원자력발전소의 안전등급 FPGA 확인 및 검증 방법

이동일*

한국수력원자력(주) 중앙연구원

Verification and Verification Method of Safety Class FPGA in Nuclear Power Plant

Dongil Lee*

Korea Hydro and Nuclear Power Central Research Institute

E-mail : diturtle@khnp.co.kr

요 약

원자력 발전소에 사용되는 제어기는 높은 신뢰도를 요구한다. 한국형 디지털 원자력 발전소인 APR1400 (Advanced Power Reactor 1400)을 비롯하여, 과거 많은 원자력 발전소에 FPGA (Field Programmable Gate Array)와 CPLD (Complex Programmable Logic Device, 이하 FPGA로 통칭)가 포함된 제어기가 적용되고 있다. 적용 초기에는 FPGA를 일반적인 IC (Integrated Circuit)처럼 기기검증 및 성능 시험으로만 검증을 하였다. 이후 90년대에 들어 FPGA검증에 대한 연구가 시작되면서, FPGA가 칩이 되기 전까지를 소프트웨어로 간주하여 IEEE 1012-2004를 적용하여 소프트웨어 확인 및 검증을 하였다. 현재에는 유럽표준인 IEC 62566을 적용하여 많은 검증을 하고 있다. 이 방법은 현재까지 가장 현명한 방법으로 평가 받고 있다. 이유는 기존의 검증 방법에서 문제가 되었던 SoC (System on Chip)의 특징을 검증하는 방법을 충분히 적용하였기 때문이다. 하지만, IEC 62566은 유럽 표준으로 아직 미국에서는 채택을 하지 않고 있으며, FPGA에 대해서는 IEEE 1012를 적용하는 것을 유지하고 있다. IEEE 1012-2004나 IEC 62566은 기술 표준으로 실무에서는 다양한 방법을 적용하여 기술 표준을 충족시켜서 적용하고 있다. 이 논문에서는 SoC의 검증 방법이 적용된 원자력 안전등급 FPGA에 대한 검증 방법의 절차 및 중요사항에 대해 설명하고자 한다.

ABSTRACT

Controllers used in nuclear power plants require high reliability. A controller including a Field Programmable Gate Array (FPGA) and a Complex Programmable Logic Device (referred to hereinafter as FPGA) has been applied to many Nuclear Power Plants (NPP) in the past, including the APR1400 (Advanced Power Reactor 1400), a Korean digital nuclear power plant. Initially, the FPGA was considered as a general IC (Integrated Circuit) and verified only by device verification and performance testing. In the 1990s, research on FPGA verification began, and until the FPGA became a chip, it was regarded as software and the software Verification and Validation (V&V) using IEEE 1012-2004 was implemented. Currently, IEC 62566, which is a European standard, has been applied for a lot of verification. This method has been evaluated as the most sensible method to date. This is because the method of verifying the characteristics of SoC (System on Chip), which has been a problem in the existing verification method, is sufficiently applied. However, IEC 62566 is a European standard that has not yet been adopted in the United States and maintains the application of IEEE 1012 for FPGA. IEEE 1012-2004 or IEC 62566 is a technical standard. In practice, various methods are applied to meet technical standards. In this paper, we describe the procedure and important points of verification method of Nuclear Safety Class FPGA applying SoC verification method.

키워드

FPGA, V&V, NPP, V-model

* Corresponding author

Ⅰ. 서 론

원자력 발전소는 안전을 최우선으로 설비들이 구성된다. 그렇기 때문에 사용되는 제어기는 높은 신뢰도를 요구한다. 또한, 제어기의 구성이 대부분 디지털화 되었고 FPGA는 제어기의 대부분에 포함되어 있다.

FPGA를 적용 초기에는 전자부품으로 간주하여 기기검증 및 성능시험으로만 검증을 하였다. 90년대부터는 FPGA가 칩이 되기 전까지를 소프트웨어로 간주하여 IEEE 1012-2004를 적용하여 소프트웨어 확인 및 검증(V&V, Verification and Validation)을 하였다.

미국을 제외한 한국을 포함한 여러 국가들은 현재 IEC 62566을 적용하여 많은 검증을 하고 있다. 기존의 검증 방법에 문제가 되었던 SoC의 특징을 충분히 반영한 표준으로 판단되기 때문이다.

이 논문에서는 IEEE 1012-2004와 IEC 62566 기술 표준을 충족시키는 방법을 제시하고자 한다.

Ⅱ. 소프트웨어 V&V

원자력분야에서 사용되는 소프트웨어 V&V 방법은 IEEE 1012-2004 표준을 만족하기 위해, 폭포수 모델에서 신뢰도를 강화한 V-모델을 기반으로 수행한다.

