원자로 제어시스템 FPGA 개발에 사용되는 상용 합성도구의 COTS 인증

건국대학교 ▌정세진·김의섭·유준범*

1. 서 론

원자력발전소의 디지털 계측제어 시스템(I&C : Instrumentation and Controller)은 원자로의 감시 및 제어, 보호 기능을 수행하는 최상위 수준의 안전필수 시스템(Safety Critical System)이다[1]. 현재 디지털 I&C 시스템은 PLC(Programmable Logic Controller)기반 제어기로 동작되고 있지만, PLC 제품의 부품단종 및 기술지원의 어려움에 의한 유지보수비용의 증가[2] 그리고 PLC 만으로 해결하기 어려운 다양성 및 심층방어를 위한 수단으로써[3] 최근 FPGA(Field-Programmable Gate Array)기반 제어기가 주목받고 있다[4,5]. 하지만 아직까지 국내 I&C 시스템에 FPGA를 사용한 이력이 없고 인증 역시 받은 적 없어 FPGA를 사용하는데 안전성과 신뢰성 측면이 문제가 되고 있다. 따라서 FPGA로 구현된 제어기가 안전기능을 충분히 수행할 것이라는 것을 합리적으로 보증하기 위한 상용 제품 인증(COTS Dedication)이 필요한 상황이다[6,7,8].

국내 법령 KINS/RG-N17.12[9] “안전성관련품목 대체사용을 위한 일반규격품의 품질검증”에 따르면 새로운 시스템을 대체 사용하기 위해서는 EPRI(미국 전력연구원) NP-5652[7]와 TR-106439[8]를 채택하여 상용 제품 인증을 해야 한다고 명시하고 있다. NP-5652는 일반규격품(CGI: Commercial Grade Item - 원전의 안전성을 고려하지 않고 설계 및 제작된 제품)을 포함한 모든 부품에 적용되는 일반론적인 절차를 규정하고 있어, 전통적인 기계・전기・계측 부품에는 적용이 용이하나, 소프트웨어가 탑재된 디지털기기에는 적용이 어려운 반면 TR-106439는 디지털기기에 대한 일반규격품 품질검증 절차를 규정하고 있어 FPGA의 상용 제품 인증에 적용하기에 적합하다[10].

FPGA의 개발 프로세스를 살펴보면 기술적으로 다양한 상용 도구들이 사용되는 것을 확인할 수 있다. 예를 들면 RTL 단계의 HDL 코드를 게이트 레벨의 Netlist로 변환해 주는 합성 도구나 Netlist를 layout하는 P&R(Place and Route) 도구들이 사용된다. 해당 도구들은 원자력 발전소의 제품을 개발하기위해 개발된 제품 즉 원자력품질보증(NQA: Nuclear Quality Assurance) 프로그램 하에서 생산되지 않은 품목이기 때문에 상용 제품 인증이 필요하다. 하지만 해당 도구들 같이 개발에 사용되는 지원 도구에 대해서 NP-5652과 TR-106439 두 표준 모두 고려하고 있지 않다. FPGA로 개발된 완제품에 대해 하드웨어/소프트웨어적으로 기능검증 및 품질검증을 수행하는 것도 중요하겠지만, 개발에 사용된 소프트웨어를 검증하는 것 역시 원전의 신뢰성과 안전성, 건전성을 위해 매우 중요하다. 항상 소프트웨어에는 다만 밝혀지지 않았을 뿐 언제나 버그를 가지고 있을 수 있기 때문이다.

본 논문은 FPGA 개발에 사용되는 개발 지원 도구인 사용 합성 도구의 상용 제품 인증에 기여할 수 있는 방법을 제시한다. 특히 NP-5652과 TR-106439 표준의 특별 시험 및 검사(Special Test and Inspection) 중 성능 특성(Performance Characteristic)을 검증 할 수 있는 방법을 제시한다. 성능 특성을 확인하기 위한 특별 시험에서는 상용 합성 도구의 기능성(Functionality) 및 정확성(Correctness)을 확인해야 하는데, 상용 합성 도구의 소스 코드 및 내부 구조 미공개 이유로 직접적인 검증 방법[11,12]의 적용이 어렵다. 따라서 이를 위해 간접적으로 상용 합성 도구를

* 정회원

† 본 연구는 한국원자력연구원의 “FPGA-기반 제어기 통합개발환경을 위한 핵심 소프트웨어 기술 개발” 사업과 “원자력 계측제어 계통 안전 적합성 평가체계” 사업의 지원으로 연구한 결과입니다.

검증 할 수 있는 방법인 동치성 검사 방법[13]을 제안한다. 이를 통해 상용 합성 도구의 필수 특성(Critical Characteristics)을 확보하는데 기여할 수 있을 것으로 기대하고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 FPGA 개발 프로세스 및 개발에 사용되는 도구들에 대해 설명하고, 3장에서는 원자력 도메인의 상용 소프트웨어 인증에 대한 표준을 설명한다. 4장에서는 표준을 바탕으로 특별 시험을 수행할 수 있는 방법을 제시하며, 5장에서 결론을 맺는다.

