COTS SW DEDICATION

Introduction

Jsjj0728@konkuk.ac.kr

내용

1.0 Commercial-Grade Item Dedication

1.1 소개

CGI (Commercial-Grade Item) dedication 은 원자력 발전소에 상용 기성 제품들을 사용하기 위한 applicable acceptance process 이다.CGI dedication 은 1970 년대 이후 새 원전 건설 중단 (US)으로 인해 부품 제공 업체들의 NQA (Nuclear Quality Assurance) 인증 및 Q 등급 제품 유지 포기, 그리고 10CFR Part 50 Appendix B [2]에 소개된 Quality assurance requirements 하에 개발된 제품들의 감소로 인해 안전성이 확보된 제품 수급이 어려워 짐으로 인해 대두되었다.

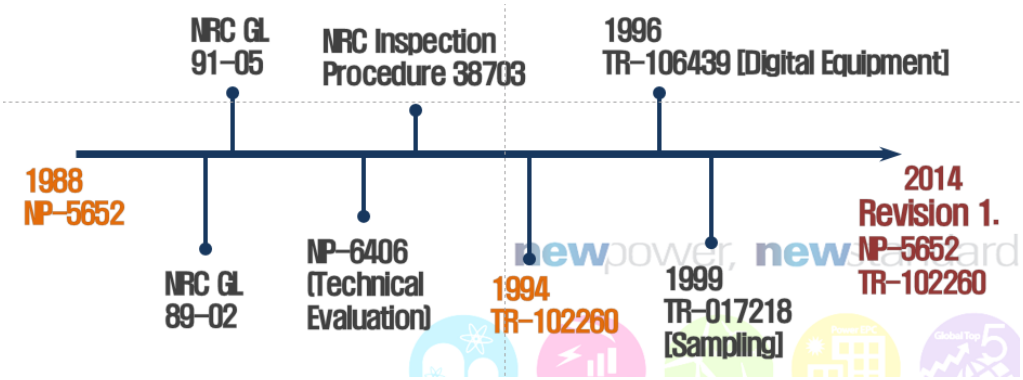

Figure 1 CGI dedication 표준 발행 순서 [1]

<Figure 1>은 CGI dedication 을 위해 발행된 technical report 및 표준, regulatory 등의 발행 순서를 간략하게 표시한 그림이다.1988 년 EPRINP-5652 [3]를 시작으로 하여 여러 technicalreport 및 표준들이 발행 되었다.NP-5652 는 "Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications" 으로,원자력 발전소에 직접 사용되는 하드웨어 및 기계/전기적 장비들에 대한 표준으로 2014 년 개정 되었다.TR-102260 [4] 은 NP-5652 를 보충 설명하는 가이드라인으로 2014 년 개정판이 발행 되며 NP-5652 에 포함 되었다.그 외에 1996 년 디지털 장비들이 원자력 발전소에 많이 사용되며 디지털 장비들에

대해 dedication 을 위한 TR-106439[5] 가 제정 되었고,Sampling guideline (TR-017218) [6] 등이 있다.

이외에도 NP-6406 [7], TR-1008256[8]은 NP-5652 의 process 중 앞부분인 technical evaluation 을 설명하기 위한 표준들 이다.또한 원자력 발전소에 혹은 개발에 소프트웨어들이 사용되며 나온 NUREG/CR-6421 [9]과 같은 가이드라인과 TR-1025243[10]과 같은 리포트들이 있다.특히 최근에 원자력 발전소에 FPGA 를 이용하는 연구가 활발히 진행 되며 FPGA 개발에 사용되는 소프트웨어들의 dedication 에 대한 이슈가 발생 되었다.국내에서는 CGI dedication 에 대해 "*KINS/RG-N17.12: 안전성관련품목 대체사용을 위한 일반규격품의 품질검증*"을 통해 NP-5652 와 TR-106439 를 채택하여 사용하고 있다.

2.0 용어 정리 및 약어

2.1 용어 정리

공학적안전설비 작동계통 (ESFAS : Engineered Safety Features Actuation System)
원자력발전소가 정상적인 운전 상태에서 벗어날 때,발전소를 안전한 상태로 유지시키고 비정상 상황을 빨리 종결시키기 위해 설치되는 설비

안전성(Safety)
사망, 재해, 질병, 시설 또는 재산의 손해나 파손, 또는 환경파괴를 일으킬 수 있는 상황이 발생하지 않는 정도

완전성 (Completeness)
소프트웨어가 요구하는 모든 기능을 제공하는가에 대한 소프트웨어 설계 결과물의 특성. 요구하는 소프트웨어의 기능은 일반기능요건과 전체계통

설계상에서 소프트웨어에 할당되는 기능 요건에 의해 도출됨

일관성 (Consistency)
소프트웨어 시스템의 문서나 구성요소 사이에 모순이 없는가에 대한 정도. 내부 일관성은 하나의 구성요소내의 서로 다른 부분 사이에 모순이 없는 정도. 외부 일관성은 구성 요소와 구성 요소 사이에 모순이 없는 정도

필수 특성 (Critical Characteristics)
일반규격품목이 안전기능을 수행하기 위해 필수적으로 보유해야 하는 특성

일반 규격품 (Commercial Grade Item)
기본기기로 설계 및 제작되지 않았지만, 안전기능에 영향을 끼치는 구조물, 계통, 기기 또는 그 부품

정확성(Correctness)
시스템이나 기기가 그 명세서, 설계 및 구현에 있어서 결함이 없는 정도 혹은 소프트웨어, 설계 문서 또는 다른 항목들이 규정된 요구사항을 만족하는 정도 이다

기본 기기 (Basic Component)
10CFR50 Appendix B를 만족하는 품질보증 프로그램을 준수하여 설계, 제작된 품목 또는 dedication 과정을 성공적으로 완료한 일반 규격 품목 (10CFR21)

품질 검증 (Dedication)
기본기기로 사용을 위해 일반규격품목을 기술평가 및 적합성 확인과정을 통하여 안전성 관련 품목으로 사용할 수 있도록 확인하는 과정

