2025 한국소프트웨어공학 학술대회 (KCSE2025)

안전 중요 분야에서 FPGA 기반 시스템의 확인 및 검증과 위험 분석에 관한 조사 연구

A Survey on V&V and Hazard Analysis of FPGA-Based Systems in Safety-Critical Domain

이영규, 김대원, 허윤아, 유준범
건국대학교 컴퓨터공학과

2025. 01. 21

연구배경 및 목적

안전 중요 시스템

- 시스템이 정상적으로 작동하지 않을 경우, 사람의 생명, 재산, 환경, 사회적 안전에 심각한 영향을 미칠 수 있는 시스템
- 신뢰성, 안전성, 결함 허용, 실시간성을 보장해야 함

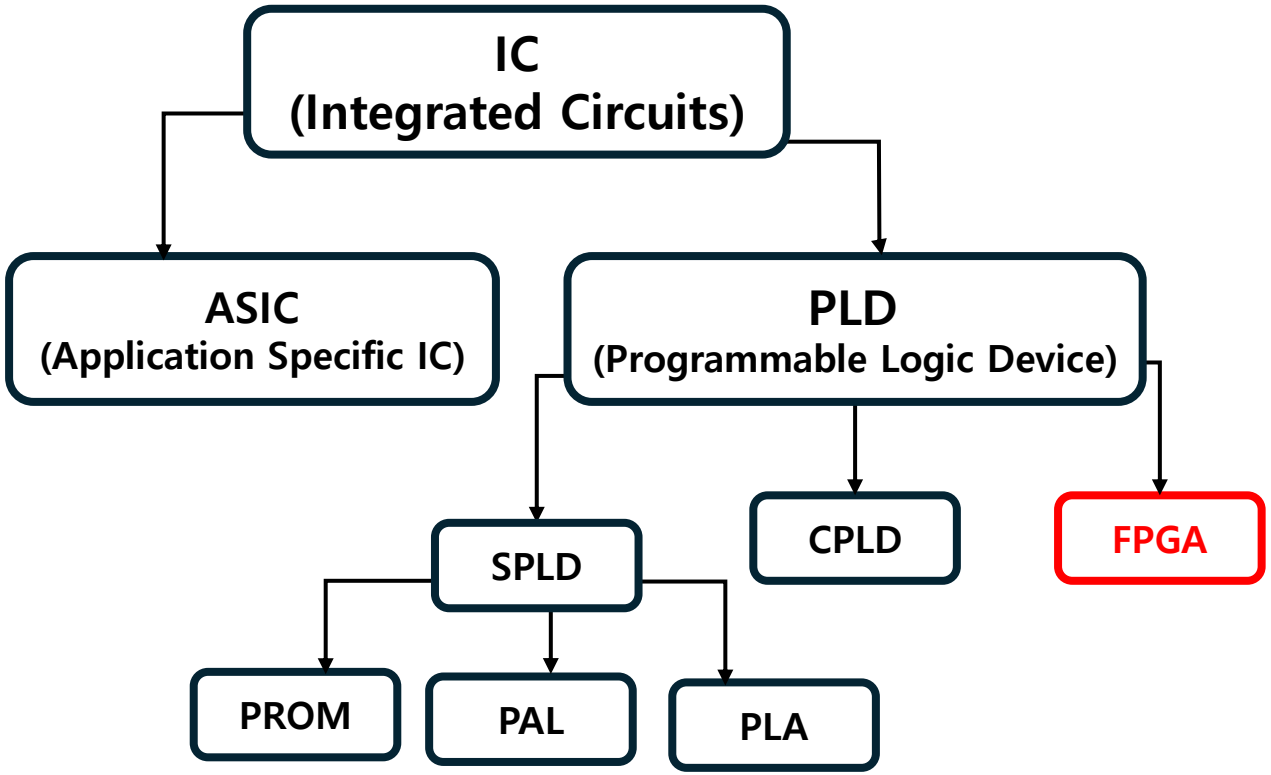
  → 신뢰성과 안전성을 보장하기 위한 검증이 필요함
- 항공, 우주, 의료, 원자력 발전소, 철도 및 대중교통

Field-Programmable Gate Array (FPGA)

- 높은 재구성 가능성, 유연성, 비용 효율성이 특징
- 빠른 프로토타이핑, 짧은 개발 주기가 장점
- 방사선 유발 장애 (Single Event Upset, SEU)
- 결함 허용 기법 (TMR, ECC, Scrubbing)