2. FPGA 개발 과정

그림 1은 일반적인 FPGA 개발 과정을 보여주고 있다. 가운데 라인은 개발과 관련된 활동들이 적혀 있고, 왼쪽과 오른쪽 라인은 각 개발 단계에서 수행할 수 있는 V&V 활동들이 적혀 있다. 모든 프로그램이 그렇듯이 FPGA를 개발하기 위해서도 제일 먼저 해야 할 작업은 개발하고자하는 시스템의 분석을 통한 요구사항을 도출하고 정리하여 문서화 하는 작업이다. 다음으로 작성한 요구사항을 바탕으로 HDL(Hardware Description Language)을 이용해 RTL 수준의 프로그램을 코딩한다. 가장 많이 사용되는 HDL 언어로는 Verilog[14]와 VHDL [15]이 있다. 만약 HDL Designer[16] 이나 SCADE[17]와 같이 상위 수준의 모델링 도구를 사용하다면 모델로부터 바로 HDL 코드를 얻을 수도 있다. RTL 단계에서는 ModelSim[18]과 같은 시뮬레이션도구를 통해 작성한 HDL 코드의 기능을 확인해 볼 수 있다

사용자에 의해 작성된 HDL은 각 칩 제조업체에서 제공하는 라이브러리와 사용자의 타이밍 제약조건을 바탕으로 합성 도구에 의해 게이트 레벨의 Netlist로 변환된다. 게이트 레벨이란 CMOS회로의 NAND, AND, 인버터, 플립플롭 등의 각종 게이트로 구성되는 것을 말하며, 여기서 게이트들은 아직 물리적인 매핑이 되지 않은 단순 게이트들과 게이트들의 연결을 나타낸다. 합성과정은 사용자가 직접 해야 고려해야 되는 칩의 속도와 전력 등의 부분을 고려하여 자동으로 최적화된 결과를 제공한다. 따라서 사용자는 최적화와 같은 복잡한 고려 없이 오로지 기능 구현 및 설계에 집중하여 칩 개발이 가능해진 장점이 있다. 하지만 합성 도구는 사용자가 설계 및 작성한 HDL 구조의 정형성을 변환 및 최적화 수행을 통하여 깨뜨린다. 단점이 존재한다. 정형성이 깨지더라도 동일한 기능을 한다면 문제가 되지 않지만 합성 도구도 소프트웨어인

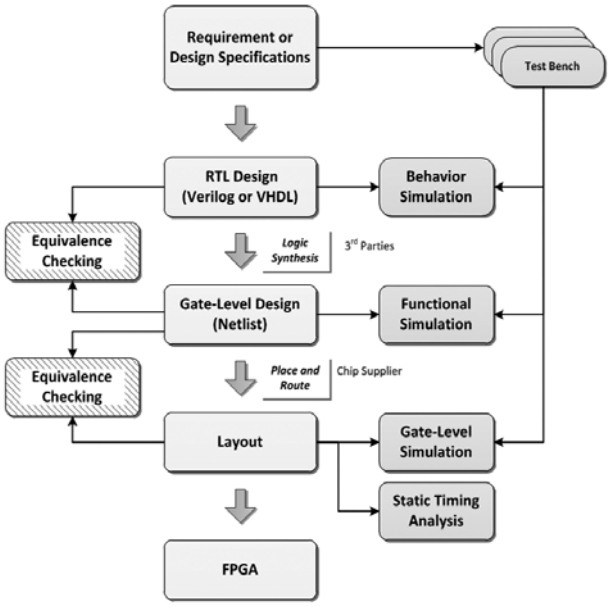

그림 1 FPGA 개발 과정

만큼 버그가 존재할 수 있기에 신뢰성의 의문을 가질 수 있다. 일반적으로 실제 산업계에서는 문제없이 동일하게 변환을 한다고 알려져 있지만 원자력발전소 같이 안전이 최우선시 되는 시스템에 사용하기 위해서는 검증을 통한 인증이 반드시 필요하다. 합성에 사용 가능한 상용 합성 도구들로는 대표적으로 'Synopsys Synplify Pro'[19], 'Precision RTL'[20], 'Encounter RTL Compiler'[21] 등이 있다.