안전 기능 (Safety Function)

IEC-61508 표준에 따라 안전 기능은 원자력 발전소에서 발생 할 수 있는 위험한 상황들로부터 발전소를 보호하기 위한 기능들을 의미

안전 필수 설계 (Safety-Critical Design)

DO-254, ISO 26262, IEC 61508 등 기능안전 관련 표준을 만족하고 performance, safety, security 부분에서 설계 목적을 위해 타협 없이 제작된 설계

RTL Design

Hardware register와 논리 계산 circuit간의 신호 흐름을 연결하여 모델로 디자인한 digital circuit design

Gate-Level Design (Netlist)

RTL Design의 Synthesis 결과를 의미하며, 하드웨어에 사용 될 수 있도록 연결 관계를 표현한 디자인

EDIF (Electronic Design Interface Format)

EDIF는 Electronic Design Interface Format의 약자로 각 회사별로 사용되는 Gate-Level Design(netlist)의 형식이다.

BLIF-MV

비 결정적 hierarchical sequential system을 디자인하기 위한 언어로 VIS에서 이용된다

PLC (Programmable Logic Controller)

여러 로직의 기능을 마이크로프로세서를 이용한 프로그램으로 제어될 수 있게 통합시킨 장치. 프로그램 가능한 메모리를 사용하고 프로세서를 제어하는 디지털 전자 장치이다.

FBD (Function Block Diagram)
FBD는 IEC 61131 표준 Part 3에 정의된 언어로 함수 블록들의 연결을 통해 표현한 그래픽 언어이다.

상용 소프트웨어 (COTS Software)
일반규격품들 중에서 소프트웨어를 칭한다.

테스트벤치 (Test Bench)
디자인 또는 모델의 correctness, soundness를 증명하기 위해 사용되는 가상의 환경

합성 (Synthesis)
상위 수준의 하드웨어 기술 언어를 보다 낮은 수준으로 변환하는 과정

2.2 약어

CGI	Commercial Grade Item
COTS	Commercial-Off-the-Shelf
EDIF	Electronic Design Interface Format
EPRI	Electric Power Research Institute
FBD	Function Block Diagram
FPGA	Field Programmable Gate Array
HDL	Hardware Description Language
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
NRC	Nuclear Regulatory Commission
PLC	Programmable Logic Controller
RTL	Register-Translator-Level
RTM	Requirement Traceability Matrix

SRE	Software Requirement Evaluation
SRS	Software Requirements Specification
SQA	Software Quality Assurance
TA	Traceability Analysis
V&V	Verification and Validation

3.0 NP-5652/TR-106439 개요

NP-5622, EPRI TR-106439는 EPRI에서 제안한 표준으로원전에 사용되는 일반규격품 (CGI : Commercial-Grade Item) 의dedication 에 대한 내용을 포함하고 있다. EPRI NP-5652는 주로 기계적/전기적 하드웨어에 관련된 일반규격품을 대상으로 하고, EPRI TR-106439는 하드웨어뿐만 아니라 하드웨어에 직접 사용되는 소프트웨어까지 대상으로 한다.

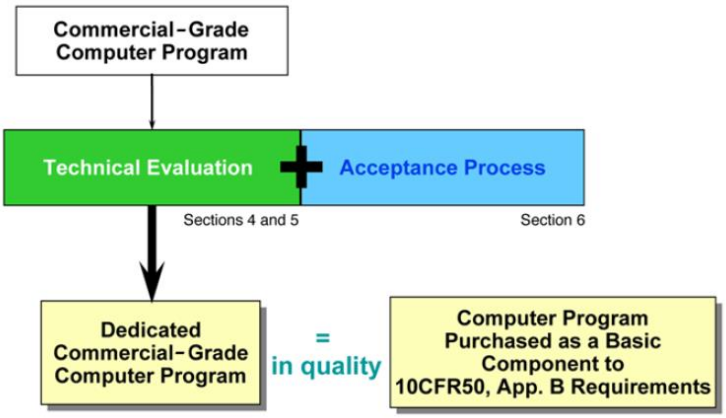

Figure 2. Commercial-grade item(computer program) dedication 개요[1]

<Figure 2>은 TR-1025243 및 NP-5652 의 commercial-item dedication 에 대한 개요이다. Commercialitem(SW)는 Technical Evaluation 과 Acceptance Process 로 구성된 두 가지 과정을 거쳐 dedication 되며 최종적으로 dedication 된 결과물은 원자력 발전소의 quality 요구사항인 10CFR50 App. B requirements 를 만족하도록 제작된 기본기기(basic component)와 동등한 자격을 가진다.

3.1 NP-5652 의 인증 방법

NP-5652 의 dedication 과정은일반규격품이 안전기능을 수행하기 위해 가져야 하는 필수 특성 식별과,필수 특성에 따른 인증 방법 선택 및 진행 과정으로 구성 되어 있다.<Figure 3>는 NP-5652 의 dedication process 로, 인증 과정을 크게 Technical Evaluation 과 Acceptance 2 부분으로 나누고 있다.

