표 2. 원전 계측제어계통 안전 등급 분류

안전등급	설명	예시 계통	소프트웨어 관련 지침
계측제어등급 1 (IC1)	DBA시 안전 기능을 수행하는 계측제어계통 원자력안전위원회 고시 제 2017-21호 제7조 (안전 등급3)에 의해 안전 등급3 으로 분류되며 DBA 발생시 안전 기능을 수행하는 계측제어설비	RPS, ESF-CCS, 등	규제지침 3.2, 3.3, 3.9, 8.2 ~ 8.10, 8.12 ~ 8.20 등의 요건 및 지침 만족 IEEE Std. 1012의 SIL-4와 동등한 수준의 소프트웨어 등급 (Safety Critical)의 V&V 활동 요구 소프트웨어 안전성 분석 요구 독립된 V&V 활동 요구
계측제어등급 2 (IC2)	IC1에 포함되지 않는 계측제어설비로서, 특정 사건 발생 시 별도의 보호 및 제어 기능 수행	DPS, 등	수행하는 기능의 중요도에 상응하는 S/W 품질보증요건 및 기술기준에 따라 개발 IC1의 기능 수행에 영향을 미치는 위험요소 내재시 안전성 분석 수행 적절히 독립된 V&V
계측제어등급 3 (IC3)	IC1 및 IC2에 포함되지 않는 계측제어설비로서, 발전소 과도 상태를 포함한 정상 운전에 필요한 계통	ITP, MTP, 등	발전소 운전에 적합한 신뢰성 있는 수준의 소프트웨어 품질보증요건 및 기술기준에 따라 개발

원전 소프트웨어의 경우, 계측제어계통의 일부 구성 요소로써 안전성 계측제어계통에 사용된 소프트웨어 안전등급은 수행되어야 할 기능의 안전 중요도에 따라 다음과 같은 3개 등급, 즉 안전-필수 소프트웨어, 안전-관련 소프트웨어 그리고 비안전 소프트웨어로 분류된다.

- **안전-필수 소프트웨어 (Safety-Critical Software)** : 안전-필수 소프트웨어는 안전등급 IC-1 계측제어계통에 사용된 소프트웨어로서 가장 엄격한 소프트웨어 품질보증요건과 기술기준을 적용하며, 심층방어 및 다양성 분석결과에 따라 필요하다면 다양성 백업설비가 요구될 수 있다. 원자로 보호계통 소프트웨어 개발에 따른 안전성 분석에서는 소프트웨어 구성요소가 원자로 보호계통에 미치는 위험요소 또는 위험도 분석들을 수행하여 공통유형고장 발생 가능성을 최소화하여야 한다. 소프트웨어 확인 및 검증 활동들은 개발조직과는 기술, 조직, 책임, 권한 및 재정적으로 독립된 확인 및 검증조직에 의해 수행되어야 한다.

- **안전-관련 소프트웨어 (Safety-Related Software)** : 안전-관련 소프트웨어는 안전등급 IC-2와 IC-3 계측제어계통에 사용되는 소프트웨어로서 안전-필수 소프트웨어

보다도 완화된 품질보증요건과 기술기준을 적용 받게 된다. 안전-관련 소프트웨어에 대한 안전성 분석은 요구되지 않지만, 그 소프트웨어가 안전-필수 소프트웨어에 영향을 미칠 수 있는 위험요소가 있다면 찾아서 시정하여야 하며, 확인 및 검증 활동들은 설계팀과는 적절하게 독립된 확인 및 검증조직에 의해 수행되어야 한다.

- **비안전 소프트웨어(Non-Safety Software)** : 비안전 소프트웨어는 비안전등급 계측제어계통에 사용된 소프트웨어이며, 발전소 안전운전에 적합한 수준의 품질보증요건과 기술기준에 맞게 개발되어야 한다. 만약 비안전 소프트웨어가 안전-필수 또는 안전-관련 소프트웨어와 함께 동일한 컴퓨터에 탑재(loading)되어 실행된다면, 그 소프트웨어가 다른 상위의 소프트웨어에 미칠 수 있는 위험요소를 분석하고 필요하다면 적절한 보완(예, 격리)을 하여야 한다.

이 중, 안전등급 (안전-필수 및 안전-관련) 소프트웨어는 그림 23과 같이 IEEE 603, IEEE 7-4.3.2, NUREG-0800, BTP 7-14 등 관련 U.S. NRC Reg. Guide 및 각종 IEEE Std 및 IEC 등 기술기준 및 표준과 경수로형 원전 안전심사지침(KINS/G-001) 7장 부록 13 [이종민 외, 2014]에 따라 체계적인 소프트웨어 개발 계획과 개발 공정에 따라 개발하고 검증한다. 소프트웨어 개발 생명주기는 개념 정립에서 구현까지 하향식 접근방법을 채택한 폭포수(Waterfall) 모델, 원형 (Prototyping) 모델 및 나선형 (Spiral) 모델 등을 조합한 모델을 따르고 있다. 각 단계별 생명 주기 업무는 IEEE Std 1074에서 선별적으로 채택하여 수행한다. 안전등급 소프트웨어의 생명주기는 NUREG-0800 제7장에 따라, 그림 24와 같이 계획, 요구사항, 설계, 구현, 통합, 검증, 설치, 운영 및 유지보수 단계로 나뉜다. 각 생명주기 단계별 수행업무는 크게 두 가지 업무로 나누어지며, 하나는 설계, 개발 및 구현 등 설계 및 개발업무이며, 다른 하나는 설계 및 개발업무의 확인 및 검증업무로 나누어진다. KINS/RS-N08.00은 다양한 계측제어계통 소프트웨어의 신뢰도 및 품질보증에 관한 규제기준을 기술한다.

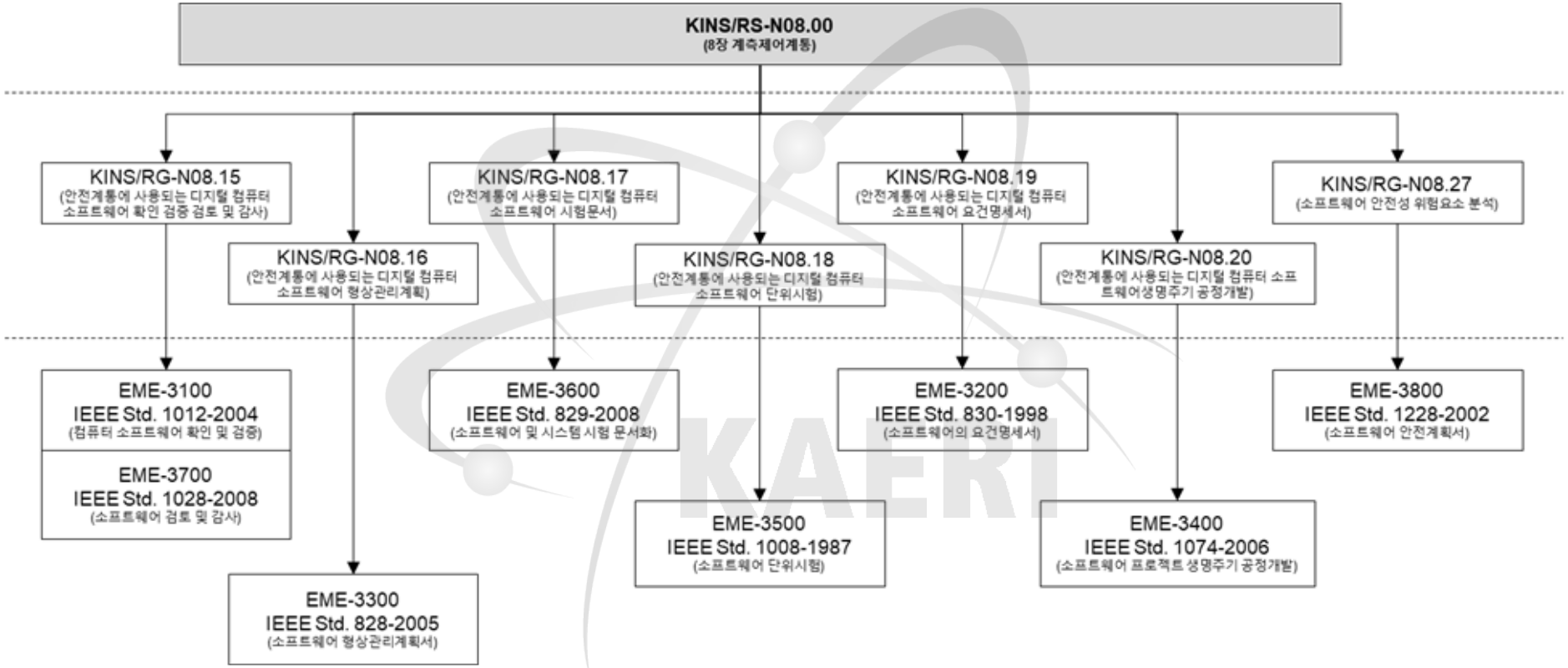


그림 23. 원전 계측제어 계통 소프트웨어 관련 KINS 규제체계

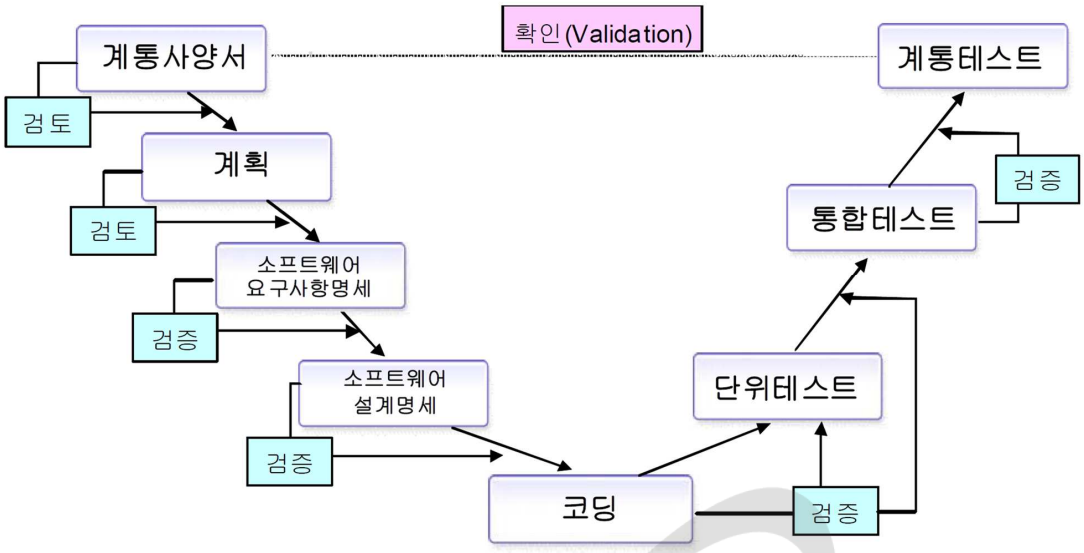


그림 24. 안전등급 소프트웨어 생명주기 및 주기별 업무

표 3. 원전 계측제어계통별 소프트웨어 관련 규제지침

계통	설명	소프트웨어 관련 지침
원자로보호계통 (RPS)	안전계통의 일부로서 안전기능을 수행하는 감지 및 명령 설비를 말하며, 원자로 정지 계통과 공학적 안전설비 작동 계통을 포함함.	**(8.2.3절 – 일반기능 및 신뢰도)** 원자로 보호계통에 대한 정량적 또는 정성적 신뢰도 목표가 달성되었음을 확증하기 위한 설계분석이 적절히 수행되어야 하며, 그 분석에는 원자로 보호계통의 하드웨어와 소프트웨어를 포함하여야 한다. **(8.2.7절 – 품질보증)** 원자로 보호계통의 소프트웨어는 의도된 보호기능을 수행할 수 있도록 엄격한 소프트웨어 개발공정과 품질보증요건에 따라 설계, 개발, 시험 및 설치되어야 한다. 소프트웨어 품질보증에 관하여는 규제지침들을 참조할 수 있다
안전관련 계측제어계통	안전정지 계측제어계통, 안전관련 정보계통(사고감시계측 포함), 안전관련 연동계통과 원자로제어실, 원격제어실(현장제어반 포함)의 안전관련 계측제어계통을 포함함.	**(8.3.7절 – 품질보증)** 안전관련 계측제어계통에 사용되는 소프트웨어는 소정의 안전관련 기능을 수행할 수 있도록 소프트웨어 개발공정에 따라 설계·개발되어야 한다.
제어계통	반응도 제어계통을 포함한 발전소 공정제어계통 등을 포함함.	**(8.5.4절 – 품질보증)** 안전계통에 영향을 미칠 수 있는 제어계통의 고장 가능성을 최소화하기 위하여 제어계통의 소프트웨어는 안전계통의 소프트웨어와 유사하게 체계적인 공정을 통하여 개발되어야 한다. 단, 제어계통 소프트웨어가 안전계통보다 비교적 낮은 중요도를 갖고 있으므로 소프트웨어 생명주기 개발 공정 중에서 각 공정별로 이루어지는 확인 및 검증 활동의 일부를 생략할 수 있다.

나. 규제사례

① 신월성 원전 1, 2호기 운영허가 심사 (2014년)

신월성 1, 2호기는 ㈜한국수력원자력 (KHNP)가 2009년 12월 운영허가 신청을 제출한 이래로 KINS가 3년 10개월간 수행한 심검사를 수행하였으며, 2014년 11월 원자력안전위원회는 제31회 원자력안전위원회에서 신월성 1, 2호기 운영허가안에 대해 심의 의결하였다. 해당 심사에서는 KINS가 수행한 신월성 1, 2호기 운영허가신청서류의 심사결과 등에 대해 검토하였고, 원자력안전법 제21조의 허가기준에 만족하는 것으로 평가하여 신월성 1, 2호기 운영 허가를 결정하였다.