합성으로 인해 의도하지 않은 버그나 에러가 생기지 않았는지 또는 사용자가 의도한 기능이 정상적으로 동작하는지 확인할 필요가 있다. 이를 위해 해당 단계에서는 RTL 단계에서 시뮬레이션을 위해 수행한 테스트 벤치를 다시 이용해 시뮬레이션을 하여 동일한 결과를 출력하는지 확인하는 작업을 통해 검증해 볼 수 있다. 또한, RTL 단계의 HDL과 게이트레벨의 Netlist가 동일한 기능을 수행하는지 시뮬레이션 이외에 동치성 검사(Equivalence Checking)를 이용해 검증해 볼 수 있다. 동치성 검사는 서로 다른 두 프로그램이 동일한지 가능한 모든 입력 조합을 이용해 수학적으로 검증하는 방법이다. 현재 상용으로 사용 가능한 검증 도구로는 대표적으로 'FormalPro' [22], 'Encounter Conformal EC' [23], 'Formality' [24], 'VIS' [25] 등이 있다. 하지만 해당 도구들이 모든 상황에서 동작하지 않는다는 문제점이 있다. 각 검증 도구들은 특정 IDE 환경에서 특정 합성 도구를 사용하였을 경우에만 검증이 가능하도록 되어있다. 따라서 사용자는 검증하고자하는 IDE와 합성 도구의 조합을 확인

하여 사용가능한 검증 도구를 선택하거나 개발해 사용해야 한다.

마지막으로 합성 결과물은 배선 및 배치(Place & Route) 도구를 거쳐 레이아웃 형태로 변환된다. 이 과정은 게이트 레벨 디자인을 실제 FPGA에 사용 될 수 있도록 매핑 시키는 과정이다. 게이트 레벨의 Netlist 정보를 받아 쎌(Cell)들을 배치(Place)하고 쎌과 쎌 사이를 와이어를 이용해 연결(Route)한다. 이 단계에서도 역시 P&R이 잘 동작하였는지 시뮬레이션을 통해 확인할 수 있다. 특히 이 단계에서는 타이밍 분석(STA: Static Timing Analysis)[26]을 통해 IC에서 발생할 수 있는 타이밍 관련 문제를 사전에 처리해주게 된다. STA는 실제 수행 없이 회로의 지연시간을 계산하여 위배되는 상황이 없는지 확인하게 된다. 최종적으로 레이아웃 형태로 변환된 결과물은 FPGA 하드웨어에 업로드 되어 사용 되게 된다.

3. 원자력 분야의 상용 제품(소프트웨어) 인증 표준

원자력 발전소의 디지털 계측제어 같이 안전계통에 상용 제품을 상용하기 위해서는 표준을 바탕으로 상용 제품 인증 과정을 수행하여 제품의 품질 보증이 이루어져야 한다. 국내에서는 법령 KINS/RG-N17.12 ”안전성관련품목 대체사용을 위한 일반규격품의 품질검증“에서 시스템을 대체 사용하기 위해서는 EPRI NP-5652와 TR-106439를 채택하여 상용 제품 인증을 해야 한다고 명시하고 있다. NP-5652은 일반규격품을 포함한 모든 부품에 적용되는 일반론적인 절차를 규정하고 있고 TR-106439 에서는 디지털기기에 대한 일반규격품 품질검증 절차를 규정하고 있다. 하지만 두 표준 모두 안전계통에 직접적으로 사용되는 제품에 대해서만 고려하고 있고 상용 합성 도구와 같이 개발에 사용 되는 간접 사용 도구에 대해서는 고려하고 있지 않다. EPRI 표준과 NRC(미국원자력규제위원회)는 표준 NUREG/CR-6421을 통해 원자력 발전소의 안전계통에 사용되는 제품을 개발하는 간접 사용 소프트웨어에 대해서도 표준을 정하고 가이드 해주고 있다. 3장에서는 해당 표준들에 대해 설명한다.

3.1 NP-5652/TR-106439

NP-5652과 TR-106439는 EPRI(미국전력연구원)에서 제안한 상용 제품 인증 과정에 대한 표준이다. TR-106439은 NP-5652를 바탕으로 디지털기기에 대한 내용을 추가한 표준이다. 여기서 상용 제품이란 일반규격품(Commercial Grade Item)은 원전의 안전성을 고려하지 않고 설계 및 제작된 제품으로 원자력품질보증(NQA: Nuclear Quality Assurance) 프로그램 하에서 설계 및 제작, 성능검증을 거치지 않고 생산된 제품을 말한다. 따라서 이 제품들이 원자력 발전소의 안전계통에 사용되기 위해서는 상용 제품 인증이 필요하다. 이를 위해 NP-5652에서는 먼저 상용 제품이 안전 기능을 수행하기 위해 가져야 하는 필수 특성을 식별하고 이를 검증하기 위해 4 가지 인증 방법제시, 해당 인증 방법을 조합하여 수행하는 것을 제시하고 있다.