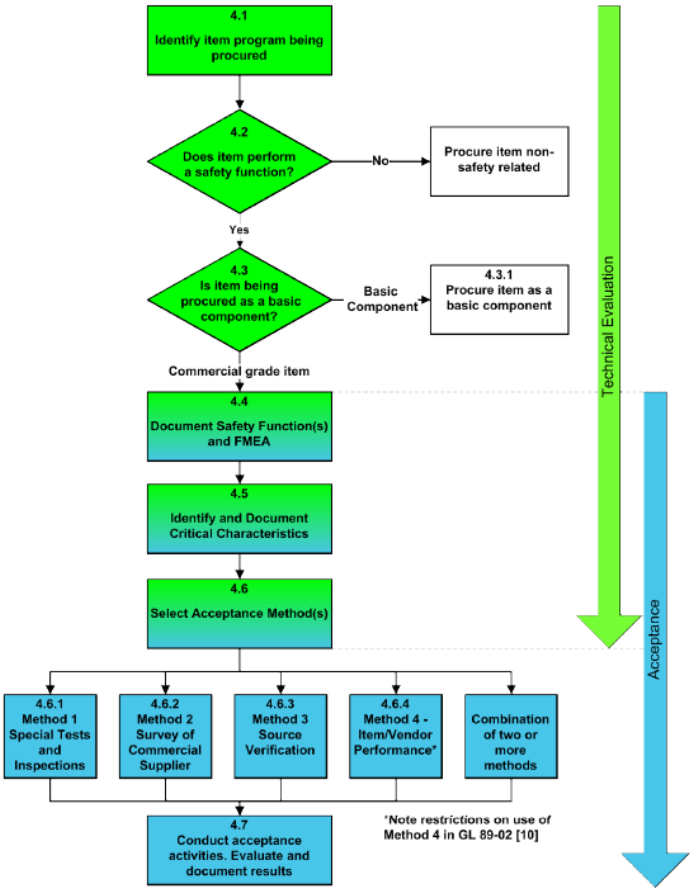

Figure 3 NP-5652 의 dedication process

Technical Evaluation 은 일반규격품의 특성 확인 및 인증 방법을 선택하는 전반부를 구성하며 Acceptance 는 인증 방법을 선택하고 인증을 진행하는 후반부를 구성하고 있다.

NP-5652 의 dedication 과정은사용하려는 제품 확인부터 시작한다.일반규격품의 안전 기능 수행 여부 확인과, 이미 인증된 기본 기기의 여부를 확인하는 작업을 거

친다.사용하려는 일반규격품이 원자력 발전소의 안전기능을 수행하지 않는다면 비안전성 등급으로 별도의 인증 과정 없이 사용 한다.또한 사용하려는 품목이 이미 dedication 과정을 거친 품목 이거나,원자력 발전소에 사용을 위한 여러 certification 을 받은 기본 기기의 경우 dedication 과정을 거치지 않고 사용 한다.NP-5652 의 dedication 은 안전 기능을 수행하지만 인증되지 않은 일반 규격품만을 대상으로 한다.사용하려는 일반 규격품이 dedication 의 대상이라면 다음 과정으로는 품목의 필수 특성을 확인한다.

필수 특성은 일반규격품이 안전 기능을 수행하기 위해 반드시 포함해야 하는 특성을 포함한 제품의 특성이다.필수 특성에는 물리적 특성 (Physical Characteristics), 성능 특성 (Performance Characteristics)과 TR-106439 에서 제안한 Dependability Characteristics 이 있다.물리적 특성은 제품의 물리적,장치적 특징에 대한 특성이고, 성능 특성은 제품의 기능적인 부분에 대한 특성이다.
Dependability characteristic 은 장비 내부의 소프트웨어가 가지는 특성들에 대한 내용으로 소프트웨어의 built-in quality, configuration control 등 소프트웨어의 개발 프로세스 및 품질 보증 체계까지 확인하는 내용이 포함된다.

4.0 NUREG/CR-6421 개요

NUREG/CR-6421은 NRC(Nuclear Regulatory Commission) 에서 제안한 표준으로서 상용소프트웨어(COTS SW) 인증 과정에 대해 설명하고 있다.NUREG/CR-6421은 원자력발전소의 소프트웨어 품질관련 표준 및 Regulatory Guide를 기반으로 작성 되었다. NUREG/CR-6421은 COTS 소프트웨어가 수행하는 안전기능을 바탕으로 소프트웨어의 안전 카테고리를 분류하고, 분류한 카테고리 별로 적용되어야 하는 인증 과정 및 수준에 대해 설명하고 있다. 안전기능을 바탕으로 한 소프트웨어의 안전 카테고리는 IEC 61226 표준에 따라 A, B, C, unclassified로 분류되며 A 카테고리가 안전 등급이 가장 중요한 카테고리 이다.

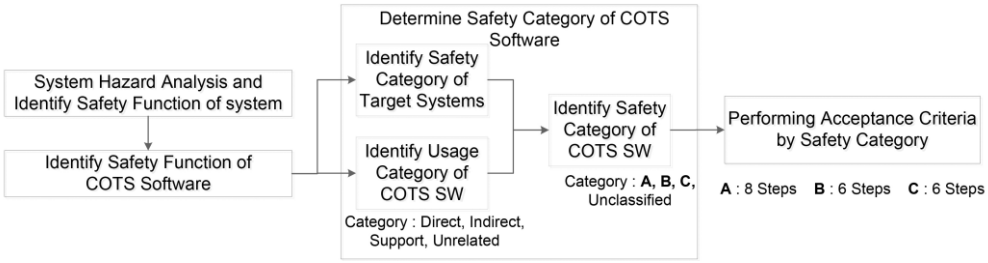

Figure 4 NUREG/CR-6421 인증 프로세스 개요

<Figure 4>는 NUREG/CR-6421에서 제안하고 있는 상용소프트웨어 인증과정을 보여준다. EPRI NP-5652와 마찬가지로 소프트웨어와 관련된 안전기능을 식별해야 하며, 카테고리 별 인증 과정은 A, B, C로 각각 구분되어 있다. NUREG/CR-6421의 인증과정 중 시스템 위험성 분석 및 안전기능 식별은 원자력 발전소의 전체 시스템분석을 통해 소프트웨어가 수행하는 안전기능을 식별하는 과정이다. 식별한 안전기능은 안전 카테고리 결정에 사용된다. 상용 소프트웨어의 안전 카테고리는 소프트웨어가 수행하는 안전 기능과 소프트웨어의 사용 방식에 따라 달라진다. 소프트웨어의 안전 기능에 따라 IEC 61226의 안전 카테고리가 정해지고, 상용소프트웨어의 사용 방식에 따라 이 안전 카테고리가 그대로 적용되기도 하고, 변화되어 적용 되기도 한다.