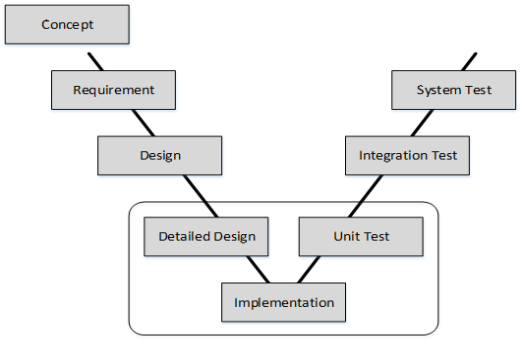

그림 1. 소프트웨어 검증 모델(V-모델)

소프트웨어 V&V는 그림 1과 같이 검증(Verification) 단계로 개념단계, 요건단계, 설계단계, 구현단계를 수행하고 확인(Validation)단계로 단위, 통합 시스템 시험을 수행한다[1,2].

소프트웨어 V&V는 원자력 안전등급과 중요성에 따라 소프트웨어 무결성 등급(SIL, Software Integrity Level)이 나누어지고, 등급에 따라 소프트웨어 V&V 수행의 강도와 절차가 구체화 된다. 소프트웨어 V&V는 각 단계별로 보고서가 생성된다.

V-모델의 단점은 폭포수모델이 가지고 있는 상위 단계의 수행이 완전히 완료되어야만 하는 단점을 가지고 있다. 이는 상위단계의 수행이 정상적으로 완료가 되지 않고 이후단계를 수행하게 된다면 상위단계부터 하위단계까지 모두 재 수행을 해야 하는 단점을 가지고 있다.

Ⅲ. FPGA의 소프트웨어 V&V

소프트웨어 V&V에 사용되는 IEEE 1012-2004를 기반으로 FPGA를 검증하게 된 것은 미국 원자력 발전소에 FPGA 기반의 제어기를 적용하기 위해 검증하는 기준이 필요했기 때문이다.

FPGA는 Schematic 설계를 제외하고는 모두 HDL(Hardware Description Language)로 설계를 한다. HDL은 하드웨어적 특성을 구현한 부분을 제외하고는 소프트웨어적 특성을 가지고 있어 소프트웨어 V&V를 수행하기에 적합하다는 판단이었다.

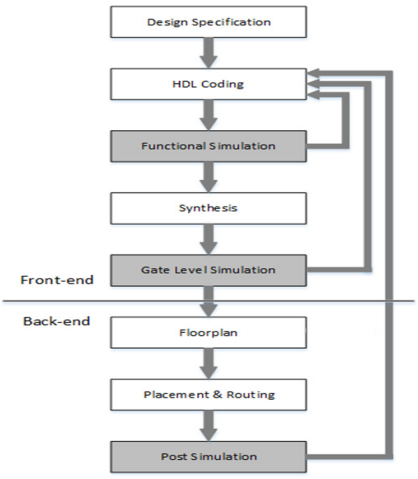

그림 2. 일반적 FPGA 개발 및 검증 모델

그림 2는 일반적인 FPGA 개발 및 검증 모델로 전형적인 폭포수 모델과 유사한 형태를 가지고 있다. 하지만 소프트웨어 V&V에서 사용되는 폭포수 모델 및 V-모델은 검증단계에서는 개발의 절차를 검증을 하고 확인 단계에서 요구사항에 부합되게 개발이 완료 되었는지를 확인 하는 시험과정을 가진다.

하지만 FPGA 개발 및 검증 모델은 개발 단계 사이에 확인단계의 시뮬레이션(시험) 단계가 포함되어있다. 이러한 모델의 차이는 소프트웨어 V&V의 V-모델을 적용하여 FPGA를 검증함에 있어서 오류를 발생시킨다.

즉, V-모델은 설계가 완료된 시점에서 시험을 시작하지만 FPGA는 설계를 하는 과정에서 시험을 수행하여야 한다. 이러한 차이점은 시험단계와 설계, 요건단계의 수행이 혼합되는 문제를 가지게 된다.

Ⅳ. IEC 62566과 FPGA 검증

IEC 62566은 유럽표준으로 원자력 안전등급에 사용되는 FPGA의 검증 방법에 대해 기술한 표준이다. 한국과 세계 여러 나라가 이 표준을 수용하고 수행 중에 있다.

간략히 요약을 하면 그림 3과 같이 앞서 설명된 V-모델(그림 1)의 구현단계에 FPGA 설계 및 검증 모델(그림 2)이 포함된 형태이다.