해당 심사보고서 [KINS, 2014a]에서는 디지털 기반 원자로보호계통, 공학적안전설비작동계통, 노심보호연산기계통 등에 설치된 소프트웨어에 대한 심사를 수행하였는데, 해당 계통에 설치된 소프트웨어의 개념단계, 설계단계, 구현/코딩단계, 시험단계, 현장설치/점검단계, 운전 및 정비단계, 폐기단계 등의 소프트웨어 생명 주기에 따라 설치 및 개발되었음을 확인하였고, 이에 대한 적합성을 검토한 결과, 해당 소프트웨어의 적합한 품질을 보장할 수 있도록 소프트웨어의 설계 및 개발절차가 U.S. NRC RG 1.168 ~ 1.173, 경수로형 원전 안전심사지침 부록 7-13, IEEE Std. 7-4.3.2 등의 요건을 만족함을 확인하였다. 또한, 소프트웨어 프로그램 매뉴얼 (Software Program Manual; SPM)에 대한 검토를 토대로 DPPS의 소프트웨어 설계특성이 U.S. NRC 1.152를 만족함을 확인하였다. 신월성 1, 2호기 DPPS 및 DESFAS-AC 소프트웨어에 대한 독립 확인 및 검증은 소프트웨어 확인 및 검증계획서의 공정에 따라 요건단계, 설계단계, 이행 및 시험단계별로 독립적인 확인 및 검증조직에 의해 수행되어 보고서가 작성되고 있으며, 한울 5, 6호기 설계와 상이한 부분에 대해서는 코드검사, 회귀 분석을 수행하고, 특별 검토보고서를 발행하여, 해당 소프트웨어에 대한 확인 및 검증 공정이 적합함을 확인하였다.

소프트웨어 시험과 관련하여, DPPS 및 DESFAS 소프트웨어는 선행 호기인 한울 5, 6호기 DPPS/DESFAS-AC 시험과 동일한 방법으로 수행되었으며, 통합시험은 공장시험 절차서에 적절히 반영되어 있음을 확인하였다. CPCS 소프트웨어 설계에 대해서는 단계별로 요건이 추적될 수 있도록 요건 추적성 매트릭스를 적절히 작성하여 운영하고 있음을 확인하였다.

결론적으로 신월성 1, 2호기의 안전 관련 계통의 소프트웨어는 소프트웨어 생명주기 동안 관련 기술기준 요건에 따라 적합하게 설계되고 관련 품질보증 활동이 적절하게 이루어졌으므로, 소프트웨어 설계 결과는 적합한 것으로 판단되었다.

② 신고리 원전 3, 4호기 운영허가 심사 (2015년, 2019년)

신고리 3호기는 2016년 12월 제3세대 가압경수로형 원자력발전소로는 세계 최초로 상업운전을 시작했으며, 신고리 4호기도 2019년 2월에 운영허가를 취득하고 2019년 8월 29일 상업운전에 착수했다. 신고리 3, 4호기는 디지털 제어설비 전면 적용, 0.3g 내진설계 강화 및 해일 대비 방수문 설치, 중대사고 발생시 원자로건물 보호를 위한 피동수소제거설비 및 이동형 발전기 설치 등을 통해 안전성을 높인 원전으로 평가받고 있다. 신고리 3호기의 경우, KHNP가 2011년 6월 운영허가를 신청한 이후로 총 12차례의 회의를 통해 신고리 3호기 운영허가 심·검사 사항 및 KINS가 수행한 신고리 3호기 운영허가 심사보고서를 검토하였으며, 제47회 원자력안전위원회에서 신고리 3호기 운영허가를 의결하였다.

해당 심사보고서 [KINS, 2014b; KINS 2019]에서는 디지털 기반으로 설계된 원자로보호계통, 공학적안전설비작동계통, 노심보호연산기계통 등의 소프트웨어에 대한 심사를 수행하였는데, 해당 계통의 소프트웨어는 개념단계, 요건분석/정의단계, 설계단계, 구현/코딩단계, 시험단계, 현장설치/점검단계, 운전 및 정비단계, 폐기단계 등의 소프트웨어 생명주기에 따라 설계 및 개발되었음을 확인하였다. 또한, KINS는 KHNP가 제출한 원자로보호계통 및 공학적안전설비작동계통 소프트웨어에 대한 계통설계자의 평가보고서를 및 최종 소프트웨어에 대한 주요한 설계문서를 검토하였다. 그 결과, 해당 소프트웨어 설계 및 개발절차가 U.S. NRC RG 1.152, 1.168 ~ 1.173, 경수로형 원전 안전심사지침 부록 7-13, IEEE Std. 7-4.3.2, IEEE Std. 1074 등의 요건 및 기술기준을 만족함을 확인하였다. 소프트웨어 독립 확인 및 검증은 소프트웨어 확인 및 검증계획서의 공정에 따라 요건단계, 설계단계, 이행 및 시험단계별로 독립적인 확인 및 검증조직에 의해 수행되어 보고서가 작성되고 있음을 확인하였다. 발전소보호계통 소프트웨어에 대한 통합시험은 공장시험 절차서에 적절히 반영되어있음을 확인하였고, 소프트웨어 설계와 관련하여 도출된 설계 결과물들에 대해 검토한 결과, 이들 결과물은 계획서에 따라 단계별로 요건이 추적될 수 있도록 요건 추적성 매트릭스를 적절히 작성되었음을 확인하였다.

결론적으로 신고리 3, 4호기의 안전 관련 계통의 소프트웨어는 소프트웨어 생명주기 동안 관련 기술기준 요건에 따라 적합하게 설계되고 관련 품질보증 활동이 적절하게 이루어졌으므로, 소프트웨어 설계 결과는 적합한 것으로 판단되었다.

③ 신한울 원전 1, 2호기 운영허가 심사 (2020년)

신한울 1호기는 2014년 12월 KHNP가 제출한 신한울 1호기 운영허가 신청을 제출한 이래로 원자력안전법 제111조에 따라 KINS가 심·검사를 수행하였다. 이후, 12회에 걸친 원안위 회의를 통해 2021년 7월 원안위 심의를 검쳐 신한울 1호기의 운영허가가 의결되었다.

KINS의 심사보고서 [KINS, 2020]에서는 디지털 기반의 발전소보호계통, 공학적안전설비기기에저계통, 원자로노심보호계통, 지진원자로자동정지계통 등 안전 계통 소프트웨어는 개념단

계, 요건분석/정의단계, 설계단계, 구현/코딩단계, 시험단계, 현장설치/점검단계, 운전 및 보수단계 등의 소프트웨어 생명주기에 따라 설계 및 개발됨을 확인하였다. 또한, KINS는 안전계통 소프트웨어에 대한 설치, 운전 및 유지보수, 훈련계획 등의 적합성 확인을 위하여 KHNP에 관련 문서를 요구하였으며, 해당 내용들을 검토한 결과, 안전계통 소프트웨어 설계 및 개발절차가 U.S. NRC RG 1.152, 1.168 ~ 1.173, 경수로형 원전 안전심사지침 부록 7-13, IEEE Std. 1074 등의 요건 및 기술기준을 만족함을 확인하였다. 또한, KHNP가 작성한 신한울 1, 2호기 원자로보호계통소프트웨어 프로그램 매뉴얼에 제시된 소프트웨어 생명주기 단계별로 해당 소프트웨어가 설계되었고 결과물이 생성되었음을 확인함으로써 IEEE Std. 7-4.3.2의 요건을 만족함을 확인하였다. 소프트웨어 독립 확인 및 검증은 V&V 공정에 따라 요건단계, 설계단계, 이행 및 시험단계별로 독립적인 확인 및 검증 조직에 의해 수행되어 보고서가 작성되었음을 확인하였다.

결론적으로, 신한울 1, 2호기의 안전 관련 계통의 소프트웨어는 소프트웨어 생명주기 동안 관련 기술기준 요건에 따라 적합하게 설계되고 관련 품질보증 활동이 적절하게 이루어졌으므로, 소프트웨어 설계 결과는 적합한 것으로 판단되었다.

KAERI

제2절 국외 규제기준 및 사례

1. 미국 NRC

가. 규제기준

미국에서는 항공우주, 통신 등 산업분야 안전 관련 시스템의 하드웨어 및 소프트웨어 개발, 확인 및 검증 기술이 세계적 수준을 유지하고, 원전 디지털 계측제어 계통에서의 고신뢰도 소프트웨어를 개발하기 위한 방법론과 확인 및 검증 기술 개발이 빠른 속도로 이루어지고 있다. 특히, 원전 계측제어 계통이 아날로그에서 디지털 기반으로 변화함에 따라 안전성 및 신뢰도 확보가 주요 현안이 되었는데, 미국 NRC는 디지털 장비의 신뢰도 평가 및 공통모드 고장우려 등에 대한 다양한 접근방법을 개발하여 인허가 근거가 되는 SRP (Standard Review Plan)인 NUREG-0800 (Rev.4, 1997)을 전면 수정하였으며, 기술 발전의 추이에 따라 지속적으로 개정하고 있다.

원전에서 사용되는 소프트웨어 중 디지털 원자로 보호계통, 공학적 안전설비 기기제어계통 소프트웨어와 같은 안전소프트웨어 (안전 필수, 안전 관련)는 높은 신뢰도를 가져야 한다. 그러므로 이러한 안전소프트웨어들에 대해 안전 계통의 계통요건을 만족하는 범주에서 소프트웨어 품질과 개발공정 전체에 대해 엄격한 규제요건이 적용된다. 미국 NRC의 소프트웨어 규제요건은 그림 1과 같이 체계적인 계층구조를 이루고 있으며 최상위 규제 요건으로 10 CFR 50 & 52, 10 CFR 50.55a(h), 10 CFR 50.49 등이 있으며 밑으로 규제지침인 SRP (NUREG-0800), Branch Technical Position (BTP), Regulatory Guide가 존재한다. 그 아래 기술기준은 IEEE/IEC Standards 등이 있으며, 그 밖에 NRC가 발간한 각종 연구보고서인 NUREG 보고서 등이 있다. NRC에서 활용하는 소프트웨어 및 디지털 계통 관련 규제기준은 다음을 포함한다.

- RG 1.152 : Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
- RG 1.168 : Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.169 : Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.170 : Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.171 : Software Unit Testing for Digital Computer Software Used in

Safety Systems of Nuclear Power Plants

- RG 1.172 : Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.173 : "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plant

KAERI

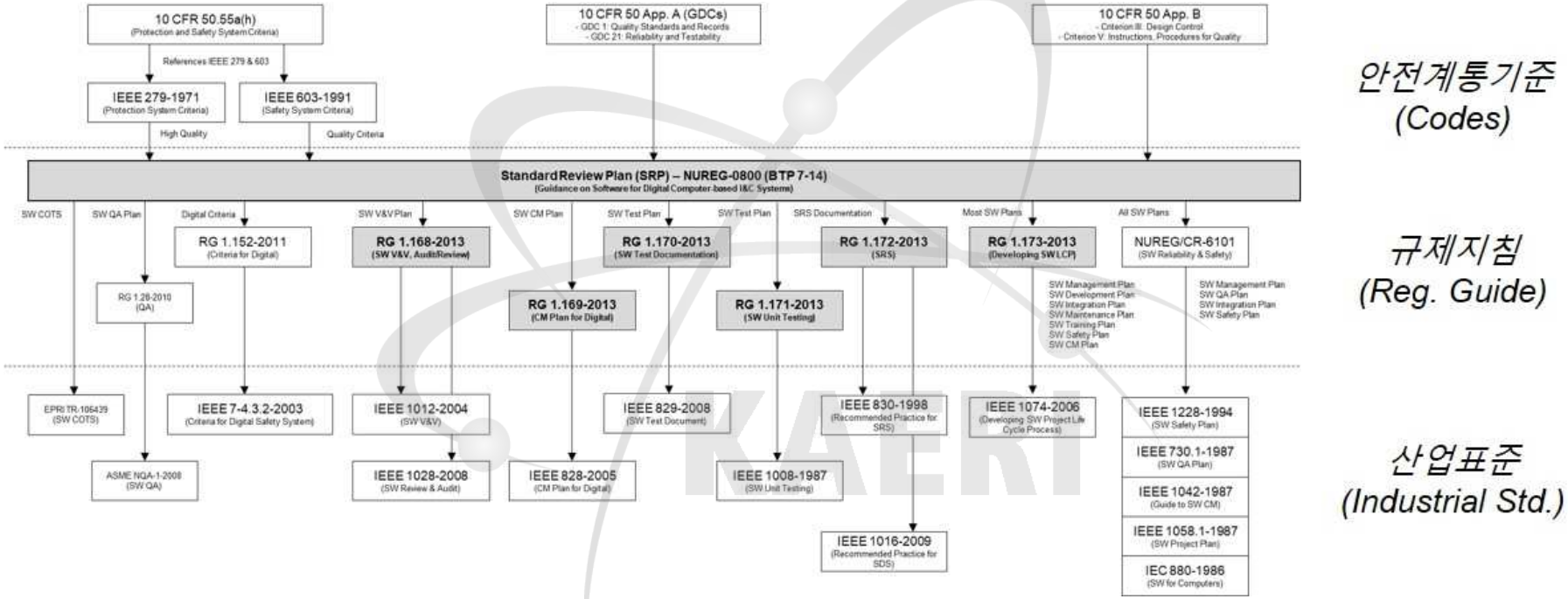


그림 25. 원자력 안전계통 소프트웨어를 위한 NRC 규제요건 체계

10 CFR 50 & 52, SRP Chapter 7, BTP-14, IEEE Std. 603-1998 (RG 1.53이 승인), IEEE Std. 7.4.3-2003 (RG 1.152 Rev. 2가 승인) 요건은 인허가를 위한 디지털 안전계통 소프트웨어의 안전기준으로 사용되는데 인허가를 위해서는 안전심사 항목 중 설계 지침의 적합성, 프로젝트 관리, 개발 계획, 확인 및 검증 등을 포함한 소프트웨어 생명주기 공정, 심층방어 및 다양성, 형상 관리 등에 대한 기준과 대책마련들이 요구되며 이를 만족하기 위하여 수행해야 할 주요 소프트웨어 규제사항 및 기술기준에 대한 내용은 다음과 같다

① 생명주기 공정(SLCP)

- 규제기준 : NRC는 RG 1.173을 규제기준으로 소프트웨어 생명주기 전체단계에 대한 감사와 검토를 수행하고 필요한 문서의 종류를 명시함. 특히 디지털 기반 안전계통의 개발공정에 소프트웨어 개발을 포함하여 하드웨어 및 소프트웨어 통합과 소프트웨어 개발공정들을 포함하도록 요구하며 소프트웨어 개발공정은 소프트웨어 개발, 기성 상용컴퓨터 (Commercial Off-the-Shelf; COTS) 검증, 소프트웨어 도구, 확인 및 검증, 형상관리 등의 품질기준을 만족하도록 요구함.
- 기술기준 : 소프트웨어 생명주기 공정에 대한 기술기준을 제공하는 IEEE Std. 1074 [IEEE, 2006]에 기반하여 소프트웨어 공정 개발 활동, 생명주기 공정 구성요소, 입출력 정보, Mapping 등이 규정되어야 함.