인증과정에서 카테고리 결정에 사용되는 상용소프트웨어의 사용 방식은 다음의<Table 1>과 같다. COTS 소프트웨어 사용방식은 직접사용, 간접사용, 지원용도, 미 연관이 있다. COTS 소프트웨어의 안전 카테고리는 사용 카테고리에 따라 적용 내용이 달라진다. 직접사용(Direct) 소프트웨어는 안전기능을 직접적으로 담당하는 소프트웨어들이 해당되며 대상이 되는 시스템, 모듈, 안전기능의 IEC 61226 카테고리에 따라 안전 카테고리가 정해진다. 간접사용(Indirect) 카테고리는 대상 시스템, 모듈을 생성하는 소프트웨어들이 해당되며 경우에 따라 같은 수준의 카테고리 혹은 한 단계 낮은 카테고리로 적용된다.

Table 1NUREG/CR-6421 COTS software 사용 카테고리

COTS 사용 카테고리	상세 설명	IEC 61226 카테고리
직접 사용 (Direct)	A, B, C 안전 카테고리의안전 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 사용이 아닌 다른 방식으로 A, B, C 카테고리 시스템 개발을 지원	unclassified
미 연관 (Unrelated)	A, B, C 카테고리에 영향을 미치지 않음	unclassified

최종적인 적용은 분류한 안전 카테고리에 따라 각기 다른 기준이 적용된다. A 카테고리의 경우 8 단계의 과정으로 구성되며 그 내용에는 가장 높은 수준의 V&V 및 소프트웨어 품질보증 체계 인증이 요구되고, 같은 버전의 소프트웨어 사용 경험에 대한 증명도 필요하다. B, C 카테고리의 경우 각각 A 카테고리보다 낮은 수준의 기준을 가지고 있으며 6 단계의 과정으로 구성된다.

5.0 TR-1025243

<Figure 1> 은 TR-1025243 및 NP-5652 의 commercial-item dedication 에 대한 개요 이다. Commercial item(SW)는 Technical Evaluation 과 Acceptance Process 로 구성된 두 가지 과정을 거쳐 dedication 되며 최종적으로 dedication 된 결과물은 원자력 발전소의 quality 요구사항인 10CFR50 App. B requirements 를 만족하도록 제작된 기본기기(basic component)와 동등한 자격을 가진다. TR-1025243 은 이를 위해 NP-5652/TR-106439 의 dedication process 를 이용하고 있다.

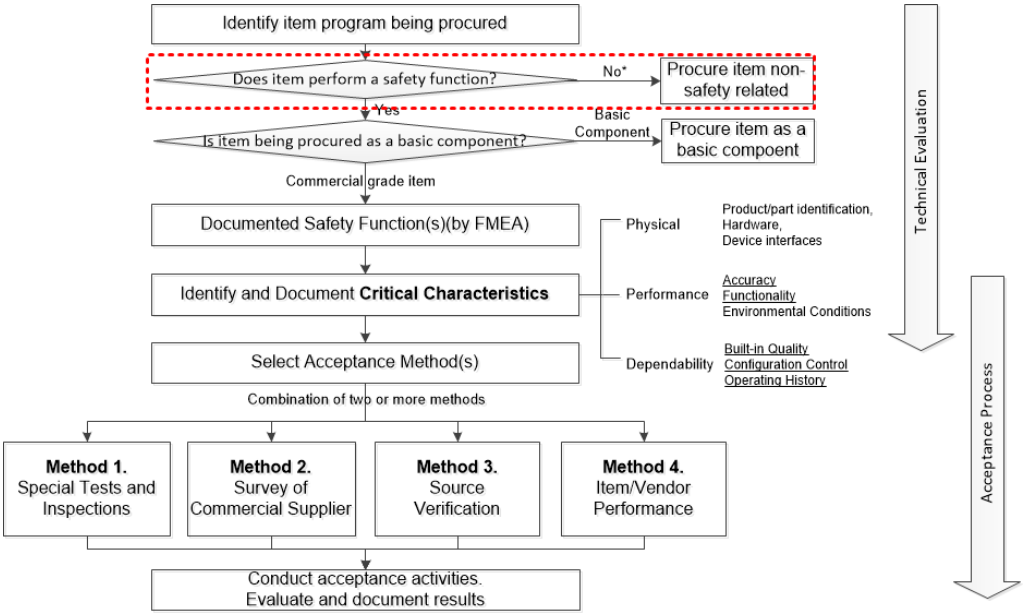

Figure 5 NP-5652/TR-106439 의 dedication process

<Figure 5> 는 TR-1025243 에서 기본으로 하고 있는 NP-5652/TR-106439 의 dedication process 의 그림이다. Technical Evaluation 은 process 의 전반부를, Acceptance process 는 process 의 후반부에 해당하며 TR-1025243 은 commercial-computer program 의 dedication 을 위해 Technical evaluation 과정중 <Figure 2> 에 표시된 부분에 computer program 을 대상으로 functional safety classification 을 적용하고 있다. 표시된 부분은 사용하려는 대상 commercial computer program 이 safety function 을 수행하는지 확인하는 부분으로 기존의 프로세스 에서는 직접적으로 safety function 을 수행하는 item 들 만이 대상이 되었지만 TR-1025243 은 이 부분에서 functional safety classification 수행을 통해 경우에 따라 구분하고 있다. 본 보고서에서는 functional safety classification 에 대해 중점적으로 설명 한다.

5.1 Functional Safety Classification

Functional safety classification 은 TR-1025243 에서 commercial computer program 의 dedication 수행 여부 및 범위를 결정하기 위해 수행하는 과정으로 computer program 의 usage, impact, failure 를 고려한 분류를 하고 있다. Functional safety classification 에서 사용하는 분류 방법으로는 2 가지 방법을 소개 하고 있다.

- Considering Failure Modes and Effects

- Considering Impact Categorization

Functional safety classification 은 위와 같은 2 가지 방법으로 하고 있으며, classification 수행 결과에 따라 대상 computer program 의 dedication 수행 여부가 결정 된다.