FPGA

Classification of ICs



Top 4 FPGA Advantages

- Programmability
- Adapatability
- Parallel Task Performance
- Real Time Application

FPGA 활용사례

Marcos S. Farias, et al. [5]

- FPGA 기반 I&C 시스템의 이점과 한계를 설계 지침과 규제를 바탕으로 평가
- 회로설계 기법을 검토해 failure 줄이고 I&C 시스템에 FPGA가 비용 효율적인 옵션이 될 수 있음을 제시

Cinzia Bernardeschi, et al. [7]

- FPGA 기반 시스템이 원자로 보호와 위기 대응 시스템에서 높은 신뢰성과 유연성을 제공함
- IEC 61508 표준에 기반한 V모델 설계 접근법을 사용함
- FMEA 기법을 적용하여 설계 단계에서 잠재적 오류를 식별함

FPGA 활용사례

Jingke She, Jin Jiang [10]

CANDU 원자로의 shutdown 시스템에서 FPGA 기반 시스템이 기존보다 빠르고 안정적으로 작동함을 HIL 테스트와 통계적분석을 통해 입증

Joon-Ku Lee, et al. [12]

HPD 개발 수명주기를 적용, IEC 61513 등 국제 표준에 따라 소프트웨어와 하드웨어의 통합 검증을 수행

원전 계측제어계통에서 FPGA 기반 제어기의 PLC 대체 가능성을 입증

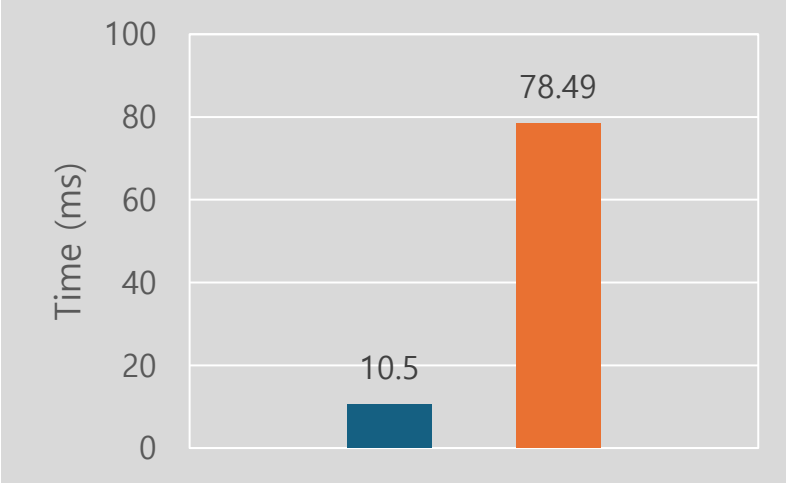


Fig.1 CANDU shutdown 시스템에서 FPGA와 PLC의 성능 반응시간

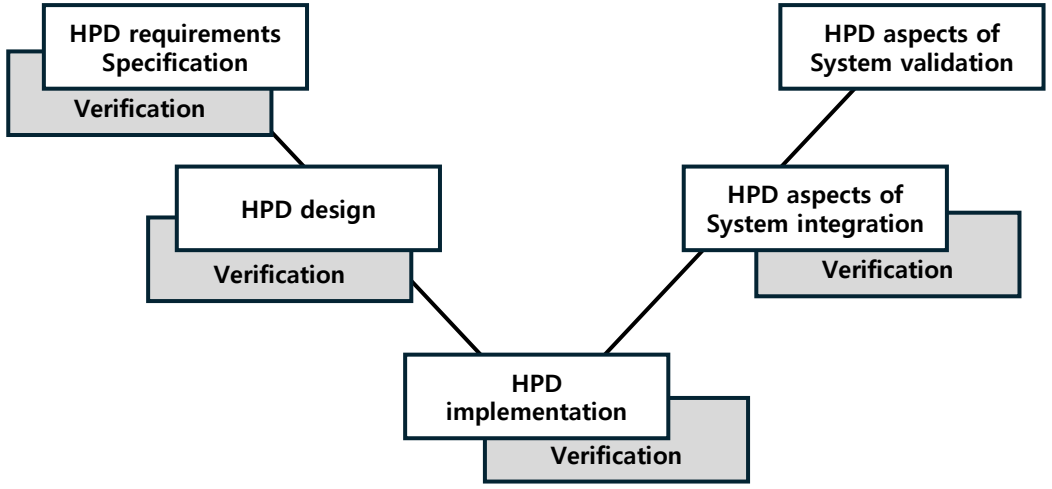


Fig.2 Development life cycle of HPD

FPGA 활용사례

고성능시스템 및 메모리 (9건)