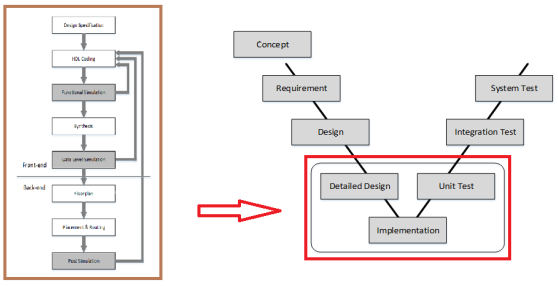

그림 3. IEC 62566의 검증 모델 간략화

FPGA 설계 및 검증모델은 하드웨어적 특성을 고려하고 있는데 이러한 특성까지를 설계 및 구현 관점으로 바라본 것이다.

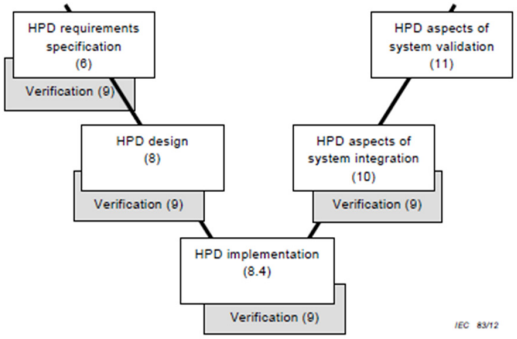

그림 4. IEC 62566의 V-모델

그림 4는 IEC 62566에서 제시한 V-모델이다. 그림 3의 과정을 요약한 것이라 볼 수 있다 [4].

IEC 62566에는 많은 내용이 기술되어 있는데 그 중 핵심적인 내용은 하드웨어적 요소이다. IEEE 1012-2004에서 포함하지 못했던 요소들이다.

FPGA의 특성 중 가장 중요한 Timing적 요소, RTL구현의 동일성, 100% 시험사례 등과 재 사용성에 대해 상세히 작성이 되어 있으며, 현재 세계 여러 국가 및 한국의 원자력 분야에서는 적극적으로 수용하고 있다.

간단히 요약을 하면 FPGA 설계에 있어서 가장 중요한 부분인 타이밍요소는 최악과 최고의 Timing에 대한 시험을 적극적으로 수행한다. 그림 2에서 설명된 기능시험과 타이밍시험이 반드시 수행되고 검증된다.

그리고 HDL의 문법과 기능에 대해서는 IEEE 1012-2004에서도 충분히 검증이 되지만 RTL이라는 하드웨어적 변환에 대한 동일성을 검증하게 된다. 단순히 소프트웨어로 검증을 하지 않는다는 것이다.

마지막으로 Core IP(Intellectual property)에 대한 사용에 대해 규정을 지어 재사용성에 대해서는 안전등급 품질 등급을 가진 제조사에서 제조한 동일 FPGA와 동일 Core IP를 사용 하였을 때만 가능한 것으로 간주 하였다. 즉, 재사용이 거의 불가능한 형태이다.

현재 한국에서는 FPGA를 검증하기 위해서 IEC 62566을 수용한 규제지침이 개발되어 있으며, 이를 적극 수용하여 검증을 수행하고 있다.

Ⅴ. 결 론

원자력 분야에서는 FPGA 검증을 하기 위해 많은 시간을 투자 해왔다. 이유는 안전이 우선되었기 때문이다. 물론 지금도 안전이 가장 중요하다. IEEE 1012-2004에서 FPGA의 특성을 모두 수용하기 힘들었으나, IEC 62566의 표준이 적극 수용되어 FPGA검증보다 견고해졌다.

특히 V&V의 절차가 구현단계에 FPGA 검증이 포함되어 설계절차의 혼란이 없어 졌다. 또한, FPGA의 핵심인 Timing 분석 및 시험, RTL 검증, 재사용성에 대한 규정을 규정하여 검증을 수행함에 따라 FPGA의 신뢰도가 보다 높아 졌다.

현재 원자력 분야에서는 IEC 62566의 표준을 따라 검증하는 것이 가장 합리적이고 정확한 검증 방법이다.

References

[1] IEEE 1012, “Software Verification and Validation”, p.10, 2004

[2] IEEE 1012, “Software Verification and Validation”, Annex B, 2004

[3] 홍성제 외5명, ”테스팅 및 테스팅을 고려한 설계”, 홍릉과학출판사, 1998

[4] IEC 62566, “Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions”, p16, 2012