5.2 Considering Failure Modes and Effects

Failure modes and effects 를 고려한 방법은 computer program 의 failure 를 상정하고 failure 가 대상 safety-related SSC (System, Structure, Component)에 미치는 영향에 따라 분류하는 방법을 기본으로 적절한 process 로 구성되어 있다.

<Figure 6 Functional Safety Classification Process[10]Figure 6> 은 Failure Modes and Effects 를 고려한 functional safety classification 과정이다. 분류는 computer program 의 사용 용도와 failure 의 영향, verification 여부 등을 이용하여 분류 한다. 분류 과정을 자세히 살펴보면 다음과 같다.

우선 대상 computer program 이 safety-related SSC 에 필수적인지 확인 한다 (5.4.1.1). 이 부분은 safety-related SSC 에 직접 사용되는, 즉 SSC 기능을 수행하는 소프트웨어들을 확인하기 위한 부분으로 여기에 해당되는 소프트웨어들은 TR-106439 에 따라 dedication 을 수행하게 된다. 이 범위에 해당하는 소프트웨어들은 TR-1025243 의 대상인 computer program 이 아닌 direct COTS SW 에 해당한다.

다음으로는 컴퓨터 프로그램이 safety-related SSC 에 영향을 미치는지 확인한다 (5.4.1.2). Safety-related SSC 에 영향을 미칠 수 있는 용도의 컴퓨터 프로그램은 디자인, 분석, 모니터링의 용도로 사용되는 소프트웨어들이다. 이 소프트웨어 들은 결과나 동작이 SSC 의 동작이나 기능, 능력 등에 미치는 영향이 존재 한다. 예를 들어 컴파일러와 같이 디자인 프로세스에서 사용되는 소프트웨어는 safety-related SSC 의 application 에 직접적인 영향을 미칠 수 있다.

Safety-related SSC 에 영향을 미치지 않는 computer program 은 SSC 의 quality program 관리 등을 지원하는 용도로 사용되는지 확인하고 (5.4.1.3), 지원 용도로 사용 된다면 non-safety related/augmented quality 로 분류하고, 지원 용도로도 사용

되지 않는 경우에는 non-safety related 로 분류 한다.

다음 과정은 컴퓨터 프로그램이 디자인, 분석, 모니터링 용도로 사용되어 safety-related SSC 에 미치는 영향이 있는 것으로 분류된 소프트웨어가 SSC 의 safety-function 과 연관이 있는지 확인 한다(5.4.1.4). 이는 컴퓨터 프로그램의 용도 및 대상과 관련된 부분으로, safety-related SSC 의 디자인이나 분석에 사용 되더라도 safety function 에 영향을 미치지 않는다면 non-safety-related/augmented quality 로 분류 한다.

SSC 의 safety function 에 영향을 미치는 컴퓨터 프로그램으로 분류된 소프트웨어에 대해 다음으로는 independently verified 여부를 확인한다(5.4.1.5). Independently verified 의 의미는 컴퓨터 프로그램으로부터 도출된 결과가 다른 방법을 통해 검증될 수 있는가를 확인하는 것이다. 다른 방법은 manual 한 검사, 인증된 같은 기능의 프로그램을 이용하여 도출된 결과와 비교, 추가 검증 방법을 통한 검증이 포함된다. 예를 들어 디자인 도구의 경우 independently verification 방법은 simulation, unit testing 등을 포함한 다른 방법의 검증 혹은 디자인 결과물의 manual 한 확인 등이 있다. 이 경우 independently verified 가 가능한 컴퓨터 프로그램의 경우는 non-safety-related/augmented quality 로 분류 된다.

Safety function 에 영향을 미치면서 independently verified 방법도 없는 컴퓨터 프로그램은 발생 가능한 failure 를 상정하고, failure 가 SSC 의 safety function 수행에 미치는 영향에 대해 확인 한다(5.4.1.6 ~ 5.4.1.8). 컴퓨터 프로그램에서 발생할 수 있는 failure 는 interface 문제, arithmetic error 등이 있으며 이러한 failure 의 결과로는 inaccurate results, malfunction 등이 발생한다. 이와 같은 failure 로 인한 결과가 safety-related SSC 이 safety function 수행에 반대의 영향을 미친다면 이는 safety-related 로 분류되고 dedication 을 수행해야 한다.