② 계획

- 규제기준 : NRC는 RG 1.169를 규제기준으로 소프트웨어 생명주기 전체단계에 대하여 감사와 검토를 수행하고 필요한 문서의 종류를 명시함.
- 기술기준 : IEEE Std. 1058.1에 의한 프로젝트 관리계획, IEEE Std. 730.1에 의한 소프트웨어 품질보증계획, IEEE Std. 1228에 의한 소프트웨어 안전계획(SSP), IEEE Std. 828에 의한 소프트웨어 형상 관리계획, IEEE Std. 1012에 의한 소프트웨어 확인검증계획이 수립되어야 함.

③ 요구분석

- 규제기준 : NRC는 RG 1.172를 규제기준으로 자연어나 명세언어에 의해 작성된 소프트웨어 요구명세에 대한 분석을 수행하는 단계로, 요구분석은 수학적으로 증명이 가능한 정형 방법이 권장됨.

- 기술기준 : IEEE Std. 830-1에 기반하여 소프트웨어 요구사항 명세서에 반드시 포함되어야 할 속성들 (정확성, 완전성, 일관성, 검토가능, 추적가능, 수정가능 등) 및 피해야 될 속성들 (모호성, 추측성, 막연성, 가능성 등)이 규정되어야 함.

④ 설계분석

- 규제기준 : 별도의 RG 규제기준은 없지만 NUREG-0800에서 요구하는 설계단계에서의 기능특성 (정확도, 신뢰성, 강인성, 안전성 등) 과 공정특성 (완전성, 일관성, 정확성 등)에 대한 체크리스트를 제공함.
- 기술기준 : NUREG-0800이 인정하는 IEEE Std. 1016은 소프트웨어 설계 명세 내용 및 구조를 규정한다. 설계 명세의 내용은 분해 명세 (Decomposition Description), 의존성 명세 (Dependency Description). 연계 명세 (Interface Description), 상세 명세 (Detailed Description)의 4가지 설계 관점을 기반으로 기술된다.

⑤ 구현분석

- 규제기준 : 별도의 RG 규제기준은 없지만 NUREG-0800에서 요구하는 구현단계 기능특성 (정확도, 신뢰성, 강인성, 안전성 등) 과 공정특성 (완전성, 일관성, 정확성 등)에 대한 체크리스트를 제공하며 구현된 코드에 대한 검사 (Inspection)을 수행하기 위해 소스코드를 요구할 수 있음.
- 기술기준 : NRC는 NUREG/CR-6463 [Hecht et al., 1996]을 안전 소프트웨어의 검토 지침으로 사용한다. 이는 안전계통에 사용되는 컴퓨터 언어 (Ada83, C/C++, Ladder Logic, Pascal, Structured Text, FBD 등)의 프로그래밍과 감사를 위한 각 언어별 지침으로 활용되며 안전에 직접적으로 관련되는 소프트웨어 품질 (신뢰성, 견고성, 강인성, 추적성, 유지보수성) 등을 평가한다.

⑥ 통합, 확인, 검증시험 분석

- 규제기준 : NRC는 RG 1.168, 1.170, 1.171을 규제기준으로 소프트웨어 품질을 확보하고 결함을 확인하기 위한 소프트웨어 확인 및 검증 활동들을 규정한다. 특히 소프트웨어 단위시험, 통합시험, 시스템 검증 및 수락시험에 대한 명세 및 보고서 등을 요구함. 상용 소프트웨어의 규제는 NUREG/CR-6421의 기성 소프트웨어에 대한 시험전략을 따르도록 한다.

- 기술기준 : IEEE Std. 1008은 소프트웨어 확인 및 검증계획뿐만 아니라 소프트웨어 단위 시험의 확인 및 검증계획 및 시험계획에서 수립된 계획정보를 규정한다. IEEE Std. 829는 시험계획 요건, 시험설계 명세, 시험사례 명세, 시험절차 명세, 시험 사고보고, 시험결과 등 안전계통의 소프트웨어 시험에 관한 문서화에 대한 내용을 기술한다. IEEE Std. 1028은 소프트웨어 검토 및 감사에 대한 기술기준을 기술한다. IEEE Std. 1074는 소프트웨어 시험활동을 반영한 생명주기 공정과 고 건전성 안전계통의 소프트웨어 개발에 대한 기술기준을 제시한다.

⑦ 설치 및 운영, 유지보수

- 규제기준 : 별도의 RG 규제기준은 없지만 NUREG-0800에서 요구하는 설치문서, 운전 및 유지보수 지침서 등 설치, 운영, 유지보수에 필요한 문서들이 마련되어야 하며 개발과정에서 발견되지 않은 결함을 보완하기 위한 보수 계획, 시험 계획과 이에 따른 형상관리 변경, 안전성분석 변경 등이 수행되어야 한다.
- 기술기준 : IEEE Std. 1219는 소프트웨어 보수 활동을 관리하고 실행하는 과정을 기술하며 결함을 정정하고 성능 및 품질 향상을 위한 소프트웨어 변경에 관한 기술기준을 제공한다.

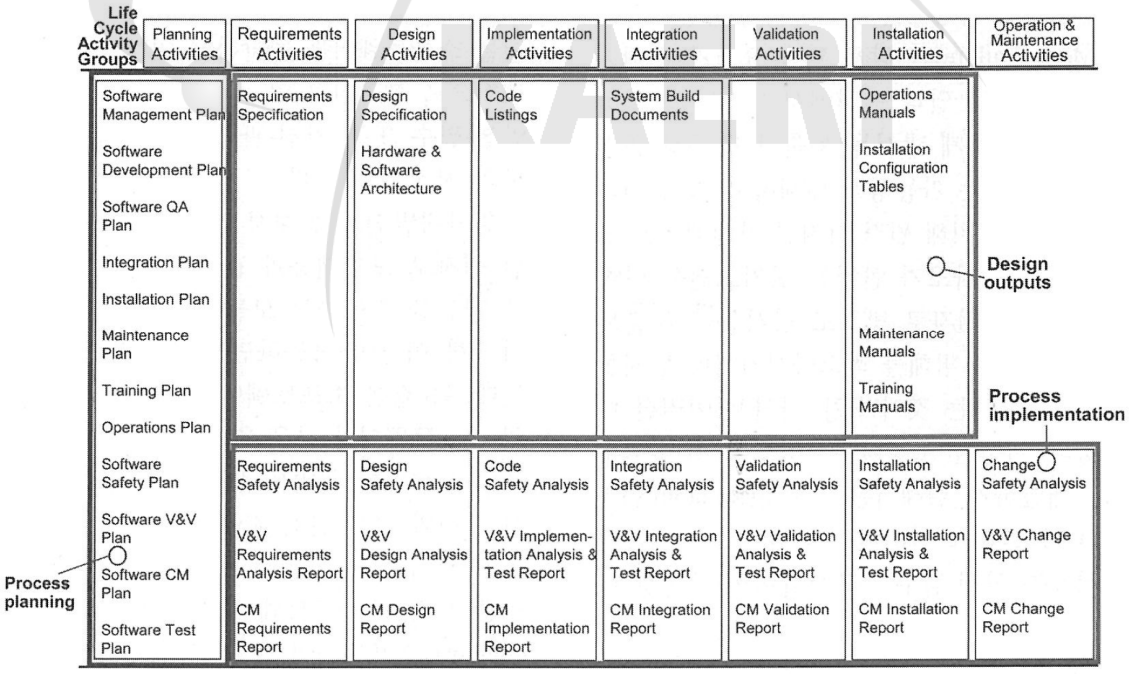


그림 26. 소프트웨어 생명주기 업무 정의

미국 NRC는 이미 활용되는 규제기준뿐만 아니라 디지털 계측제어계통의 고신뢰도 소프트웨어의 개발방법론, 확인 및 검증기술 개발에 주력하여 규제기준에 활용할 수 있는 소프트웨어 신뢰도 평가 방법론을 도출하기 위한 노력이 있어왔다. 특히, 1990년대부터 계측제어 및 인간공학위원회 (Control, Instrumentation, and Human Factors Branch)가 주관이 되어 LLNL, OSU, 한국원자력연구원 (KAERI), Brookhaven National Laboratory 등과 공동으로 다양한 정성적, 정량적 소프트웨어 신뢰도 평가 방법론을 개발해왔으며 각 방법론의 적용가능성을 확인한 바 있다.

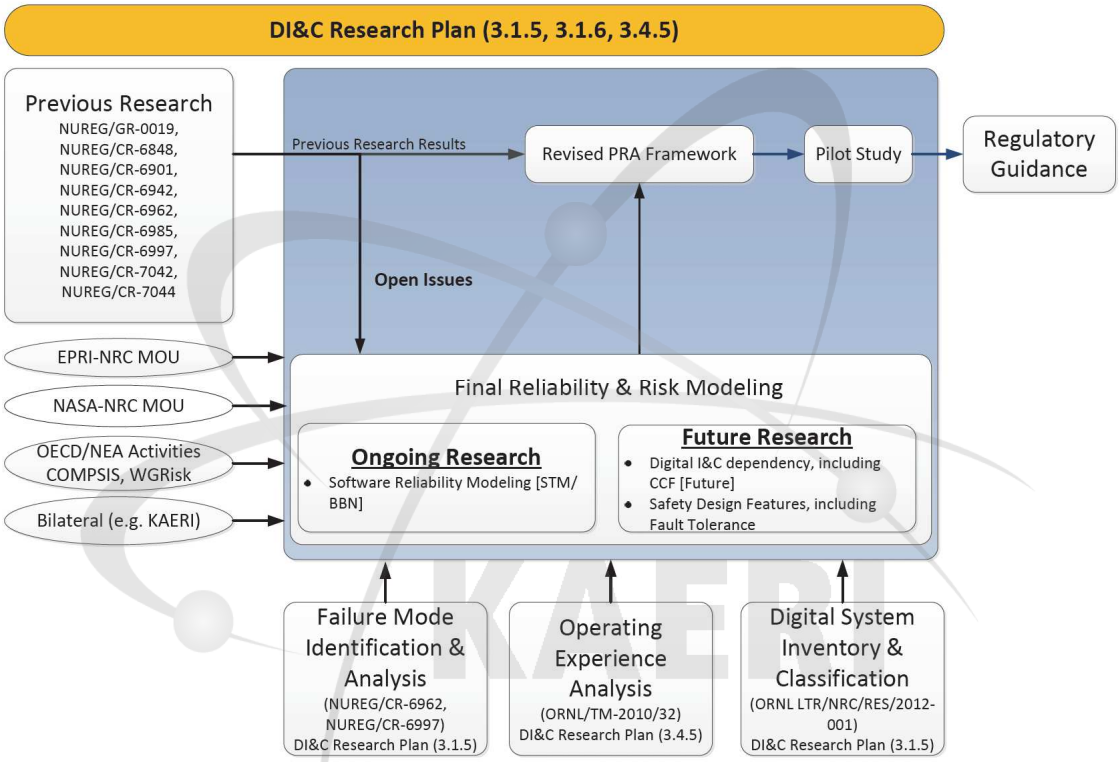


그림 27. 디지털 계통 신뢰도 평가를 위한 NRC 연구 활동 [Chu et al., 2018]

나. 규제사례

① VEGP-4 PMS Software

미국 NRC의 통합건설 및 운영허가 (COL) 제도는 원전건설허가와 조건부 운영허가를 일괄적으로 발급하는 제도 (10 CFR Part 52, Subpart C)이다. COL 신청자는 발전소가 공중의 건강과 안전, 공동의 방위와 안보에 부합하는 방식으로 건설되어 운영될 수 있음을 입증할 수 있는 모든 자료를 제출하여야 하며 발전소가 설계를 준수하여 건설되었음을 확인할 수 있는 검사시험분석합격기준 (ITAAC)을 제출하여야 하며 완공 후 원전운영을 개시하기 전에 NRC로부터 ITAAC 준수여부를 확인받아야 한다 [윤혜선, 2014]. 미국 NRC는 2019년 건설 중인 미국 Southern Nuclear Operating Company (SNC)의 Vogtle Electric Generating Plant (VEGP) 4호기의 Protection and Safety Monitoring System (PMS)의 소프트웨어에 대한 설계, 시험, 설치, 유지에 대한 검사를 완료하여 ITAAC 준수여부를 확인한 바 있다 [SNC, 2019]. PMS 소프트웨어에 대해 검사된 ITAAC 사항은 다음과 같으며 주로 소프트웨어 개발과 확인 및 검증 프로세스에 대한 정성적인 검사내용 등을 포함한다.

a) Software management (documentation requirements, standards, review requirements, procedures for problem reporting and corrective action)
b) Software configuration management (including historical records of software and control of software changes)
c) Software configuration management requirements are provided in the software configuration management plan
d) Verification and validation (V&V) requirements
e) Verification and validation (including requirements for reviewer independence)

이를 기반으로 ITAAC 완료를 위한 절차에 따라, SNC는 대상 ITAAC 및 관련된 교정 조치에 관련된 모든 사항에 대한 검토를 수행하였으며 PMS 소프트웨어는 관련된 ITAAC 사항을 만족하며 ITAAC으로 검증된 PMS 소프트웨어의 시스템, 구조 및 구성요소는 승인된 발전소 프로그램 및 절차에 따라 설계된 ITAAC 준수 상태로 유지되고 있음을 NRC에 제출하였고 이를 승인받은 바 있다.