그림 2는 NP-5652의 인증 과정에 대한 그림이다. 먼저 사용하려는 제품이 일반 규격품인지 확인하고, 안전기능을 수행하는지 확인한다. 그 다음 해당 제품이 안전기능을 수행하는지 기본 기기(Basic Item - 원자력발전소의 안전계통에 사용될 목적으로 안전등급 및 규격에 따라 생산된 기본 품목)인지 확인한다. 만약 안전기능을 수행하지 않거나 안전등급 및 규격에 따라 생산된 품목이라면 기본 기기로 사용한다. 반면 기본 기기가 아닌 일반 규격품이고 안전기능을 수행할 것으로 평가되었으면 상용 제품 인증을 수행한다.

인증하려는 제품을 선정한 후에는 제품의 필수 특성(Critical Characteristics)을 확인한다. 필수 특성은 상용 제품/소프트웨어가 안전기능을 수행하기 위해 필수적으로 가져야 하는 특성으로 물리적 특성(Physical Characteristic), 성능 특성(Performance Characteristic), 신뢰성 특성(Dependability Characteristic)으로 구분되어진다. 물리적 특성은 제품의 크기, 기계적인 구조와 같이 하드웨어적인 특성을 의미한다. 특히 TR-106439은 하드웨어적인 특성 이외에 소프트웨어 및 기기의 버전, 성능 요건 등을 포함하고 있다. 성능 특성은 안전기능 수행에 필요한 기능 필수특성과 제품의 고유 설계 필수특성이 있고, 이를 입증하기 위해서는 기능 항목 및 정확도에 대한 신뢰수준 및 환경적인 영향에서 건전성을 확인한다. 신뢰성 특성은 하드웨어적으로는 고장 발생 확률 또는 수명을 의미하며 소프트웨어적으로는 마모와 같은 하드웨어적인 특성이 없어 설계와 불일치등을 예로 들 수 있다.

인증을 위한 4 가지 방법에는 4 가지가 있다(표 1). (Method.1) 특별 시험은 소프트웨어, 제품의 기능 및 정확성 등을 직접 시험하여 평가하는 방법으로 설치 후 시험 방식까지 포함되어 있다. 특히, 소프트웨어에 대해서는 주로 성능 특성을 증명하기 위해 사용된다.

(Method 2.) 공급자 조사는 상용 소프트웨어를 제공하는 공급자의 품질 보증 체계를 확인하는 방법으로 공급자의 품질 보증 체계 인증을 통해 제품의 품질을 인증하는 방법이다. (Method 3.) 소스 검증은 소스 확인 또는 제작 중 입회 검사를 통해 수행하는 방식으로 제품의 경우 제작 공정 확인 등이 포함된 방법이다. (Method 4.) 사용이력 조사는 인증하려는 제품에 대해 기존의 인증 과정이나, 사용 이력 등을 조사하고 확인하는 방법이다.

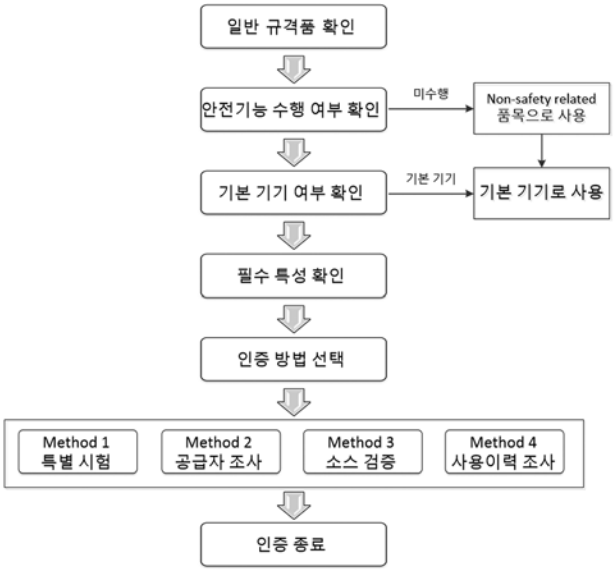

그림 2 NP-5652 인증 과정

표 1 NP-5652의 인증 평가 방법

Method	Title
1	Special test and inspection
2	Commercial grade survey of supplier
3	Source verification
4	Acceptable supplier/item performance record

3.2 NUREG/CR-6421

NUREG/CR-6421은 U.S.NRC(미국원자력규제위원회)에서 제안한 원자력 분야의 상용 소프트웨어 인증 과정에 대한 표준 이다. NUREG/CR-6421의 특징은 완제품뿐만 아니라 제품을 개발하는데 사용되는 간접 사용 소프트웨어까지도 고려하고 있다는 점이다. 이를 위해 NUREG/CR-6421은 상용 제품이 담당하게 될 안전기능의 등급(안전 카테고리)과 제품이 사용되는 방법(직접 대체 사용, 개발에 간접 사용)의 등급을 통해 새로운 등급을 도출하고 이를 통해 인증 절차를 다르게 하여 인증을 수행할 것을 명시하고 있다.