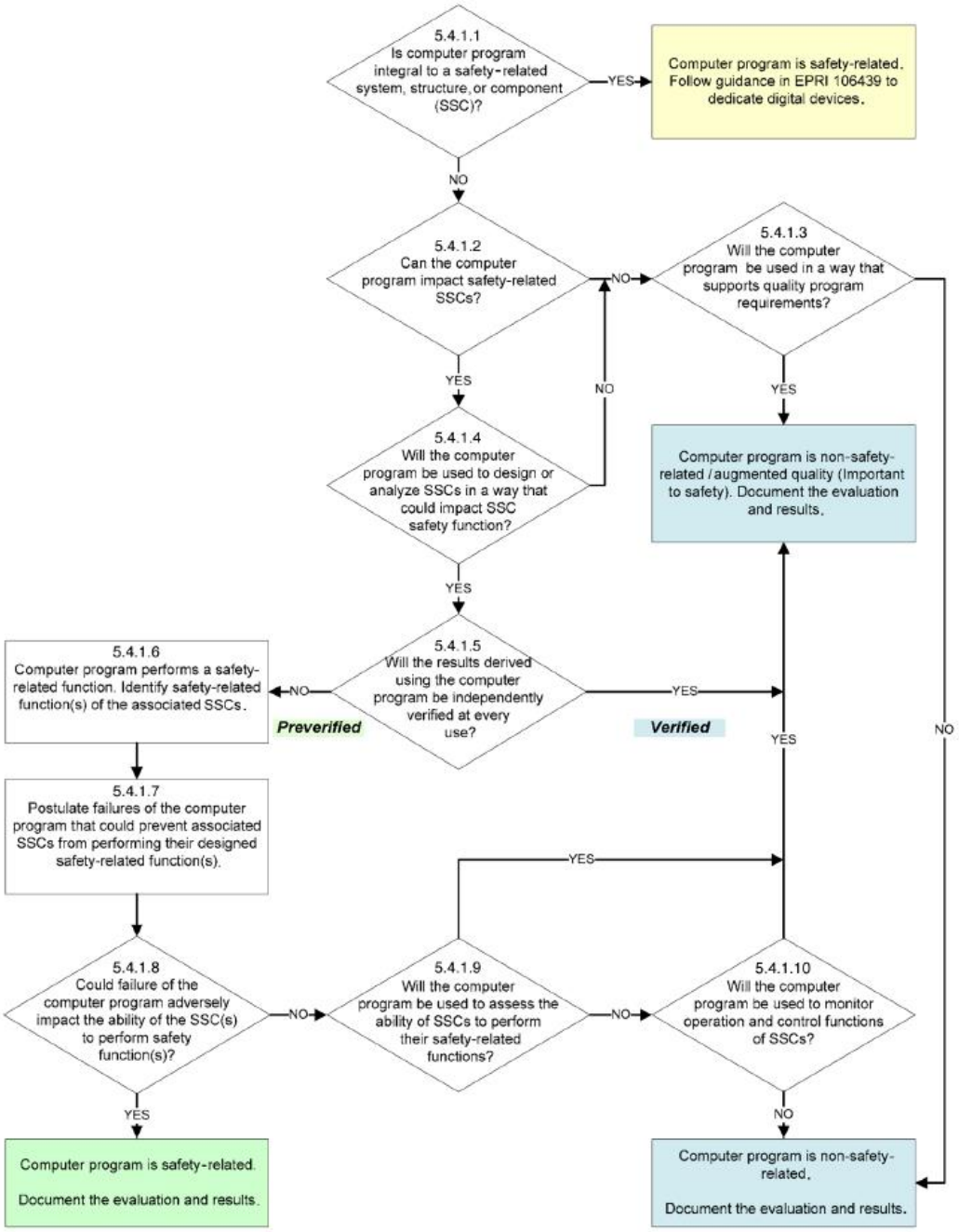

Figure 6 Functional Safety Classification Process[10]

5.3 Considering Impact Categorization

Impact categorization 방법은 computer program 이 SSC 에 미치는 impact 에 따라 카테고리를 분류하여 dedication 여부를 결정하는 방법이다. Impact category 는 4 가지로 분류 하고 있다.

IMPACT CATEGORY	DESCRIPTION
HIGH IMPACT	SSC 의 safety function 수행 능력에 직접적으로 영향을 미치는 소프트웨어
MEDIUM IMPACT	SSC 의 safety function 수행 능력을 평가하거나 monitoring 하는데 사용되는 소프트웨어
LOW IMPACT	직접적이 영향 없이 지원 행동을 하는 소프트웨어
OTHER	위 분류에 포함되지 않는 소프트웨어

소프트웨어를 4 가지 카테고리로 분류하며, high impact category 의 소프트웨어들은 safety-related 로, medium impact 의 경우 non-safety-related/augmented quality 로 그 외의 분류는 non-safety-related 로 분류 하고 있다.

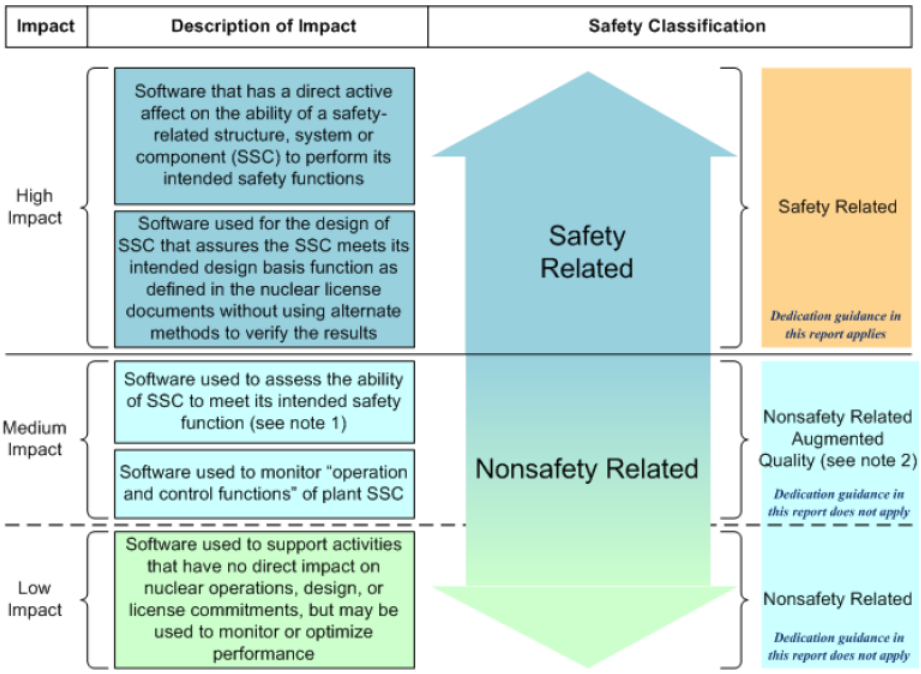

Figure 7 TR-1025243 의 impact categorization 을 통한 classification 그림[12]

<Figure 7>은 impact categorization 을 이용한 safety classification 에 대한 그림이다. Impact categorization 을 통한 safety classification 은 첫 번째 방법인 failure mode and effects 를 이용한 분류와 유사하게 분류 하고 있다. 즉, SSC 의 safety function 수행에 영향을 미치지만 independently verified 되지 않는 소프트웨어들이

safety-related 로 분류되고, 영향을 미치지만 독립적 검증이 가능한 소프트웨어들은 non-safety related/augmented quality 로 분류되는 점에서 그 내용과 과정이 동일하다.