② APR-1400 NRC DC

한국수력원자력(주)는 APR-1400 원전의 미국 NRC 설계인증을 취득하기 위하여 설계인증 설계문서를 2013년 9월에 미국 NRC에 최초 제출한 바 있다. 미국 NRC 설계인증은 미국 NRC가 특정원전의 표준설계에 대해 안전성을 평가하여 인증해주는 제도로 미국 내 해당 원전을 건설 및 운영할 수 있음을 의미한다. 하지만 일부 설계내용 부족으로 서류적합성 심사에서 반려된 바가 있으며, 서류미비사항 중 하나로 비안전제어계통의 소프트웨어 공통원인고장, 소프트웨어의 결정론적 성능 및 개발프로세스에 대한 평가를 요구하였다.

해당 서류미비사항을 해결하기 위해 한국수력원자력(주)는 디지털 원자로보호계통 (RPS)와 공학적 안전설비계통 (ESF-CCS) 내 안전신호를 생성하는 계통의 소프트웨어 개별 신뢰도 및 공통원인고장 신뢰도를 IEC 61226을 기반으로 가정하여 안전신호 가용도에 미치는 영향을 확률론적 안전성 평가 관점에서 분석하였다 [KEPCO/KHNP, 2015]. 또한, 소프트웨어 신뢰도에 대한 여러 민감도 분석을 수행하여 안전신호 가용도에 미치는 영향을 다방면으로 분석한 결과를 소프트웨어 공통원인고장 및 신뢰도에 대한 답변으로 제출하였다.

Digital I&C Sensitivity Cases

Case	Case Description	CDF	% Increase	LRF	%Increase
Base CDF	No changes	1.10E-06	N/A	1.00E-7	N/A
Case #1	OS CCF x 10	1.12E-06	3%	1.04E-7	4%
Case #2	All x 10	1.53E-06	39%	1.54E-7	54%
Case #3	All x 100	6.13E-06	459%	6.92E-7	592%
Case #4	DPSO-AP-DPS x 100	1.10E-06	<1%	1.00E-7	<1%
Case #5	DPSO-OS-DPS x 100	1.10E-06	<1%	1.00E-7	<1%
Case #6	PPSO-AP-BPM x 100	1.21E-06	10%	1.15E-7	15%
Case #7	PPSO-AP-GC x 100	2.10E-06	92%	2.22E-7	122%
Case #8	PPSO-AP-LC x 100	4.26E-06	289%	5.05E-7	405%
Case #9	PPSO-AP-LCL x 100	1.21E-06	10%	1.15E-7	15%
Case #10	PPSO-OS-PPS x 100	1.42E-06	30%	1.38E-7	38%
Case #11	No DPS	5.43E-06	396%	6.43E-7	543%
Case #12	All = 0	1.05E-06	-4.4%	9.43E-8	-5.7%

그림 28. NRC DC 심사 중 소프트웨어 신뢰도 민감도 분석 결과

이를 기반으로 한국수력원자력(주)는 2018년 9월 미국 NRC로부터 APR-1400 원전에 대한 표준설계승인서 (Standard Design Approval)을 취득하였으며 CFR Appendix에 최종적으로 등재되어 NRC DC를 취득하였다. 해당 규제사례는 안전계통에 사용되는 소프트웨어에 대해

기존 정성적 신뢰도뿐만 아니라 정량적 신뢰도 평가의 중요성을 NRC가 인지하며 사업자에게 권고한다는 점을 제시하며 원전 확률론적 안전성 평가 모델 내 소프트웨어 신뢰도의 모델링 방법 및 원전 신뢰도에 미치는 영향을 확률론적 안전성 평가 관점에서 적절히 평가하는 것에 대한 중요성을 나타낸다. 이러한 사례를 토대로 국내에서도 선제적으로 규제에 활용할 수 있는 소프트웨어의 정량적 신뢰도 평가 방법론을 개발하여 이를 규제지침에 적절히 반영할 수 있는 방안을 모색하는 것이 필요하다.

2. 캐나다 CNSC

가. 규제기준

캐나다 Canadian Nuclear Safety Commission (CNSC)는 원자력발전소로부터 원자력 연구시설, 동위원소 이용에 이르기까지 원자력 에너지와 물질이 활용되는 활동들을 규제한다. CNSC는 그 전신인 Atomic Energy Control Board (AECB)에서 1946년에 채택한 원자력에너지통제법(Atomic Energy Control Act)에 의거하여 원전인허가 및 안전규제 활동을 추진하여 왔으나 보다 체계적이고 효율적인 규제를 위해 1997년에 새롭게 원자력안전통제법(Nuclear Safety and Control Act)을 개정하여 규제에 적용해왔다.

CNSC의 경우 과거 안전규제를 미국이나 우리나라와 같이 명시적 규제가 아닌 협의 규제 방식으로 시행하였으며 안전 규제 체계와 문서가 미국이나 우리나라와 같이 상세하게 법적으로 명문화되어 있지 않았다. CNSC는 규제기준의 합리성을 알리고 그 이행을 장려하며, 저해요인을 사전 제거하고 현실적으로 달성 가능한 규제기준을 관련 이해당사자들의 의견을 수렴하여 제정하는 규제요건의 조성, 규제 기준 만족 검증, 시정 조치를 통해서 원자력 규제를 실시하였다. 여기서 규제 기준 만족 검증은 검사, 감사, 심사를 통해서 이루어지는데 검증에 적용되는 기준은 법령, CNSC 자체 규제문서, CNSC 전문가의 판단이 활용된다. 특히 검증 시 CNSC는 Atomic Energy Control Regulation (Public Whole Body Dose 〈 0.5 rem/yr)과 같은 상위 수준의 안전성 목표들을 제시하며 이 목표의 달성을 설계자에게 위임하되 이러한 설계가 안전성 목표를 합리적 신뢰도를 지니며 달성하는지 여부를 독립적으로 판단하였다. 이후 발전 및 연구용 원자로에 대한 규제체제는 과거의 관례 관행 및 개선을 종합한 협의 문서 (Consultative Documents)와 이를 근거로 작성된 규제문서 (Regulatory Documents)를 기준 및 지침으로 하여 수행해오던 규제활동들을 계층화 된 규제지침문서들 (Regulatory Policy, Regulatory Standard, Regulatory Guide, Regulatory Notice, Regulatory Practice 등)을 추가하면서 보다 명시적 규제기준과 지침에 근거하는 새로운 규제체계를 갖추었다. CNSC가 원자력발전소 안전과 관련한 규제에 활용하는 대표적인 문서 및 지침들은 다음과 같다.

- 규제문서(RECDOC) : 규제문서는 일반적으로 요건과 지침 모두를 단일 문서로 제시하며 필수 및 비필수 언어를 사용하여 이를 구별한다. CNSC는 원자력 규제에 대한 CNSC의 접근방식을 규제문서에 지속적으로 반영한다.

  - REGDOC-2.3.2 : Accident Management, Version 2
  - REGDOC-2.3.3 : Periodic Safety Reviews
  - REGDOC-2.4.1 : Deterministic Safety Analysis
  - REGDOC-2.4.2 : Probabilistic Safety Assessment (PSA) for Reactor Facilities, Version 2
  - REGDOC-2.6.1 : Reliability Programs for Nuclear Power Plants
  - REGDOC-3.3.1 : Reporting Requirements for Nuclear Power Plants, Version 2

- 규제정책(P) : 규제정책은 특정 주제 또는 관심 영역과 관련된 규제활동의 기초가 되는 철학, 원칙 또는 기본 요소를 설명한다. 규제정책 문서는 규제활동이 보증되는 이유를 설명하고 규제요건의 해석에 대한 일관성을 증진한다.

  - P-119 : Policy on Human Factors
  - P-223 : Protection of the Environment
  - P-242 : Considering Cost-Benefit Information
  - P-299 : Regulatory Fundamentals

- 규제표준(S) : 규제표준은 면허소지자가 무엇을 해야 하는지에 대한 CNSC의 기대를 명확히 하며 면허나 기타 법적 집행이 가능한 문서에 언급될 때 법적 요건이 된다. 규제 표준은 CNSC가 면허소지자가 달성하기를 기대하는 결과에 대한 상세한 설명을 제공한다.

  - S-99 : Reporting Requirements for Operating Nuclear Power Plants
  - S-294 : Probabilistic Safety Assessment (PSA) for Nuclear Power Plants

- S-296 : Environment Protection Policies, Programs and Procedures at Class I Nuclear Facilties and Uranium Mines and Mills

- 규제지침(G) : 규제지침은 면허소지자에게 CNSC의 기대치와 요건을 충족할 수 있는 방법을 알려준다. 면허소지자에게 각자의 면허활동과 관련된 요건 및 기대치의 특정 측면을 충족시키기 위한 권장 접근법을 제공한다.

  - G-225 : Emergency Planning at Class I Nuclear Facilities and Uranium Mines and Mills
  - G-276 : Human Factors Engineering Program Plans
  - G-278 : Human Factors Verification and Validation Program Plans
  - G-296 : Developing Environmental Protection Policies, Programs and Procedures at Class I Nuclear Facilties and Uranium Mines and Mills
  - G-306 : Severe Accident Management Programs for Nuclear Reactors

- 규제통보(N) : 규제통보는 특정 사안별 지침 또는 정보를 제공하는 것으로 사업자와 기타 이해관계자의 적기에 조치를 취해야하는 중요한 건강 안전 또는 법적 쟁점 사항을 통지한다.

- 기타 : 규정이나 인허가 조건으로 명시하지 않은 특정한 요건을 명문화한 것으로 주어진 방법이 아닌 다른 방법으로 추구하는 목적을 달성하여 요건을 충족시킬 수 있거나 요건을 만족시킬 필요가 없음을 입증할 때 예외를 인정한다.

  - R-7 : Requirements for Containment Systems for CANDU Nuclear Power Plants
  - R-8 : Requirements for Shutdown Systems for CANDU Nuclear Power Plants
  - R-9 : Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants
  - R-10 : The Use of Two Shutdown Systems in Reactors

- R-77 : Overpressure Protection Requirements for Primary Heat Transport Systems in CANDU Power Reactors Fitted with Two Shutdown Systems
- R-152 : Guidance on the Use of Deterministic and Probabilistic Criteria in Decision-making for Class I Nuclear Facilities
- C-6 : Requirements for the Safety Analysis of CANDU Nuclear Power Plants
- C-83 : Proposed General Amendments to the Atomic Energy Control Regulations
- C-98 : Requirements for Reliability Analysis of Safety-Related Systems in Nuclear Reactors

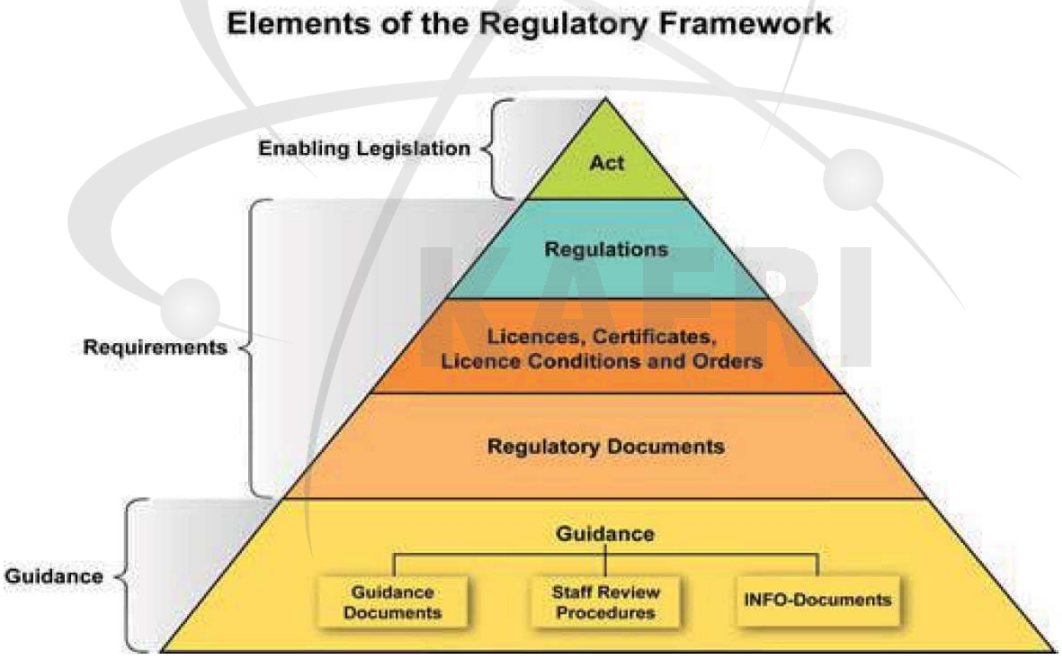


그림 29. 캐나다 CNSC의 원자력 안전 규제 체제

이러한 규제문서 중 원전 디지털 계통 안전 관련 규제요구사항이 명시된 문건은 R-8이 있으며 해당 문서에서는 원자로 정지계통의 설계, 환경, 가용도, 분리 및 독립성, 엑츄에이터, 상태 감시, 운영, 시험 등 다양한 요구사항들이 명문화되어 있다. 이 중 가용도 요구사항에는 정지 시스템의 불가용도가 10^{-3}/yr가 넘지 않도록 설계되어야 하며 이때 시스템의 불가용도는 엑츄에이터 등 시스템과 관련된 모든 매개변수들의 불가용도와 계통을 이루는 모든 기기의 불가용도를 결합하여 계산되어야 함을 명시하였다.