그림 3은 NUREG/CR-6421의 인증 과정에 대한 그림으로, 먼저 시스템의 안전성 및 위험성 분석을 통해 안전기능들을 식별해 놓는다. 그다음 대체 사용하고자 하는 상용 소프트웨어가 어떤 안전기능을 수행하는지 확인한다. 이를 바탕으로 상용 소프트웨어의 안전 카테고리를 분류한다. 안전 카테고리는 IEC 61226[1]을 바탕으로 분류한다. IEC 61226을 따르는 안전 기능의 카테고리는 A, B, C, Unrelated가 존재하며 가장 안전성이 중요한 시스템이 A 카테고리로 분류 된다.

최종 인증 수준 및 과정을 결정하기 위한 상용 소프트웨어의 안전 카테고리는 분류된 안전 카테고리와 상용 소프트웨어의 사용 카테고리를 이용하여 결정한다. 표 1은 상용 소프트웨어의 사용 카테고리와 사용 카테고리별로 분류되어지는 최종 카테고리에 대한 표이다. 사용 카테고리는 직접 사용과 간접사용, 지원 용도, 미 연관으로 총 4 가지가 존재한다. 사용 카테고리별로 상용 제품이 담당한 안전 기능의 카테고리에 따라 최종 안전 카테고리가 분류된다. 마

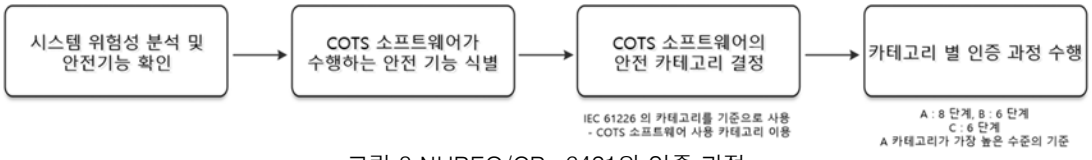

그림 3 NUREG/CR-6421의 인증 과정

표 2 COTS 소프트웨어 사용 카테고리 및 분류

COTS 사용 카테고리	상세 설명	IEC 61226 카테고리
직접 사용 (Direct)	A, B, C 안전 카테고리의 안전 기능에 직접적으로 사용	A, B, C
간접 사용 (Indirect)	A, B, C 카테고리의 모듈을 생성 (예, 컴파일러, 링커 등)	A, B, C, unclassified
지원 용도 (Support)	지원 시스템, 간접 사용 이외의A, B, C 카테고리 시스템 개발을 지원	unclassified
미 연관 (Unrelated)	A, B, C 카테고리의 안전 기능에 영향을 미치지 않음	unclassified

지막으로 최종 분류된 안전 카테고리에 따라 표준에서 제시하고 있는 절차를 수행하여 인증 과정을 진행할 수 있다.

4. 상용 합성 도구의 원자력 분야 인증을 위한 방법

상용 합성 도구는 RTL 레벨의 HDL 코드를 게이트 레벨의 최적화된 Netlist로 변환해주는 도구이다. 변환을 하면서 IC의 면적 및 연산 최적화를 수행하는 도구로 사용자가 직접 해야 하는 복잡한 과정을 대신해서 자동으로 수행해 주는 도구이다. 이를 통해 사용자는 IC의 면적 및 연산의 최적화등과 같은 복잡한 고려 없이 프로그램의 기능 구현 및 설계에 집중할 수 있게 된다.

하지만 문제는 상용 합성 도구가 변환을 하면서 개발자가 설계한 HDL의 정형성을 최적화를 통해 깨뜨리게 된다는 점이 있다. 일반적으로 산업계에서는 좋은 결과를 낸다고 하지만, 원자력 분야같이 안전성이 최 우선시되는 시스템에 사용하기 위해서는 상용 제품 인증을 통해 안전성 및 신뢰성, 강건성 등을 확보할 필요가 있다. 특히 상용 합성 도구를 이용해 안전 기능을 수행하는 원자로 보호 계통이나 공학 안전 설비 등의 제품을 개발할 경우 개발에 사용된 상용 합성 도구의 상용 제품 인증은 개발된 완 제품의 상용 제품 인증에 기여할 것이다.

본 장에서는 NP-5652과 TR-106439 표준의 특별 시험 및 검사(Special Test and Inspection) 중 성능 특성(Performance Characteristic)을 수행을 위해 동치성 검사의 필요성에 대해 설명한다. 또한 기존 상용 동치성 검사 도구들의 제한적인 사용성에 대해서도 소개한다. 그림 4 는 FPGA 개발 프로세스 내 본 논문에서 타겟으로 삼고 있는 상용 합성 도구와 검증 방법의 모습을 보여준다.