5.4 Acceptance Process

Functional safety classification 이후의 dedication process 는 NP-5652/TR-106439 의 수행 과정과 동일하다. 대상 computer program 의 critical characteristics 를 확인 및 선정하고, acceptance methods 선정 후에 인증을 진행한다.

Critical characteristics 는 physical, performance, dependability 가 있으며 physical characteristics 는 컴퓨터 프로그램의 특성상 critical characteristics 에서 제외 할 수 있다. 위 두 가지 특성을 인증하기 위한 인증 방법으로는 4 가지 방법이 있으며 각각 Method 1. 특별 시험, Method 2. 공급자 조사, Method 3. 소스 검증, Method 4. 사용이력 조사 이다.

특히 공급자 조사를 통해 소프트웨어의 개발 과정이나 단계, safety lifecycle requirements, QA assurance, SCM, V&V 등의 내용을 확인하는 것이 필요하고, 소스 검증은 commercial 소프트웨어의 한계로 거의 적용이 불가능하다.

6.0 An Extended COTS SW Dedication Process

국내에서는 법령 KINS/RG-N17.12 "안전성관련품목 대체사용을 위한 일반규격품의 품질검증" 에서 EPRI NP-5652와 EPRI TR-106439를 사용한다고 정의되어 있다. 하지만 두 표준은 그 대상이 직접사용 되는 하드웨어 및 소프트웨어 기반 장비이기 때문에 컴파일러나 합성도구 같은 개발을 지원하는 간접 소프트웨어에 직접 적용하기에는 무리가 있다.또한 합성도구의 인증은 컴파일러의 역할을 수행함으로써 매우 중요하지만 TR-1025243에 따라 인증 대상으로 분류되지 않는다.위 표준들은 수행되는 방법에 대해서도 NUREG/CR-6421과 같은 정량적인 기준(부록A)도 없는 상황이다. 따라서, 효과적인 간접사용 상용소프트웨어의 인증을 위해 NUREG/CR-6421표준을 정량적인 기준으로 삼고, 간접사용 소프트웨어에 이를 적용하려고 한다.

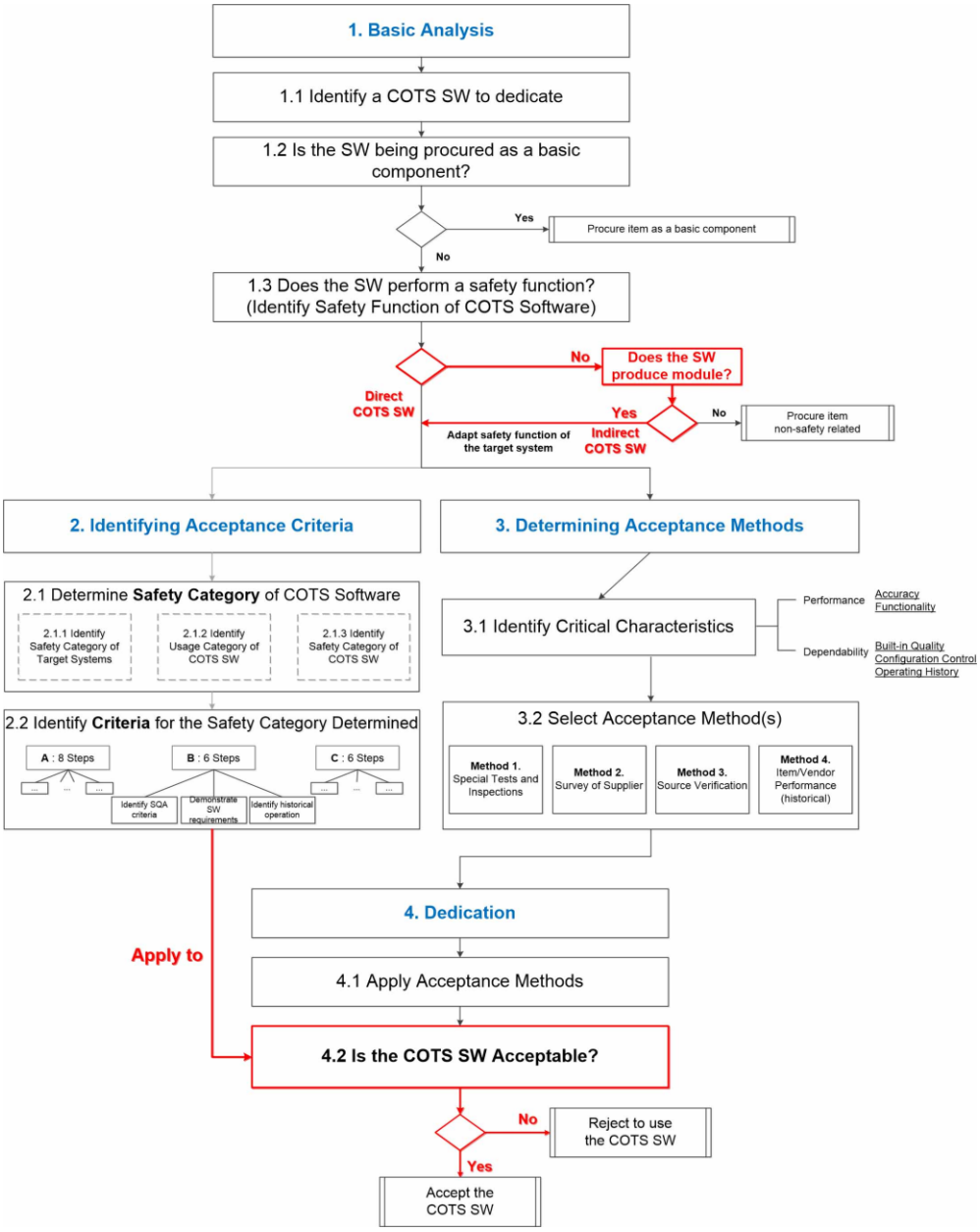

Figure 8 통합 인증 프로세스

<Figure 8>은 본 문서에서 두 표준을 이용해인증을 진행하는 통합 인증 프로세스를 표현한 것이다. 기본적인 인증 방법은 EPRI NP-5652, TR-106439를 통해 결정하나,간접 사용되는 도구들에 대한 내용이 추가되고,또한 각각의 인증 방법을 적용함에 있어 정량적인 기준 및 수준을 NUREG/CR-6421을 통해 간접사용 카테고리에 맞도록 결정한다.