원자력 (8건)

산업 자동화 (4건)

방사선 (4건)

IoT 및 에너지 응용 (4건)

자율주행 (3건)

기타 (3건)

No.	활용 분야						
	원자력 발전소	산업 자동화	방사선 환경	자율주행 및 차량 응용	IoT 및 에너지 응용	고성능시스템 및 메모리	기타
[5]	√						
[6]	√		√				
[7]	√	√	√			√	
[8]	√						
[9]	√		√				
[10]	√					√	
[11]	√						√
[12]	√	√	√			√	
[13]		√				√	√
[14]				√	√		
[15]					√	√	
[16]				√		√	
[17]		√			√	√	
[18]				√		√	√
[19]					√	√	

V&V 기법과 위험분석 적용사례

V&V 분류 항목 | 위험 분석 분류 항목

No.	적용분야	요구사항 검증	설계검증	구현검증	방사선검증	통합검증	시스템 안전성 검증	FTA	FMEA	STPA	MBSE	Formal Methods	HIL	Dynamic Flowgraph
[1]	원자력 발전소 – 설계 검증		√	√			√					√	√	
[24]	계측제어 시스템	√	√	√			√					√		
[25]	원자력 발전소	√	√	√			√					√		
[27]	원자로 보호 시스템		√	√			√					√		√
[28]	오류 진단 시스템	√	√	√										
[29]	자율 시스템		√	√			√					√	√	
[30]	원자로 보호 시스템	√	√				√	√				√		
[31]	디버깅 및 검증		√	√		√								
[32]	원자로 보호 시스템	√	√	√			√					√	√	
[33]	제어 시스템			√			√	√	√			√		√
[34]	설계 자동화	√	√	√		√	√							
[35]	디지털 I&C 시스템		√	√			√			√	√	√	√	
[37]	FPGA SW 테스트	√	√	√			√					√		
[38, 39]	FPGA SW	√	√	√			√					√		
[40]	산업 안전 분석						√	√	√	√		√		
[41]	원자력 I&C 시스템 설계	√	√				√				√	√		
[42]	방사선 환경 FPGA 설계			√	√		√					√	√	
[43]	고장 내성 FPGA 설계		√	√				√	√	√				
[44]	고장 추정 FPGA 분석			√			√	√	√			√		

V&V란?