4.1 상용 합성 도구의 인증을 위해 제안하는 방법

상용 합성 도구는 안전 기능을 수행하는 원자로 보호 계통이나 공학 안전 설비 등의 제품 개발을 위한 간접 사용 소프트웨어로 분류 할 수 있다. 따라서 상용 합성 도구의 상용 제품 인증을 위해서는 성능 특성 및 신뢰성 특성 검증을 통해 인증을 해야 한다. 확인해야 될 합성 도구의 성능 특성으로는 기능성(Functionality) 및 정확성(Correctness)으로 볼 수 있다. 여기서 상용 합성 도구의 정확성은 합성 도구가 모든 RTL 레벨의 HDL 코드를 기능적으로 일치하는 게이트 레벨의 Netlist를 변환하는가를 통해 볼 수 있다. 이를 위한 인증 방법으로는 (Method 1.) 특별 시험을 수행할 수 있다.

하지만 상용 합성 도구는 영리적으로 사용되는 소프트웨어로써 내부 소스 코드 및 소프트웨어의 구조가 공식적으로 오픈되어 있지 않아 직접적인 검증을 통해 기능성 및 정확성을 확인하기 어려운 상황이다. 따라서 간접적인 검증 방법을 통해서라도 합성 도구의 정확성 및 기능성을 반드시 확인할 필요가 있다. 이를 위해 사용할 수 있는 방법으로 동치성 검사(Equivalence Checking)가 있다. 동치성 검사는 서로 다른 두 프로그램이 동일한지 가능한 모든 입력 조합을 이용해 수학적으로 검증하는 방법이다. 현재 상용으로 사용가능한 검증 도구로는 대표적으로 'FormalPro', 'Encounter Conformal EC', 'Formality', 'VIS' 등이 있다. 하지만 위에 나열한 동치성 검사 도구가 모든 합성 도구를 검증할 수 있지 않고 특정 합성 도구와 특정 개발 환경(IDE: Integrated Development Environment) 에서만 검증을 지원하고 있다. 따라서 사용자의 개발 환경과 합성 도구에 따라 동치성 검증 도구를 선택 및 필요하다면 커스터마이즈된 검증 도구를 개발해야 한다. 기존 상용 검증 도구들에 대한 자세한 내용은 4.2장에서 다루어진다.

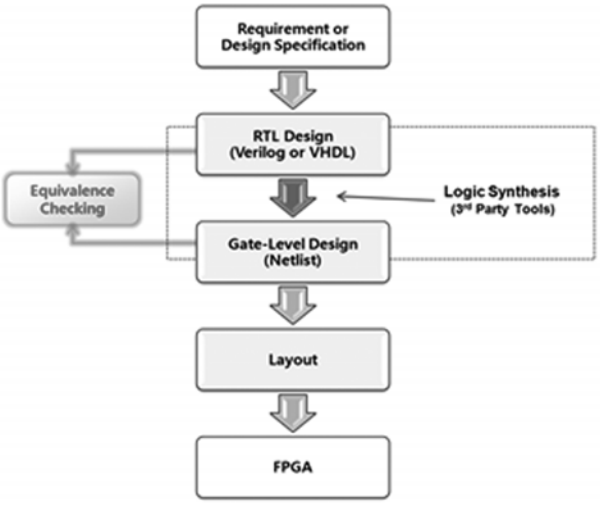

그림 4 상용 합성 도구와 검증 방법

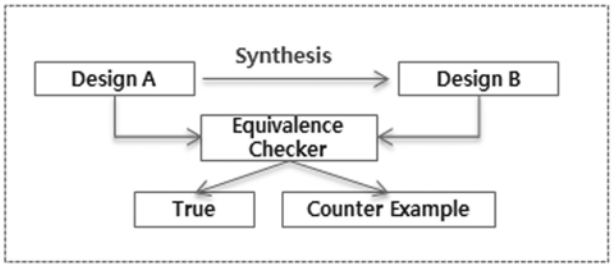

그림 5 동치성 검사 개요

그림 5는 동치성 검사 개요에 대한 그림으로, 두 대상의 동일성에 대해 수학적으로 확인하는 방법이다. 합성 도구에 대해서는 특정 입력과 입력에 대한 출력이 항상 같은 행동을 하는지 검사하는 방법으로, 동치성 검사를 통해 합성 도구의 정확성 및 기능성 간접적으로 검증 할 수 있다. 합성 도구의 입력과 출력이 수학적/논리적으로 동일하다면, 대상 입력에 대해서 합성이 올바르게 수행되었음을 간접적으로 확인 할 수 있다. 그림 5의 그림을 보면 Design A가 입력 RTL 코드(Verilog 또는 VHDL)이고, Design B는 합성 결과물인 게이트 레벨의 Netlist 이다.