캐나다 CNSC는 디지털 계측제어계통 확률론적 안전성 평가 모델링 방법론과 소프트웨어 및 고장검출 신뢰성 평가 방법론 개발에 주력하여 확률론적 안전성 평가 기반 규제기준에 활용할 수 있는 다양한 디지털 특성에 대한 신뢰도 평가 방법론을 도출하기 위한 노력이 있어왔다 [McNelles et al., 2017; Renganathan et al., 2012; Chun, 2014]. 특히, 디지털 확률론적 안전성 평가의 관점에서 소프트웨어 모델링, 소프트웨어 공통고장원인, 소프트웨어 신뢰도 목표 등 여러 소프트웨어 규제 관련 이슈들을 도출하고 이러한 디지털 특성들을 고려한 디지털 계통 확률론적 안전성 평가모델 개발 및 리스크 평가 방법론을 개발해왔으며 각 방법론의 적용가능성을 원자로 정지계통 및 이중 제어 컴퓨터에 대해 확인한 바 있다 [Popvic et al., 1989].

나. 규제사례

캐나다 Darlington 원전 (Darlington Nuclear Generating Station; DNGS) 4기는 모두 CANDU 노형으로 캐나다원자력공사가 공급하였다. 이 중 1호기 및 2호기는 전 범위(Full scope) 디지털 계측제어 계통을 채택한 최초의 CANDU형 발전소로서 1990년에 시운전한 이래로 계속 운영되고 있다. 해당 원전의 원자로 정지계통은 물리적 원리 (중력의 원리를 이용하여 정지봉을 낙하시킴)로 정지시키는 정지계통 1번, 화학적 원리 (붕산 등 화학적 물질을 주입하는 방식으로 정지시킴)로 정지시키는 정지계통 2번으로 구성되어 있다. 그림 6과 같이 SDS1과 SDS2는 이중화 형태의 중복 (Redundancy) 및 디비전 내에서는 단일 고장 사고를 대비하기 위한 2/3 동시논리로 구성된다. 각 정지계통의 개발 (컴파일러, 프로그래밍 언어 및 개발 소프트웨어)는 서로 다른 개발팀에 의해서 수행되었으며, SDS1의 경우 FORTRAN 및 GA 어셈블리로 프로그래밍한 Model 220 (GA-16/220 μP)을 사용하였고 SDS2의 경우 PASCAL 및 MACRO 어셈블리 언어로 프로그래밍한 LS2-11/23 μP에 기반한 Digital Equipment Corporation (DEC)의 Programmed Data Processor (PDP) 컴퓨터를 사용하였다.

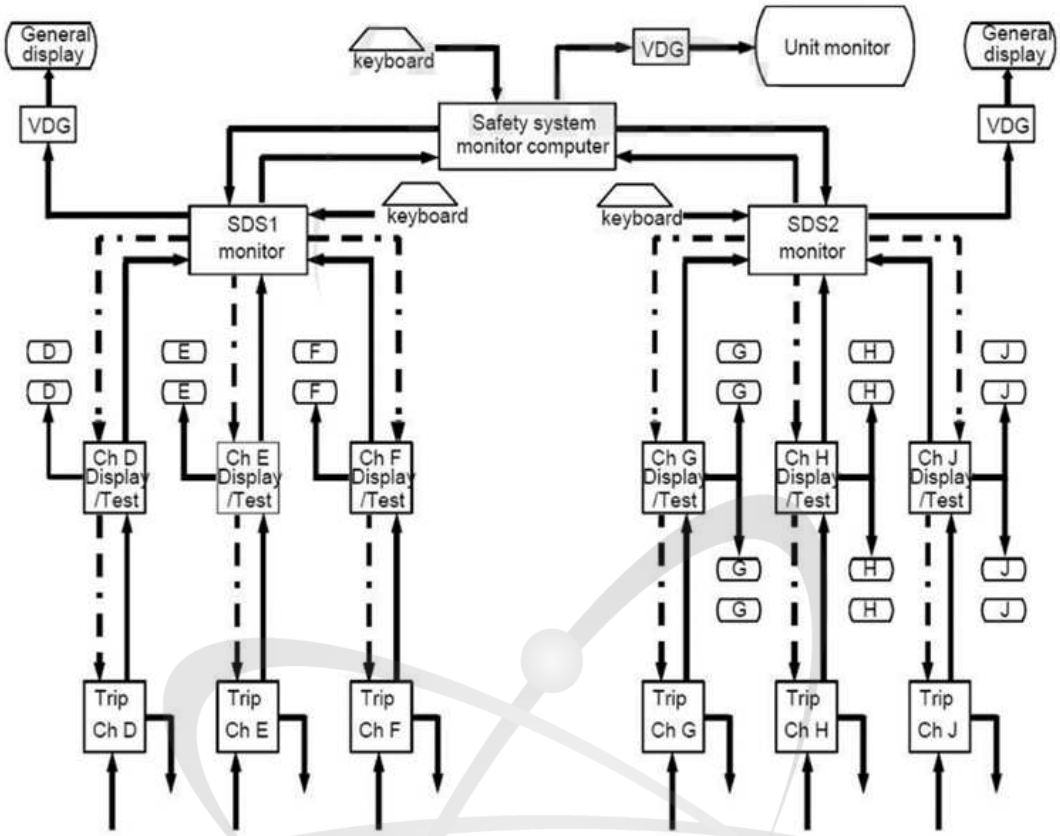


그림 30. 캐나다 DNGS 원자로 정지계통 구조도

캐나다 CNSC는 2017년 DNGS 트립 컴퓨터 교체 프로젝트의 일환으로 원자로 정지계통 1번, 2번의 신뢰성 적격성 문서를 검토하였다. CNSC는 R-8 규제문건의 Clause 3.4.1 (Each shutdown system shall be designed such that the fraction of time for which it is not available can be demonstrated to be less that 10^{-3} years per year)에 근거하여 Darlington Safety Report Part 2 Section 5.1.2 [OPG, 2018]를 검토하였다. Darlington Safety Report에서는 소프트웨어 신뢰도 평가를 위해 Statistical Random Testing 기반 Confidence Seeking Random Testing 방법론을 활용하여 신뢰성 요건이 달성됨을 입증하고자 하였으며 해당 방법론은 컴퓨터 소프트웨어가 기능 요건을 충족할 확률을 추정하기 위해 통계적으로 유의한 수의 관측치를 사용함으로서 특정 신뢰수준 (Confidence Level)에 대한 신뢰도를 평가할 수 있다.

해당 시험 방법론은 소프트웨어가 현장에 설치되었을 때 응답할 것으로 예상되는 입력 집합에 대해 목표한 신뢰도로 실현될 것이라는 증거로 예상되는 사용 프로필 (Usage Profile)을 통해 많은 횟수로 시험된다. 해당 원전의 운영사인 Ontario Power Generation (OPG)은 DNGS에 설치된 원자로 정지계통에 대해 Category I 계통의 소프트웨어 신뢰도 목표치인 10-4를 적용하기 위해 7982개의 시험 케이스를 생성하여 소프트웨어 실패가 발생하지 않는

시험 결과를 활용하여 소프트웨어 신뢰도가 54.9% 신뢰도 수준으로 10^{-4} 이하로 평가된 결과를 제출하였으며 이는 R-8 규제문건의 가용성 요구 조건을 만족하는 수준으로 평가되었다.

하지만 CNSC는 2017년 해당 시험에서 50% 신뢰도 수준을 선택하는 근거를 제공할 것을 OPG에 요청하였으며 OPG는 1990년대 수행된 OASES Safety Critical Software Engineering Standard 등의 근거에 기반하여 소프트웨어 시험이 수행되었으며 소프트웨어는 시험 이외에도 신뢰성 적격심사, 제품의 철저한 검토 및 검증, 유효성 검사의 완료로 실제 신뢰수준은 50%보다 높을 것으로 예상된다고 답변하였다. 하지만 CNSC는 INFO-0611 보고서 [AECB, 1995]와 ONR NS-TAST-GD-046 보고서를 근거로 하여 안전에 중요한 기능이 있는 계통에 대해 95~99% 신뢰수준을 적용한 소프트웨어 신뢰성 시험을 하도록 권고하였으며, 향후 OPG가 50% 신뢰수준에 대한 정당한 사유를 제공하지 않는 한 99% 신뢰수준을 가정하였을 경우 도출되는 46050개의 시험 케이스에 대한 시험 결과를 생성할 것을 권고하였다. 실제로 ONR의 신뢰도 요건을 만족하기 위해, 프랑스 운영사인 EdF와 AREVA는 TXS 기반 원자로보호계통의 프로그래머블 로직 컨트롤러 플랫폼인 TELEPERM-XS에 대해 높은 수준의 신뢰수준으로 10-4의 신뢰도를 입증하고자 하는 계획서를 제출한 바 있다.

	SLOCA	LLOCA	Mod. Sys. (pipe break)	Mod. Sys. (Loss of cooling)	Loss of Class IV	Feedwater	Steam Supply (Bal. Hdr)	Steam Supply (MSL & Reheater)	LORC	LOR from Low Power
Event Classification (1 – 5) "EC"	2	3	2	1	1	3	5	3	1	1
# of Trip Parameters Expected "NP"	3	4	2	1	5	3	4	3	3	2
Length of Average Trajectory "T"	175	6	300a.	230a.	15	190	70	190	50	80
Distribution Factor (DF) = EC-1+ NP/10 + 15/T	.89	1.73* * "T" too small, assigned value of 15 for calculation	.75	1.17	2.50	.71	.81	.71	1.60	1.39
Number of Test Cases = 7000*DF/ΣDF	502	982	425	660	1472	403	461	403	906	786
Appendix B Tables and number of test cases	B-9: 125 B-10: 125 B-11: 127 B-12; 125	B-13: 982	B-8: 425	B-7: 660	B-1: 500** B-2: 250 B-3: 361 B-4; 361	B-5: 200 B-6: 203	B-15: 461	B-16: 403	B14: 906	B-17: 786

* Because of the small number of reactor parameters affected by this accident scenario, and the long transient times involved, the length of the transient modeled in the input test files will be compressed to a time duration significantly shorter (~30 seconds) than those indicated in the table.

** Table B-1 (Total loss of Cl IV power from high power) is more likely than from reduced power (Table B-2), hence has more test cases.

그림 31. DNGS SDS1, SDS2 소프트웨어 시험 케이스 일부

3. 핀란드 STUK

가. 규제기준

핀란드에서 원자력 관련 운영규제는 핀란드의 원자력 관련 최상위 법령인 원자력에너지법 (Nuclear Energy Act)과 방사능법 (Radiation Act)에 의거해 고용경제부 (Ministry of Employment and the Economy)와 사회보건부 (Ministry of Social Affairs and Health)가 총괄하고 있으며, 실질적인 규제업무는 원자력안전청 (Radiation and Nuclear Safety Authority; STUK)이 담당하고 있다. 핀란드의 현행 원자력 법률은 1987년부터 시행된 원자력에너지법 (Nuclear Energy Act)에 기초하며 2008년 원자력 에너지 법안은 현행 안전 요건 수준과 2000년에 시행된 새로운 핀란드 헌법에 부합되도록 갱신되었다.

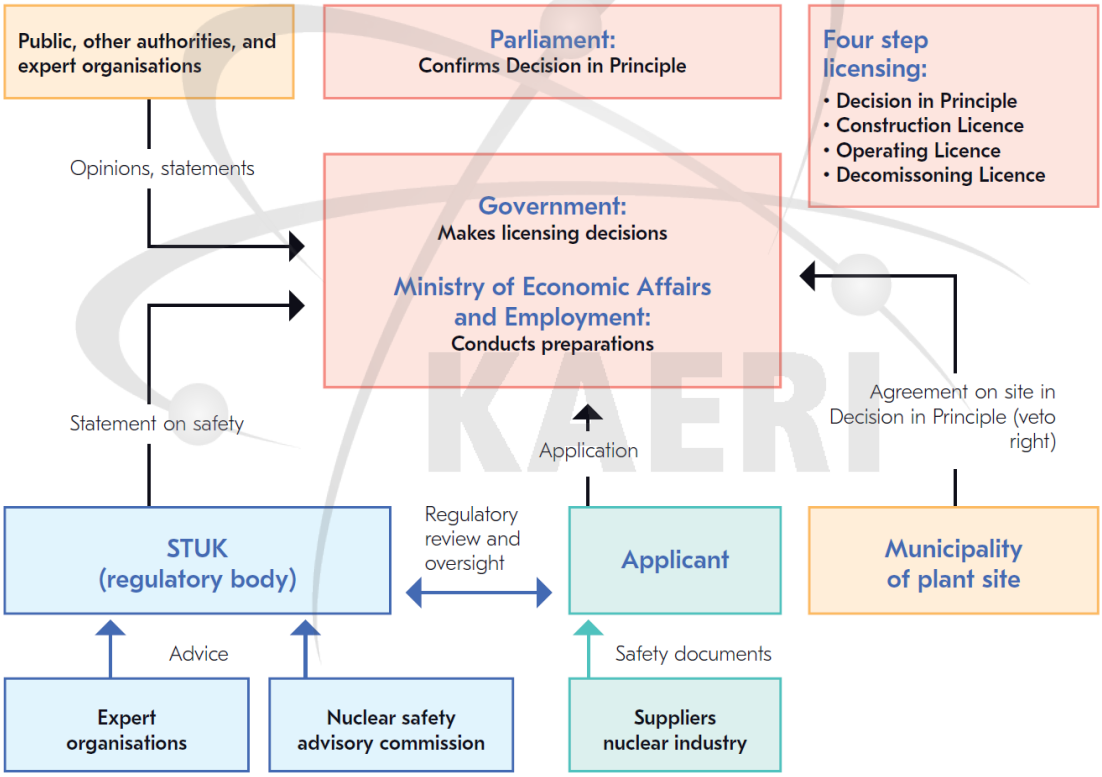


그림 32. 원자력 관련 핀란드 규제기관 및 프로세스 [STUK, 2019a]

원자력에너지법 하위에 Nuclear Energy Decree 및 STUK Regulation 등 법적 강제성을 가지는 법령 등이 있으며, 그 중 STUK Regulation은 2012년에 원자력 및 방사선 안전에 대한 핀란드 규제 체제는 IRRS (Integrated Regulatory Review Service) 프로세스에서 검토되었으며, 이에 따라 STUK의 독립성을 높이고 권한을 확대하기 위해 과거 Government Decree에 명시되어 있던 내용을 2015년에 STUK Regulation으로 변경하여 법률에 일부 개

정이 이루어졌으며, 원자력 폐기물 처리의 안전, 원자력 시설의 비상 및 보안 배치, 우라늄 및 토륨 생산을 목표로 하는 광업 및 제분 운영에 관한 새로운 영역의 규제체계를 규정하였다. STUK Regulation은 다음과 같이 크게 5가지가 있으며, STUK에 원자력 시설 근처의 방사선 감시 권한, 원자력 발전소의 안전, 원자력 폐기물의 처리 안전, 비상 및 보안 준비 등 법적 구속력 있는 조항들을 포함한다. 해당 규제규정은 2016년 발행되었으며, 2018년 12월 15부터 시행되었다.