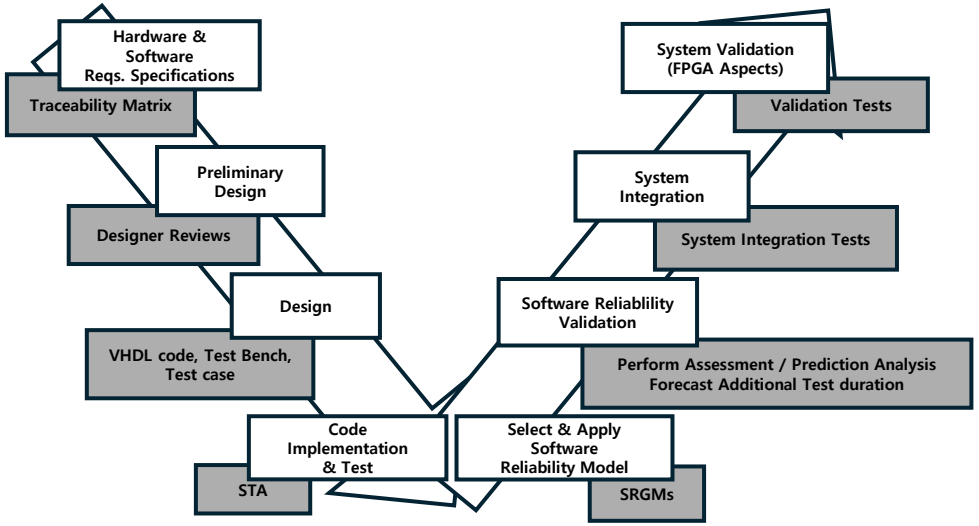
Verification

- 개발 산출물이 주어진 활동의 **요구사항에 부합하는지**를 확인

Validation

- 최종 산출물이 **의도된** 사용 목적과 **사용자 요구를 충족하는지**를 확인

요구사항 정의 > 설계 > 구현 > 신뢰성 측정 > 시스템 통합 > 확인 및 검증



Verification and Validation V-model for software critical safety

V&V 기법 분류 항목

요구사항 검증

- 설계 요구사항 검토로 누락이나 모호성을 식별, 설계 오류 예방

설계 검증

- 설계와 요구사항 일치 여부 검토, 시뮬레이션으로 오류 발견

구현 검증

- 구현이 설계 사양에 부합하는 지 확인, 타이밍 분석과 디버깅 도구 활용

방사선 검증

- 방사선 환경에서 안전성 검증, TMR, PR 기법과 방사선 테스트 수행

통합 검증

- 모든 구성요소 통합 후 요구사항 충족여부 확인

시스템 안전성 검증

- 위험 분석과 시스템 테스트로 위험 식별 및 완화방안 제시

V&V 적용사례

Serhii Naumenko, et al. [1]

정형검증과 시뮬레이션 도구가 설계 오류를 조기에 발견하고, 비용 절감과 설계 복잡성 완화에 기여

Yong Suk Suh, et al. [25]

V&V 활동의 구조화된 단계 (리뷰 > 테스트 > 분석)가 설계 복잡성을 관리하는데 효과적임을 입증

Yoshifumi Narukawa [28]

하드웨어 - 소프트웨어 통합 검증에서 Monte Carlo 시뮬레이션이 효과적임을 보여줌

Ibrahim Ahmed, et al. [30]

모델 기반 설계와 검증이 중복 작업을 줄이고, 통합된 방식으로 효율성을 높임

Yichun Wu, et al. [32]

기존 표준과 지침을 기반하여 다양한 검증 및 시뮬레이션 언어와 도구를 활용해 테스트 다양성 확보

Javier Pérez Fernández, et al. [34]

하드웨어-소프트웨어 통합에서 발생할 수 있는 결함 분석으로 실시간 요구사항 충족과 효율성 증대

Richard Hite, et al. [35]

복잡성을 줄이는 프레임워크가 V&V 효율성을 높이고 설계 가능성을 확장.

Jaeyeob Kim, et al. [37]

통합 테스트 프레임워크가 시간과 비용 절감에 효과적임을 입증.

V&V 기법: 공통 목표

설계 오류의 조기 발견	• 설계 및 구현 과정에서 발생할 수 있는 잠재적인 오류를 초기에 발견. • 정형검증, 시뮬레이션, 자동화도구 (BIST, Co-simulation) 등으로 초기 탐지
신뢰성과 안전성 강화	• V&V와 위험 분석을 통해 설계와 구현이 요구사항을 충족하는지 확인
설계 복잡성 관리	• FPGA는 재구성 가능한 구조, 병렬 처리 특성 등으로 설계 자체가 복잡 • 모델기반설계(MBSE), 계층적 설계 프레임워크(SymPLe)등으로 복잡성을 줄여서 관리하고자 노력
효율성 향상	• 자동화 도구와 모델 기반 접근법으로 테스트 시간 단축, 중복작업 최소화
국제 표준 준수	• IEC 62566, IEEE 1012, IEC 61508 등

위험분석이란?

설계 및 구현단계에서 발생할 수 있는 잠재적 위험 식별, 관리

잠재적 위험의 조기 탐지

- 설계, 구현, 통합 단계에서 발생할 수 있는 위험 요소를 초기에 식별

시스템 신뢰성과 안전성 확보

- 위험 요소를 제거하거나 완화하여 시스템의 안전성 강화

설계 복잡성 관리

- 설계의 복잡성에서 비롯된 오류와 상호작용 문제 분석

위험분석 기법

FTA (Fault Tree Analysis**)**

- 고장의 원인과 가능성을 트리 구조로 분석

FMEA (Failure Mode and Effect Analysis**)**

- 실패 모드와 영향을 식별, 평가하여 설계 개선 및 예방조치 제안

정적 분석
➔ 동적 상호작용 분석에 한계점

위험분석 기법

STPA (Systems-Theoretic Process Analysis**)**

- 제어 구조와 상호작용 분석으로 위험 요소 식별, 안전성 확보

MBSE (Model-Based Systems Engineering**)**

- 모델 기반 설계로 설계 오류 감소, 정형화 모델활용으로 자동화 극대화

Formal Methods

- 수학적 기법으로 설계 명세와 구현의 논리적 오류 검증

HIL (Hardware-in-the-Loop**)**

- 실제 하드웨어와 시뮬레이션 통합으로 실시간 설계, 구현 불일치 검증

Dynamic Flowgraph

- 동적 상호작용과 상태 변화를 그래프로 모델링해 신뢰성과 안전성 분석

위험분석 기법 적용사례

Serhii Naumenko, et al. [1]