4.2 상용 동치성 검사 도구

표 3은 기존 상용 동치성 검사 도구들을 보여주고 있는 표이다. FormalPro, Formality, Encounter Conformal EC, VIS 등 표에 나타난 바와 같이 RTL 레벨의 디자인과 합성 결과물의 동치성 검사를 제공하는 도구들이 다수 존재한다. 일반적으로 상용 합성 도구들은 FPGA 공급회사(ex, Microsemi, XILINX, ALTERA)에 따라 제공되는 IDE (Integrated Development Environment)와 조합되어 제공 및 사용 되게 되는데 공급회사 별로 각각 지원하고 있는 합성 도구가 다르다.

한계점은 동치성 검증 도구 역시 특정 합성 도구와 특정 IDE 조합만 지원한다는 것이다. 예를 들어 표 4에 나타난 바와 같이 Mentor Graphics사의 FormalPro는 자회사의 Precision RTL이 Xilinx사의 ISE [27] 환경에서 합성이 되었을 경우 검증을 지원한다. 또한 Actel사의 Libero SoC [28] 환경에서 합성이 되었을 경우 동치성 검사를 지원하고 있다. 하지만 Altera사의 Quartus 2 [29] 환경에서 Synopsys사의 Synplify Pro를 이용하여 합성을 하였을 경우 동치성 검사를 지원하고 있지 않다. 특히, Actel Libero SoC 환경에서 Synplify Pro로 합성을 수행하였을 경우 지원하고 있는 동치성 검증 도구가 없는 상황이다. 동치성 검증 도구가 모든 환경과 합성도구를 지원하고 있지 않은 이유는 다음과 같다. 동치성 검사를 하기위해 상용 동치성 검사 도구들이 보다 빠른 속도를 위해 합성에서 사용된 라이브러리와 합성 중에 생성된 입출력 및 내부 레지스터 정보를 참조하여 검사를 진행하기 때문이다. 따라서 검사를 하기 위해서는 라이브러리와 합성 과정에 대한 정보가 필요한데 이는 업무제휴를 맺은 업체에게만 제공되고 있어 다양한 상황에서의 검증이 이루어지지 않고 있다. 만약, 상용 합성 도구의 상용 제품 인증을 위해 동치성 검사 방법을 사용하고자 한다면 사용자는 자신의 개발 환경과 합성 도구를 검증할 수 있는 동치성 검사 환경을 구축 및 개발할 필요가 있다.

표 3 상용 동치성 검사 도구

제조 회사	도구 이름
Mentor Graphics	FormalPro
Synopsys	Formality
Cadence	Encounter Conformal EC
Cadence	Jasper Gold
Magma Design Automation	Quartz Formal
OneSpin Solutions	360 EC
VIS	VIS Working Group

5. 결론 및 향후 연구

FPGA 개발에는 합성 도구를 포함한 여러 상용 도구들이 사용되고 있다. 이를 원자력 발전소에 사용하기 위해서는 상용 제품 인증이 필요하다. 본 논문에서는 원자력 분야의 상용 제품 인증 표준인 NP-5652과 TR-106439, NUREG/CR-6421에 대해 소개하였고, NP-5652과 TR-106439 표준의 특별 시험 및 검사(Special Test and Inspection) 중 성능 특성(Performance Characteristic)을 검증하기 위한 방법으로 동치성 검사의 사용을 제

표 4 상용 동치성 검사 도구별 대상 비교

합성 도구	IDE	Mentor Graphics FormalPro	Cadence Encounter Conformal EC	Synopsys Formality
Mentor Graphics Precision RTL	Xilinx ISE	O		
	Actel Libero SoC	O		
Synopsys Synplify Pro	Xilinx ISE	O	O	
	Actel Libero SoC	How to ?		
	Altera Quartus 2		O	
Xilinx XST	Xilinx ISE		O	O
Synopsys DC Ultra				O

시하였다. 제시한 방법인 동치성 검사는 상용 합성 도구가 비공개라는 점에서 매우 효과적일 것이라 평가할 수 있고, 이를 통해 상용 합성 도구의 필수 특성(Critical Characteristics)을 확인하는데 충분한 기여할 수 있을 것으로 기대하고 있다. 동치성 검사를 위해 현재 상용적으로 사용 가능한 도구들이 많이 존재한다. 하지만 각 도구들은 특정 개발 환경 및 합성 도구의 조합에 따라 지원 여부가 다르다. 때문에 사용자는 자신의 개발 환경과 합성 도구에 맞는 검증 환경을 선택 및 개발해야 할 것이다.

앞으로 우리는 현재 지원되고 있지 않은 개발환경과 합성도구의 조합에 대해 동치성 검사를 수행할 수 있도록 검증 환경을 구축할 계획이며, 본 논문에서 제시한 방법을 바탕으로 실제 상용 합성 도구의 상용 제품 인증 과정을 수행 할 예정이다.

참고문헌

[1] International Electrotechnical Commission, IEC 61226, "Nuclear Power Pllants - Instrumentation And Control Systems Important For Safety - Classification," 1994.