- STUK Regulation on the Safety of Nuclear Power Plants (STUK Y/1/2018)
- STUK Regulation on the Emergency Arrangements of a Nuclear Power Plant (STUK/Y/2/2018)
- STUK Regulation on the Security in the Use of Nuclear Energy (STUK Y/3/2016)
- STUK Regulation on the Safety of Disposal of Nuclear Waste (STUK Y/4/2018)
- STUK Regulation on the Safety of Mining and Milling Operations aimed at Producing Uranium or Thorium (STUK Y/5/2016)

STUK은 원자력법 제 7조 R항에 따라 STUK Regulation에 따라 안전수준의 이행에 관한 상세한 안전요건을 명시하여야 한다. 이러한 요구사항은 YVL Guide라고 하는 규제 가이드에 제시되어 있다. YVL Guide는 2013년 개정된 이후, 총 47개의 YVL Guide가 5개 주제의 영역으로 구분되어 있으며, 단일 가이드에는 표준 형식과 번호가 매겨진 요구 사항들이 간략히 제시되어 있다. STUK은 2013년 말 새로운 YVL 지침을 발표한 후 2014년 1월에 면허소지자에게 요구사항의 이행에 관한 평가(요건 평가에 의한 요건, 이행의 정당성, 발전소 문서화에 대한 참조 등)를 수행하도록 요청하였으며, 운영 중 및 건설 중 원전, 연구용 원자로에 별도로 적용되었다.

- A. Safety Management of a Nuclear Facility
  - A.1 Regulatory oversight of safety in the use of nuclear energy
  - A.2 Site for a nuclear facility
  - A.3 Leadership and management for safety
  - A.4 Organization and personnel of a nuclear facility
  - A.5 Construction and commissioning of a nuclear facility
  - A.6 Conduct of operations at a nuclear power plant
  - A.7 Probabilistic risk assessment and risk management of a nuclear power plant
  - A.8 Ageing management of a nuclear facility
  - A.9 Regular reporting on the operation of a nuclear facility
  - A.10 Operating experience feedback of a nuclear facility

- A.11 Security of a nuclear facility
- A.12 Information security management of a nuclear facility

- B. Plant and System Design

- B.1 Safety design of a nuclear power plant
- B.2 Classification of systems, structures and components of a nuclear facility
- B.3 Deterministic safety analyses for a nuclear power plant
- B.4 Nuclear fuel and reactor
- B.5 Reactor coolant circuit of a nuclear power plant
- B.6 Containment of a nuclear power plant
- B.7 Provisions for internal and external hazards at a nuclear facility
- B.8 Fire protection at a nuclear facility

- C. Radiation Safety

- C.1 Structural radiation safety at a nuclear facility
- C.2 Radiation protection and exposure monitoring of nuclear facility workers
- C.3 Limitation and monitoring of radioactive releases from a nuclear facility
- C.4 Assessment of radiation doses to the public in the vicinity of a nuclear facility
- C.5 Emergency arrangements of a nuclear power plant
- C.6 Radiation monitoring at a nuclear facility
- C.7 Radiological monitoring of the environment of a nuclear facility

- D. Radiation Safety of a Nuclear Facility and Environment

- D.1 Regulatory control of nuclear safeguards
- D.2 Transport of nuclear materials and nuclear waste
- D.3 Handling and storage of nuclear fuel
- D.4 Predisposal management of low and intermediate level nuclear waste and decommissioning of a nuclear facility
- D.5 Disposal of nuclear waste
- D.6 Production of uranium and thorium in the mining and milling industry
- D.7 Release barriers of spent nuclear fuel disposal facility

- E. Structures and Equipment of a Nuclear Facility

- E.1 Authorized inspection body and the licensee's in-house inspection organization
- E.2 Procurement and operation of nuclear fuel and control rods
- E.3 Pressure vessels and piping of a nuclear facility
- E.4 Strength analyses of nuclear power plant pressure equipment
- E.5 In-service inspection of nuclear facility pressure equipment with nondestructive testing methods
- E.6 Buildings and structures of a nuclear facility

- E.7 Electrical and I&C equipment of a nuclear facility
- E.8 Valves of a nuclear facility
- E.9 Pumps of a nuclear facility
- E.10 Emergency power supplies of a nuclear facility
- E.11 Hoisting and transfer equipment of a nuclear facility
- E.12 Testing organizations for mechanical components and structures of a nuclear facility
- E.13 Ventilation and air conditioning equipment of a nuclear facility

이러한 규제문서 중 원전 디지털 계통 안전 관련 규제요구사항이 명시된 문건은 YVL E.7 Chapter 6이 있으며, 해당 조항에서는 소프트웨어가 설치된 기기들에 대한 품질 등 다양한 요구사항이 명문화되어 있다. 특히, YVL E.7 518a, 608, 611항에는 Safety Class 2나 3에 해당하는 소프트웨어의 고장 원인을 충분히 식별하고 분석해야 함을 명시하였다 [Haapanen et al., 2000]. 원자력 발전소 안전 설계 관련 규제지침인 YVL B.1 Chapter 3에는 안전 기능을 수행하는 시스템의 안전 요구사항이 명문화되어있는데, 이 중 351, 352항에는 안전 기능을 수행하는 시스템의 고장 및 공통 원인 고장은 설계 시 내결함성(failure tolerance)분석을 통해 평가되어야 하며, 안전 기능을 수행하는 시스템에 영향을 미치는 하드웨어와 소프트웨어를 포함한 모든 구성부품에 대한 모든 고장모드를 분석해야 함을 명시하였다.

나. 규제사례

핀란드 Olkiluoto 3호기는 프랑스 AREVA의 EPR 노형으로 2005년 건설 시작되었으며 I&C 계통에는 소프트웨어가 설치된 Teleperm XS (TXS) PLC 플랫폼 기반의 디지털 RPS가 설치되었다. 개발사인 AREVA와 핀란드 원자력연구소인 NKS (Nordic Nuclear Safety Research)는 원자력발전소에 대한 확률론적 안전성 평가 목적을 위해 TXS에 설치된 응용 소프트웨어에 대한 신뢰성 정량화 방법을 개발하였으며, 확률론적 안전성 평가에서 모델링해야 할 소프트웨어 실패를 설명하는 고장 모드, 각 고장 유형에 대한 정량화 모델, TXS 플랫폼에 대한 소프트웨어 오류에 대한 작동 데이터들을 분석하였다. 또한, 확률론적 안전성 평가를 통해 소프트웨어가 TXS 계통 불가용도에 미치는 영향을 평가하였다 [Bäckström et al., 2000].

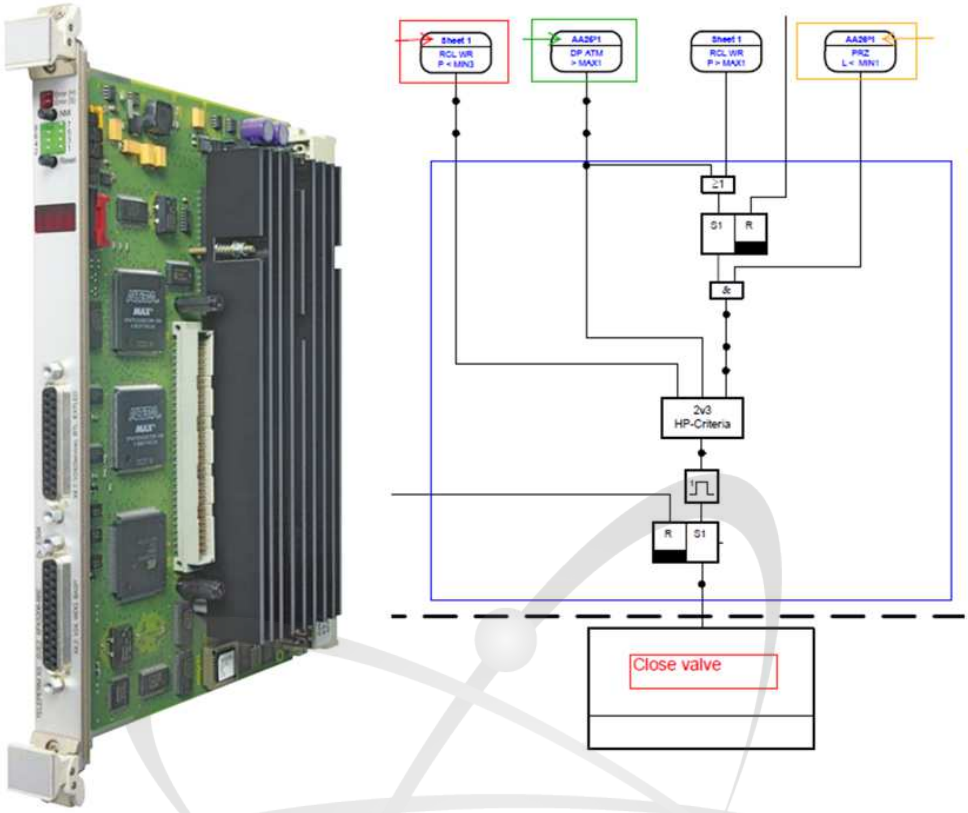


그림 33. TXS PLC 플랫폼 및 응용 소프트웨어 로직 일부 [STUK, 2019b]

STUK은 해당 원전의 I&C 계통에 대해 시험 환경 (Test Bay)와 발전소 현장에서 소프트웨어에 수행된 시험들을 감독했으며, 여러 차례 분석 방법과 절차에 대한 교정을 요구하였다. 발전소 공급자는 시스템별 고장과 영향 분석을 통해 계측제어 장비들이 고장나는 상황에서 STUK이 제시한 기준을 충족함을 입증했다. 특히, I&C 시스템과 소프트웨어 기반 부품에 몇 가지 고장이 발생한 상황에서도 발전소가 YVL 허용 기준을 충족한다고 Olkiluoto 3호기 FSAR 보고서에서 평가하였다 [STUK, 2019b].

KAERI

제5장

국내 소프트웨어 신뢰도 규제기술 개선방향 제안

KAERI

KAERI

제5장 국내 소프트웨어 신뢰도 규제기술 개선방향 제안

현재 국내 SW 신뢰도 관련 규제기술은 SW 생명주기 공정 품질 평가 등 기존 정성적 신뢰도 검증 분야에 초점이 맞추어져 있으며, 보호계통의 경우 계통 신뢰도에 대한 수용은 정량적인 신뢰도 목표보다 결정론적인 기준에 근거한다. 중요한 안전 기능을 수행하는 RPS 계통의 경우 KINS/RS-N08.00 8.2.3절에 따라 정성적 또는 정량적 신뢰도 목표가 달성되었음이 확인되어야 함. 현재 소프트웨어에 대한 국내 규제는 정성적 신뢰성 확인을 위주로 수행되지만, 원전의 안전기능 수행 및 계통 신뢰성 향상을 위해 KINS/RS-N08.01에 근거하여 IEEE Std. 1012 기준 SIL-4가 요구되는 RPS SW가 IEC 61508과 같은 국제표준에서 제시하는 정량적 신뢰도 목표를 만족하는지 확인할 필요가 있다.

디지털 안전 계통 소프트웨어의 정량적 신뢰도 평가 결과는 리스크 정보를 활용한 디지털 안전 계통 운영기술지침서 감시시험주기 연장 등에도 활용 가능할 것으로 평가되었다. 미국 NRC는 지난 20년간 규제체계에 적합한 SW 신뢰도 평가 방법론을 시도하고 원전 PSA 모델에 반영하려는 노력이 있어왔다. 국내에서도 이러한 국제적 흐름에 맞추어 사업자와 독립적으로 규제자의 측면에서 SW 정량적 신뢰도 평가 방법론을 개발하고 이를 규제에 활용할 수 있는 방안에 대한 모색이 필요하였다.