설계 초기 단계에서 구문 오류와 요구사항 위반을 탐지하며 설계 복잡성을 줄이고 추가 결함 53건 발견

Satrio Pradana, Jae Cheon Jung [26]

요구사항 정의에서 검증까지의 통합적 위험 관리하며 신뢰성 평가를 위해 SRGM 방법을 적용

Zequn Lin, et al. [27]

FPGA 기반 원자로 보호 시스템에 블랙박스 테스트로 하드웨어와 소프트웨어 상호작용 오류 조기 탐지, 테스트 시간 70% 단축, 진단 정확도 100% 달성

Narukawa Yoshifumi [28]

FPGA 기반 ATLAS 실험 트리거 로직에 Monte Carlo 시뮬레이션 적용하여 다양한 환경에서 트리거 알고리즘의 위험 요소 분석 및 최적화

Jaeyeob Kim, et al. [37]

IST-FPGA와 Co-simulation 기법으로 시뮬레이션과 요구사항 검토를 통합
설계단계에서 위험 평가를 하며 시간과 비용 절감

Philippa Conmy, lain Bate [40]

Top-Down Safety analysis, FPTC를 이용하여 상위 수준 및 구조적 위험 요소를 통합적으로 분석

Fanyu Wang, et al. [41]

I&C 시스템 설계에 FTA와 FMEA를 통합한 MBSE 기반 신뢰성 분석 적용

Jakub Lojda, et al. [44]

FT-EST(Fault Tolerance ESTimation) 프레임워크로 고장 확률 정량 평가, 신뢰성과 고장 영향 분석

기술적 한계

검증 과정의 복잡성과 비용증가

- FPGA는 설계 자유도가 높은 만큼 설계와 검증과정의 복잡성 증가
- 설계 오류의 조기 발견에 필요한 자동화 도구 필요
- 시스템 개발주기가 길어져 실시간 애플리케이션에 적합하지 않을 수 있음

표준화의 부재

- 안전 중요 시스템에 특화된 FPGA 표준

위험 분석 기법의 한계

- 기존 방법으로 FPGA 의 동적 재구성과 하드웨어 수준 병렬처리까지 고려하기 어려움
- 실시간 위험 분석을 위한 도구와 접근법 필요

비트스트림 검증의 어려움

- 디버깅의 어려움
- 설계와 구현의 불일치 검출 도구 필요
- 타이밍 문제 같은 하드웨어 종속 이슈

발전방향

자동화된 설계 및 검증도구 개발

- 계층적 설계를 통해 복잡성 줄이기
- 설계와 검증 간의 상호작용을 간소화하기 위한 통합 프레임워크 도입 필요

산업별 요구를 반영한 설계 표준화

- 표준 준수의 자동화 도구 개발
- 산업별 맞춤형 표준화

FPGA 기반 시스템의 발전 방향성

- 자동화된 디버깅 도구 개발
- 고성능 데이터 처리와 신뢰성 높은 설계로 고효율이 요구되는 산업 진출
- DPR (Dynamic Partial Reconfiguration)
- 시스템 성능 최적화

극한 환경에서의 성능 평가와 실증 연구

- FPGA 특성상 방사선, 고온 같은 극한 환경에서의 작동 평가는 지속적으로 필요함

결론

- FPGA의 높은 신뢰성과 안전성을 보장해주는 특징이 기존의 기술들보다 뛰어나며 안전 중요 시스템에서의 유리한 위치를 잡아가고 있음
- 이에 따른 다양한 연구들을 확인하였고 각 연구에서 FPGA 기반 시스템의 검증의 중요성도 언급하고 있음을 확인
- 사례 분석을 통해 공통적인 V&V와 위험분석 분류 항목을 설명하고 FPGA의 특성을 바탕으로 다양한 기법을 적용한 연구들이 진행되고 있음을 확인
- 또한, 각 사례들에서 공통적으로 말하는 FPGA 기반 시스템 검증의 목표점과 한계점을 살펴보았음
- 제시된 발전 방향을 통해 FPGA 기반 시스템이 안전 중요 시스템에서 핵심 기술로 자리 잡기를 기대함

Q&A

출처

Fig.1 SRAM-Based FPGA Systems for Safety-Critical Applications
Fig.2 On the Speed of Response of an FPGA-Based Shutdown System in CANDU Nuclear Power Plants
Fig.3 Approach Adopted by RPC Radiy for the Verification and Validation of FPGA Based Platforms for Nuclear Safety Applications