[2] 이준구, 정광일, 박근옥, 손광영, “HPD 개발수명주기를 적용한 원전 FPGA 기반 제어기의 설계와 검증,” 한국전자통신학회 논문지, Vol. 9, No. 5, 2014.

[3] Jong Gyun Choi, Dong Young Lee, "Development of RPS Trip Logic Based on PLD Technology," Nuclear Engineering and Technology, vol. 44, no. 6, pp.697-708, 2012.

[4] Junbeom Yoo, Jong-Hoon Lee and Jang-Soo Lee, "A Research on Seamless Platform Change of Reactor Protection System from PLC to FPGA," Nuclear Engineering and Technology, Vol. 45, No.4, pp.477-488, 2013.

[5] J. She, “Investigation on the benefits of safety margin improvement in CANDU nuclear power plant using an FPGA-based shutdown system,” Ph.D. dissertation, The University of Western Ontario, 2012.

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

[7] Electric Power Research Institute, "Plant Engineering : Guidelines for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications," 2013.

[8] Electric Power Research Institute, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," 1996

[9] KINS, "KINS/RG-N17.12," http://scale.kins.re.kr/service/main/main.do

[10] 배창호, 이동희, 김규로, 장중순, “원전용 디지털 인디케이터의 검증 규정 EPRI TR-106439 에 관한 고찰,” Vol. 15, No.4, pp. 248-255, 2014.

[11] T. Hoare, "The verifying compiler: A grand challenge for computing research," Journal of the ACM, Vol.50, No.1, pp.63-69, 2003.

[12] Leroy X. “Formal Verification of a Realistic Compiler,” Communication of the ACM 2000, Vol. 52, No.7, pp.107-115, 2000.

[13] Huang SY, Cheng KT. Fromal Equivalence Checking and Design Debugging, chap. 4. Kliwer Academic Publishers, 1998.

[14] Institute of Electrical and Electronics Engineers, “IEEE Standard Verilog Hardware Description Language,” 2001.

[15] Institute of Electrical and Electronics Engineers, “IEEE Standard VHDL Language Reference Manual,” 2008.

[16] Mentor Graphics Corporation, “HDL Designer SeriesTM User Manual,” Tech. Rep., 2008.

[17] Esterel Technologies, www.esterel-technologies.com/products/scade -suite/, 2007

[18] Mentor Graphics, “ModelSim,” http://www.mentor.com/products/fv /modelsim/.

[19] Synopsys, "Synopsys synplify pro," http://www.synopsys.com/Tools/.

[20] Mentor Graphics, "Precision RTL," http://www.mentor.com/products /fpga/synthesis/precision_rtl/.

[21] Cadence, "Encounter RTL Compiler," http://www.cadence/products/ld /rtl_compiler/pages/default.aspx/.

[22] Mentor Graphics, “FormalPro,” http://www.mentor.com/products/fv /formalpro/.

[23] Cadence, “Encounter Conformal LEC,” http://www.cadence.com/products/ld/equivalence

[24] Synopsys, “Formality,” http://www.synopsys.com/tools/verification /formalequivalence/pages/formality.aspx/.

[25] Brayton RK, Hachtel GD, Sangiovanni-Vincentelli A, Somenzi F, Aziz A, Cheng ST, Edwards SA, Khatri SP, Kukimoto Y, Pardo A, et al.. VIS : A system for verification and synthesis. the Eighth International Conference on Computer Aided Verification, CAV ’96, 1996; 428 – 432.

[26] Wikipedia, “Static timing analysis,” https://en.wikipedia.org/wiki /Static_timing_analysis
[27] Xilinx. Xilinx ise design suite. http://www.xilinx.com/products/.
[28] Actel, "Actel libero ide," http://www.actel.com/products/software/.
[29] Altera. Altera quartus ii. http://www.altera.com/products/software/.

약 력

정 세 진

2015 건국대학교 컴퓨터공학부 졸업(학사)
2015~현재 건국대학교 컴퓨터 정보통신공학부 석사과정
관심분야: 소프트웨어 공학, 상용 소프트웨어 인증
Email: jsjj0728@konkuk.ac.kr

김 의 섭

2012 건국대학교 컴퓨터공학부 졸업(학사)
2015 건국대학교 컴퓨터 정보통신공학부 졸업(석사)
2015～현재 건국대학교 컴퓨터 정보통신공학부 박사과정
관심분야: 소프트웨어 공학, 정형기법
Email: atang34@konkuk.ac.kr

유 준 범

2005 KAIST 전자전산학과 전산학전공 졸업(박사)
2008 삼성전자주식회사 통신연구소 책임연구원
2008～현재 건국대학교 컴퓨터공학부 부교수
관심분야: 소프트웨어 공학, 안전성 분석, 정형기법
Email: jbyoo@konkuk.ac.kr