일반적으로 원전에서 사용되는 안전 필수 SW는 정상 운전 상태에서 무결성이 보장된다 하더라도 [KHNP, 2019], 예측하기 어려운 HW-SW 상호작용 등이 고려되어야 할 비정상상태에서는 SW의 신뢰성을 확인하기 어렵다. SW 결함 촉발 조건이 될 수 있는 다양한 비정상상태가 존재할 수 있으므로, SW 생명 주기 동안 마주할 수 있는 대부분의 동작 환경들을 고려해 SW 신뢰도 분석 결과를 생성할 수 있는 SW 신뢰도 평가 방법이 요구된다.

KAERI

제6장

결 론

KAERI

KAERI

제6장 결 론

본 연구에서는 “원전 디지털 I&C 소프트웨어 신뢰성 평가 규제 방법론 개발” 과제의 당해연도 연구목표인 “국내외 디지털 I&C 소프트웨어 신뢰도 평가 방법론 분석”을 위해 SW 정성적/정량적 신뢰도 평가 방법론 조사 및 국내외 SW 신뢰도 관련 규제기준 및 사례들을 분석하고 국내 규제기술의 개선방향을 제안하였다.

국내외 여러 정성적/정량적 방법론들의 특징 및 한계점 분석 결과, 국내 SW 신뢰도 규제기준을 고려하여 시험 기반 기법이 가장 적합할 것으로 판단된다. 특히, 미국 NRC, 캐나다 CNSC 규제 사례에서 확인할 수 있듯이, 국외에서 시험 기반 방법론을 적극적으로 도입하고 있으며 타 방법론에 비해 평가 결과의 불확실성 최소화, 시험 과정 및 결과검증 측면에서 장점을 가진다. 다만, 운전이력의 반영방안, SW 시험케이스의 형태에 대한 정의 및 효율적 도출방안 개발, 구동환경과 유사하면서도 단시간에 많은 수의 시험을 수행할 수 있는 시험환경 구축이 요구된다. 이 중 시험환경 구축과 관련하여, 국내 원전 디지털 안전등급 플랫폼으로 활용되고 있는 PLC SW 시험용 시뮬레이션 환경 [Lee et al., 2020], 디지털 트윈 [KHNP, 2021] 등을 시험 환경으로 활용할 수 있을 것으로 기대된다.

국내 규제기준 및 기술과 관련하여, 현재 KINS는 SW 안전성 분석과 관련하여 SW 생명주기 품질 관리 등 미국 NRC의 정성적 평가 요건들을 규제지침으로 활용하고 있지만, 향후 미국 NRC의 APR-1400 NRC DC 사례, 캐나다 CNSC의 DNGS SDS 사례 등을 기반으로 정량적 평가 요건을 규제 지침에 추가할 것을 고려해야 한다.

당해연도 연구결과는 해당 과제의 차차기년도 “원전 디지털 I&C 소프트웨어 신뢰도 정량화(실패율) 방법론 개발” 업무에 활용되며, 사례분석을 통해 최종 선정된 SW 신뢰도 평가 방법론의 적용가능성을 평가할 예정이다.

KAERI

제7장

참고문헌

KAERI

KAERI

제7장 참고문헌

[AECB, 1995] AECB, INFO-0611 Report, Reliability Assessment for Safety Critical Systems by Statistical Random Testing, AECB Project No. 2.127.5, Atomic Energy Control Board, 1995.

[AECL, 1993] AECL, Program Functional Specification, SDS2 Programmable Digital Comparators, Wolsong NPP 2,3,4. Technical Report 86-68300-PFS-000 Rev.2, Atomic Energy of Canada Limited, 1993.

[Aldemir et al., 2009] Aldemir T., Guarro S., Kirschenbaum J., Mandelli D., Mangan L. A., Bucci P., Yau M., Johnson B., Elks C., Ekici E., Stovsky M. P., Miller D. W., Sun X., Arndt S. A., Nguyen Q., Dion J., A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems. NUREG/CR-6985, U.S. Nuclear Regulatory Commission, 2009.

[Bäckström et al., 2000] Bäckström O., Holmberg J.-E., Jockenhövel-Barttfeld M., Porthin M., Taurines A., Tyrväinen T., Software Reliability Analysis for PSA: Failure Mode and Data Analysis, NKS-341, Nordic Nuclear Safety Research, 2000.

[Cho et al., 2019] Cho J., Shin S. M., Lee S. J., Jung W., Exhaustive Test Cases for the Software Reliability of Safety-critical Digital Systems in Nuclear Power Plants, Nuclear Engineering and Design, 352, 110151, 2019.

[Chu et al., 2009] Chu T. L., Martinez-Guridi G., Yue M., Samanta P., Vinod G., Lehner J., Workshop on Philosophical Basis for Incorporating Software Failures in a Probabilistic Risk Assessment, BNL-90571-2009-IR, Brook Haven National Laboratory, 2009.

[Chu et al., 2013] Chu T. L., Yue M., Martinez-Guridi G., Lehner J., Development of Quantitative Software Reliability Models for Digital Protection Systems of Nuclear Power Plants. NUREG/CR-7044, BNL-NUREG-99068-2013, U.S. Nuclear Regulatory Commission, 2013.

[Chu et al., 2016] Chu T. L., Varuttamaseni A., Baek J. S., A Statistical Testing Approach for Quantifying Software Reliability: Application to an Example System, BNL-112743-2016, Brookhaven National Laboratory, 2016.

[Chu et al., 2017] Chu T. L., Varuttamaseni A., Baek J. S., Yue M., Kaser T., Marts G., Murray P., Harwood B., Johnson N., Li M., Development of A Statistical Testing Approach for Quantifying Safety-Related Digital

System on Demand Failure Probability, NUREG/CR-7234, U.S. Nuclear Regulatory Commission, 2017.

[Chu et al., 2018] Chu T. L., Varuttamaseni A., Yue M., Lee S. J., Kang H. G., Cho J., Yang S., Developing a Bayesian Belief Network Model for Quantifying the Probability of Software Failure of a Protection System, NUREG/CR-7233, U.S. Nuclear Regulatory Commission, 2018.

[Chun, 2014] Chun G., Licensing of Safety Critical Software for Nuclear Reactors, Task Force on Safety Critical Software Working Group Meeting, 2014.

[Dalem, 1994] Dalem D. V. Logic and Structure. Springer-Verlag, 1994.

[Dunjo et al., 2010] Dunjo J., Hazard and Operability (HAZOP) analysis. A literature review, Journal of Hazardous Materials, vol. 173, pp. 19-32, 2010.

[Emerson et al., 1986] Emerson E. A., Edmund M. C., Sistla A. P., Automatic Verification of Finite State Concurrent System using Temporal Logic Specification. ACM Trans. Programming Languages and Systems, vol. 8, no. 2, pp. 244-263, 1986.

[Eom et al., 2009] Eom H. S., Park G. Y., Kang H. G., Jang S. C., Reliability Assessment of a Safety-Critical Software by Using Generalized Bayesian Nets, 6th ANS Topical Meeting on Nuclear Plant Instrumentation, Controls and Human-Machine Interfaces Technologies (NPIC&HMIT 2009), 2009.

[Eom et al., 2013] Eom H. S., Park G. Y., Jang S. C., Son H. S., Kang H. G., V&V-based Remaining Fault Estimation Model for Safety-critical Software of a Nuclear Power Plant. Annals of Nuclear Energy, vol. 51, pp. 38-49, 2013.

[Ericson, 2016] Ericson C. A., Hazard Analysis Techniques for System Safety, Wiley, 2016.

[Fenton et al., 2008] Fenton N., Neil M., Marquez D., Using Bayesian Networks to Predict Software Defects and Reliability, Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, vol. 222, no. 4, pp. 701-712, 2008.

[Garrett et al., 1999] Garrett C., Apostolakis G., Context in the Risk Assessment of Digital Systems, Risk Analysis, vol. 19, pp. 23-32, 1999.

[Goševa-Popstojanova, 2001] Goševa-Popstojanova K., Trivedi K. S., Architecture-based Approach to Reliability Assessment of Software Systems. Performance Evaluation, vol. 45, no. 2-3, pp. 179-204, 2001.

[Haapanen et al., 2000] Haapanen P., Korhonen J., Pulkkinen U., Licensing Process for Safety-critical Software-based Systems, STUK-YTO-TR171, Radiation and Nuclear Safety Authority, 2000.

[Hassapis et al., 1998] Hassapis G., Kotini I., Doulgeri Z., Validation of a SFC Software

Specification by using Hybrid Automata, Information Control in Manufacturing Symposium (INCOM 98), 1998.

[Hecht et al., 1996] Hecht H., Hecht M., Graff S., Green W., Lin D., Koch S., Tai A., Wendelboe D., Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems, NUREG/CR-6463, U.S. Nuclear Regulatory Commission, 1996.

[Heitmeyer et al., 1998] Heitmeyer C., Kirby J., Labaw B. , Bharadwaj, R., SCR: A Toolset for Specifying and Analyzing Software Requirements, 10th International Conference on Computer Aided Verification (CAV'98), 1998.

[IAEA, 2009] IAEA, Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants, IAEA NP-T-1.5, International Atomic Energy Agency, 2009.

[IAEA, 2018] IAEA, Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants, IAEA NP-T-3.27, International Atomic Energy Agency, 2018.

[IEEE, 2006] IEEE, IEEE Standard for Developing a Software Project Life Cycle Process, IEEE Std. 1074, Institute of Electrical and Electronics Engineers, 2006.

[IEEE, 2016] IEEE, IEEE Recommended Practice on Software Reliability, IEEE Std. 1633-2016, Institute of Electrical and Electronics Engineers, 2016.

[ISO/IEC, 2015] ISO/IEC, Information Technology - Vocabulary, ISO/IEC 2382:2015, International Organization for Standardization/International Electrotechnical Commission, 2015.

[KAERI, 2008a] 한국원자력연구원, 원자로보호계통 소프트웨어 요구사항 명세 안전성 분석 보고서, KNICS-RPS-SVR122(Rev.02), 한국원자력연구원, 2008.

[KAERI, 2008b] 한국원자력연구원, 원자로보호계통 소프트웨어 설계명세 안전성 분석 보고서, KNICS-RPS-SVR132(Rev.02), 한국원자력연구원, 2008.

[KAERI, 2008c] 한국원자력연구원, 원자로보호계통 소프트웨어 구현단계 안전성 분석 보고서, KNICS-RPS-SVR142(Rev.02), 한국원자력연구원, 2008.

[KAERI, 2008d] 한국원자력연구원, 원자로보호계통 소프트웨어 통합단계 안전성 분석 보고서, KNICS-RPS-SVR152(Rev.02), 한국원자력연구원, 2008.

[KAERI, 2008e] 한국원자력연구원, 원자로보호계통 자동시험 및 연계 프로세서 소프트웨어 안전성 분석 보고서, KNICS-RPS-AR111(Rev.01), 한국원자력연구원, 2008.

[Kang et al., 2009] Kang H. G., Lim H. G., Lee H. J., Kim M. C., Jang S. C., Input-profile-based Software Failure Probability Quantification for Safety Signal Generation Systems. Reliability Engineering & System Safety, vol. 94, no. 10, pp. 1542-1546, 2009.

[KEPCO/KHNP, 2015] KEPCO/KHNP, Revised Response to Request for Additional Information, RAI 271-8290, KEPCO/KHNP, 2015.

[KHNP, 2019] 한국수력원자력㈜ 중앙연구원 (2019). 디지털 환경의 인적오류확률 및 안전 소프트웨어 신뢰도 평가(최종보고서), TR-A11NJ10, 한국수력원자력(주).

[KHNP, 2021] 한국수력원자력㈜ 중앙연구원 (2021). 원전 전주기 엔지니어링 고도화를 위한 국산 MMIS 디지털 트윈 개발, 1차년도 중간보고서.

[Kim et al., 2007] Kim M. C., Jang S. C., Ha J., Possibilities and Limitations of Applying Software Reliability Growth Models to Safety-critical Software. Nuclear Engineering and Technology, vol. 39, no. 2, pp. 145-148, 2007.

[KINS, 2014a] 한국원자력안전기술원, 신월성 2호기 운영허가 심사보고서 (초안), 한국원자력안전기술원, 2014.

[KINS, 2014b] 한국원자력안전기술원, 신고리원자력 3호기 운영허가 심사보고서, KINS/AR-1050, 한국원자력안전기술원, 2014.

[KINS, 2019] 한국원자력안전기술원, 신고리원자력 4호기 운영허가 심사보고서, KINS/AR-1140, 한국원자력안전기술원, 2019.

[KINS, 2020] 한국원자력안전기술원, 신한울 원전 1호기 운영허가 심사보고서, 한국원자력안전기술원, 2020.

[Kotonya et al., 1998] Kotonya G., Sommerville I., Requirements Engineering: Process and Techniques, Wiley, 1998.

[Lawford et al., 2012] Lawford M., Wassyng A., Formal Verification of Nuclear Systems: Past, Present and Future, Information & Security An International Journal, 2012.

[Lawrence, 1993] Lawrence J. D., Software Reliability and Safety in Nuclear Reactor Protection Systems, NUREG/CR-6101, UCRL-ID-114839, U.S. Nuclear Regualtory Commission, 1993.

[Lawrence, 1995] Lawrence J. D., Software Safety Hazard Analysis, NUREG/CR-6430, U.S. Nuclear Regulatory Commission, 1995.

[Lee et al., 2020] Lee S. H., Lee S. J., Shin S. M., Lee E.-C, Kang H. G., Exhaustive Testing of Safety-critical Software for Reactor Protection System, Reliability Engineering & System Safety, 193, 106667, 2020.

[Li et al., 2003] Li M., Smidts C., A Ranking of Software Engineering Measures based on Expert Opinion, IEEE Transactions on Software Engineering, vol. 29, no. 9, pp. 811-824, 2003.

[McMillan, 1993] McMillan K. L., Symbolic Model Checking, Kluwer Academic Publishers, 1993.

[McNelles et al., 2017] McNelles P., Zeng Z. C., Renganathan G., Lemoine E., Akl Y., Analysis of Fault-Tolerant Design Methods and Architectures for Digital I&C Systems Using the Dynamic Flowgraph Methodology. The 2nd International Seminar on Probabilistic Methodologies for Nuclear Application, 2017.

[Mehdi et al., 2010] Mehdi H. T., Ali P., Saman, T., HAZOP-study on Heavy Water Research Reactor Primary Cooling System, Annals of Nuclear Energy, vol. 37, no. 3, pp. 428-433, 2010.

[Miller et al., 1992] Miller K. W., Morell L. J., Noonan R. E., Park S. K., Nicol D. M., Murrill B. W., Voas M., Estimating the Probability of Failure when Testing Reveals no Failures. IEEE transactions on Software Engineering, vol. 18, no. 1, pp. 33-43, 1992.

[Moon, 1994] Moon I. Modelling Programmable Logic Controllers for Logic Verification, IEEE Control Systems Magazine, pp. 53-59, 1994.

[OPG, 2018] OPG, 2018. Darlington Safety Report, Part 2 Design Description, NK38-SR-03500-10001 Rev 5, E-DOCS #5733298, Ontario Power Generation.

[Park et al., 2004] Park G. Y., Jang S. C., A Software Reliability Estimation Method to Nuclear Safety Software. Nuclear Engineering and Technology, vol. 46, no. 1, pp. 55-62, 2004.

[Park et al., 2008] Park G.-Y., Koh K. Y., Jee E., Seong P. H., Kwon K.-C., Lee D. H., Fault tree analysis of KNICS RPS software, Nuclear Engineering and Technology, vol. 40, no. 5, pp. 397-408, 2008.

[Park et al., 2014] Park G.-Y., Kim D.-H., Lee D. Y., Software FMEA Analysis for Safety-related Application Software, Annals of Nuclear Energy, vol. 70, pp. 96-102, 2014.

[Parnas et al., 1991] Parnas D., Madey J., Functional Documentation for Computer Systems Engineering, CRL-237, Telecommunications Research Institute of Ontario (TRIO), McMaster University, 1991.

[Parnas et al., 1993] Parnas D., Schouwen Van A. J., Maday J., Documentation of Requirements for Computer Systems, IEEE International Symposium on Requirements Engineering (Re'93), 1993.

[Popovic et al., 1989] Popovic J. R., Hinton G. J. (1989). CANDU Computerized Safety System, Advanced Computer Technology for the Power Industry, Electric Power Research Institute.

[Renganathan et al., 2012] Renganathan G., Gheorghe R., Overview of some challenges in PSA reviews for existing and new nuclear power plants in Canada, E-Doc#3957854, International Atomic Energy Agency, 2012.

[Shin et al., 2017] Shin S. M., Cho J., Jung W., Lee S. J., Test based reliability assessment method for a safety critical software in reactor protection system. Proceedings of the 10th International Topical Meeting on Nuclear Plant Instrumentation, Control & Human Machine Interface Technologies (NPIC & HMIT 2017), San Francisco, CA, June 11-15, 2017.

[Smidts et al., 2000] Smidts C., Li M., Software Engineering Measures for Predicting Software Reliability in Safety Critical Digital Systems, NUREG/GR-0019, U.S. Nuclear Regulatory Commission, 2000.

[Smidts et al., 2004] Smidts C., Li M., Validation of A Methodology for Assessing Software Quality, NUREG/CR-6848, U.S. Nuclear Regulatory

Commission, 2004.

[SNC, 2019] Southern Nuclear Operating Company, ITAAC Closure Notification on Completion of ITAAC 2.5.02.12 [Index Number 5511], ML19354A051, U.S. Nuclear Regulatory Commission, 2019.

[Stamatelatos et al., 2011] Stamatelatos M., Dezfuli H., Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NASA/SP-2011-3421, National Aeronautics and Space Administration, 2011.

[Stringfellow et al., 2002] Stringfellow C., Andrews A. A., An Empirical Method for Selecting Software Reliability Growth Models, Empirical Software Engineering, vol. 7, no. 4, pp. 319-343, 2002

[STUK, 2019a] STUK, Finnish Report on Nuclear Safety, STUK-B 237, Radiation and Nuclear Safety Authority, 2019.

[STUK, 2019b] STUK (2019). Olkiluoto 3 – FSAR Review Report, 43/G42242/2016, Radiation and Nuclear Safety Authority.

[WNPP, 1993] Wolsong NPP 2/3/4, Software Requirements Specification for Shutdown System 2 PDC, Design Document no. 86-68350-SRS-001, 1993.

[WNPP, 1994] Wolsong NPP 2/3/4, Software Verification Report Code Verification, SDS2 PDC, Design Document no. 86-68350-SVR-002, 1994.

[Xu et al., 2013] Xu L., Zhang H., An Improved SFMEA Method Integrated with Assistive Techniques, Software Reliability Engineering Workshops 2013 IEEE International Symposium., 2013.

[Yoo et al., 2005] Yoo J., Kim T., Cha S., Lee J., Son H. S., A Formal Software Requirements Specification Method for Digital Nuclear Plants Protection Systems, Journal of Systems and Software, vol. 74, no. 1, pp. 73-83, 2005.

[Yun et al., 2010] Yun S., Lee D. A., Yoo. J., NuFTA: A CASE Tool for Automatic Software Fault Tree Analysis, 2010 한국원자력학회 춘계학술발표회, 2010.

[김만철 외, 2008] 김만철, Smidts C., 척도-기반 소프트웨어 신뢰도 분석의 예제 소프트웨어에의 적용, KAERI/TR-3594/2008, 한국원자력연구원, 2008.

[김태호 외, 2002] 김태호, 차성덕, PVS를 이용한 SCR 스타일의 소프트웨어 요구사항 명세에서 기능 요구 사항의 정형 검증, 정보과학회논문지: 컴퓨팅의 실제, vol. 8, no. 1, 2002.

[김효정 외, 2005] 김효정, 구철수, 고정수, 김복렬, 윤원영, 오성헌, 최성남, 김대일, 정윤형, 김영미, 이동훈, 지성현, 정출희, 강석철, 김경죠, 김철환, 조원서, 차우창, 디지털 계측제어 안전규제 기술개발, KINS/GR-291, 한국원자력안전기술원, 2005.

[엄흥섭 외, 2010] 엄흥섭, 박기용, 손한성, 강현국, V&V 기반 Bayesian Nets를 이용한 원전 보호계통 안전소프트웨어의 신뢰도 평가 방안, KAERI/TR-4092/2010, 한

국원자력연구원, 2010.

[오해철 외, 2019] 오해철, 이준승, 이은찬, 황석원, 전호준, 최병렬, 김보선, 송우진, 권희곤, 서보선, 김태영, 박진균, 정원대, 장승철, 김승환, 최선영, 김재환, 남지희, 김요찬, 조재현, 신성민, 윤재영, 신승기, 김희은, 디지털 환경의 인적오류 확률 및 안전소프트웨어 신뢰도 평가, Technical Report 2012-50003339-단-0168TR, ㈜한국수력원자력 중앙연구원, 2019.

[윤혜선, 2014] 윤혜선, 미국 원자력규제위원회의 원자력안전규제체계와 시사점 -원자력 발전소에 대한 허가제도와 검사제도를 중심으로-, 일감법학, vol. 2014, no. 27, pp. 3-56, 2014.

[이장수 외, 2003] 이장수, 천세우, 손한성, 차경호, 김장열, 이영준, 권기춘, 소프트웨어 요구명세 안전성 분석을 위한 HAZOP 방안, 2003 한국원자력학회 춘계학술발표회, 2003.

[이종민 외, 2014] 이종민 외, 경수로형 원전 안전심사지침(개정6판) 제3권(7장 ~ 8장), KINS/GE-N001, 한국원자력안전기술원, 2014.

[장승철 외, 2019] 장승철, 김재환, 리스크 정보 활용을 위한 디지털 I&C 계통의 이용불능도 평가 모델 개발, KAERI/TR-7659/2019, 한국원자력연구원, 2019.

[조재명, 2003] 조재명, NuEditor: An Environment for NuSCR Specification and Verification, Masters' Thesis, 건국대학교, 2003.

[지은경 외, 2011] 지은경, 유준범, 이장수, 이영준, 제어기기 FBD 프로그램 테스팅 기법 및 정형 검증기법 기술현황분석 보고서, KAERI/AR-901/2011, 한국원자력연구원, 2011.

[천세우 외, 2005] 천세우, 이장수. 원전에서의 안전-필수 시스템에 대한 소프트웨어 안전성 분석, 2005 한국산업안전학회 학술대회, 2005.

KAERI

KAERI

서지정보양식

KAERI보고서번호	KAERI/TR-8697/2021	보고서 종류	기술보고서
제 목 / 부 제	디지털 I&C 소프트웨어 신뢰도 평가 방법론 및 규제기준/사례 분석		
주저자 및 부서명	이상훈/리스크평가연구실		
공저자 및 부서명	신성민/리스크평가연구실, 장승철/리스크평가연구실, 최종균/자율운전연구실		

출 판 지	대전	발 행 일	2021.8.31	총 페이지	102 p.
공 개 여 부	공개(○), 비공개( )	참 고 사 항	표(3)개, 그림(33)개, 참고문헌(87)개		
비 밀 여 부	대외비( ), __ 급 비밀				

초록 (15-20줄 내외)

본 연구에서는 “원전 디지털 I&C 소프트웨어 신뢰성 평가 규제 방법론 개발” 과제의 당해연도 연구목표인 “국내외 디지털 I&C 소프트웨어 신뢰도 평가 방법론 분석”을 위해 기존 소프트웨어 신뢰도 평가 방법론을 조사하고 국내외 SW 신뢰도 관련 규제기준 및 사례들을 분석하고 국내 규제기술의 개선방향을 제안하였다. 소프트웨어 신뢰도 평가 방법론으로 정성적 (SW HAZOP, SW FMEA, SW FTA, 정형 기법), 정량적 (SRGM, BBN, 척도 기반 기법, CSRM, 시험 기반 기법) 방법론들을 검토하였다. 소프트웨어 관련 국외 규제 기준 및 사례로는 미국 NRC, 캐나다 CNSC, 핀란드 STUK의 기준과 사례들을 검토하였다.

현재 국내 SW 신뢰도 관련 규제기술은 SW 생명주기 공정 품질 평가 등 기존 정성적 신뢰도 검증 분야에 초점이 맞추어져 있으며, 보호계통의 경우 계통 신뢰도에 대한 수용은 정량적인 신뢰도 목표보다 결정론적인 기준에 근거한다. 다만, 원전의 안전기능 수행 및 계통 신뢰성 향상을 위해 KINS/RS-N08.01에 근거하여 IEEE Std. 1012 기준 SIL-4가 요구되는 RPS SW가 IEC 61508과 같은 국제표준에서 제시하는 정량적 신뢰도 목표를 만족하는지 확인할 필요가 있다.

디지털 안전 계통 소프트웨어의 정량적 신뢰도 평가 결과는 리스크 정보를 활용한 디지털 안전 계통 운영기술지침서 감시시험주기 연장 등에도 활용 가능할 것으로 평가되었다. 미국 NRC는 지난 20년간 규제체계에 적합한 SW 신뢰도 평가 방법론을 시도하고 원전 PSA 모델에 반영하려는 노력이 있어왔다. 국내에서도 이러한 국제적 흐름에 맞추어 사업자와 독립적으로 규제자의 측면에서 SW 정량적 신뢰도 평가 방법론을 개발하고 이를 규제에 활용할 수 있는 방안에 대한 모색이 필요하다.

주제명키워드 (10단어내외)	디지털 I&C, 소프트웨어 신뢰도, 소프트웨어 규제

BIBLIOGRAPHIC INFORMATION SHEET

KAERI Report No.	KAERI/TR-8697/2021		Report Type	Technical Report	
Title / Subtitle	Analysis on Digital I&C Software Reliability Assessment Methods and Regulation Standards/Cases				
Main Author and Department	Sang Hun Lee/Risk Assessment Research Team				
Co-Author and Department	Sung-Min Shin/Risk Assessment Research Team, Seung-Cheol Jang (Risk Assessment Research Team), Jong-Gyun Choi (Autonomous Operation Research Team)				
Publication Place	Daejeon	Date of Publication	2021.8.31	Total number of page	102 p.
Open	Open(○), Closed ( )		Reference	Tabs. (3) Figs. (33) Refs. (87)	
Classified	Restricted( ),__Class Document				

Abstract (15-20 Lines)

In this study, the existing software reliability assessment methodology was investigated for the current year's research objective of "Development of Regulatory Methodology for Digital I&C Software Reliability Assessment" and proposed the improvement of domestic and international SW reliability regulation technology. The software reliability assessment methodologies were considered qualitative (SW HAZOP, SW FMEA, SW FTA, formal method), quantitative (SRGM, BBN, Metric-based method, CSRM, and test-based method). For software-related foreign regulatory standards and examples, the standards and examples of U.S. NRC, Canada CNSC, and Finland STUK were reviewed.

Currently, domestic SW reliability-related regulatory technologies focus on existing qualitative reliability verification fields such as SW life cycle process quality evaluation, and acceptance of system reliability is based on deterministic standards rather than quantitative reliability goals. However, it is necessary to ensure that the RPS SW meets the quantitative reliability objectives for SIL-4 based on KINS/RS-N08.01 and international standards such as IEEE Std. 1012, IEC 61508.

Quantitative reliability evaluation results of digital safety system software are estimated to be available for extended monitoring and testing cycles of digital safety system operating technical guidelines using risk information. For the past 20 years, U.S. NRC has been trying to evaluate SW reliability suitable for regulatory systems and reflect it in its nuclear power plant PSA model. In Korea, it is also necessary to develop a SW quantitative reliability evaluation methodology in terms of regulators independently of operators in line with these international trends and find ways to utilize it in regulations.

Subject Keywords (About 10 words)	Digital I&C, Software Reliability, Software Regulation