7.0 IP Core Library 사용이 dedication에 미치는 영향

IP(Intellectual Property) Core library 는 복잡한 시스템의 설계를 간단히 하기 위해 미리 정의한 기능과 회로의 라이브러리이다.일반적으로 vendor 에서 제공하거나 3rd party library 를 이용 할 수 있다.상용 합성도구에서 이러한 IP Core library 를 합성 과정에 이용하게 되는 경우 합성도구의 dedication 과정에서 이에 따른 고려가 필요하다.상용 합성도구에서 IP Core library 를 사용하여 합성을 수행할 수 있는 경우의 수를 2 가지로 분류하면 다음과 같다.

1) 디자인 단계에서 사용한 IP Core library 사용
2) 합성도구 임의로 IP Core library 를 사용하여 합성

디자인 단계에서 사용한 IP Core library 를 사용하여 합성하는 경우는 일반적으로 RTL design 지원 도구를 통해 사용하는 경우이다. Libero SoC 11.5 의 경우 Smart Design 을 이용 가능하다.또한 Mentor Graphics 의 HDL Designer, Xilinx 의 ISE, Altera 의 Quartus 2 등이 있다.

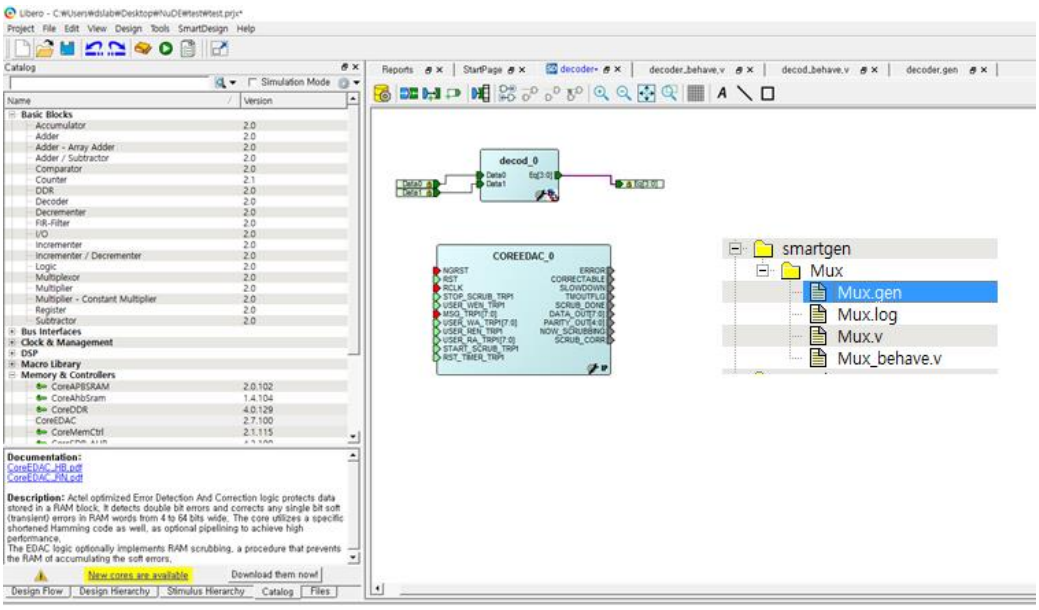

Figure 9 Smart Design 을 이용한 라이브러리 사용 화면

1), 2)번 각각의 경우에 따라 IP Core library 의 사용이 상용 합성 도구의 dedication

에 미치는 영향을 살펴보면 다음과 같다. 1)번 과 같이 디자인 단계에서 사용된 IP Core library 의 경우 해당 라이브러리는 디자인에 의존적이고, 디자인 대상의 verification 범위에 포함 된다고 할 수 있다. 그 이유는 디자인에 사용 되어야만 IP Core library 를 사용하기 때문이다. 따라서 1)에 해당되는 IP Core library 사용은 합성도구의 COTS SW dedication 수행 시 미치는 영향이 없다고 할 수 있다. 반대로 2)번 과 같은 사용은 합성도구의 기능, 능력과 연관된다고 할 수 있다. 디자인과 관계없이 합성도구의 기능으로 사용하는 것이기 때문이다. 이 경우 상용합성도구의 COTS SW dedication 과정에서 IP Core 사용에 대한 고려 및 분석이 필요하다. 고려해야 할 점은 합성 과정에서 사용되는 IP Core library 의 종류 및 기능과 대상 IP Core 들에 대해 V&V 수행 여부 및 결과 확인 또는 사용되는 IP Core 들에 대해 특별시험을 통한 확인 등 이다.

7.1 Synplify Pro 의 IP Core library 사용여부확인결과

라이브러리를 사용한 디자인과 라이브러리를 사용하지 않지만 같은 기능을 하는 Verilog 디자인을 각각 합성하여 그 결과를 확인하는 방식으로 Synplify Pro 의 IP Core library 사용 여부에 대해 확인 하였다. 실험을 위해 'Synplify Pro' 사용을 지원하는 통합개발환경인 'Libero SoC'의 Smart Design 을 통해 라이브러리를 사용한 디자인을 생성하고, 같은 기능의 라이브러리를 사용하지 않은 디자인을 작성 하였다. 실험은 'Libero SoC'의 에서 사용 가능한 디자인 도구의 라이브러리 중 basic block 에 해당하는 사칙연산 블록(adder, subtractor, counter, incrementer), 비교블록(Comparator)과 multiplexer 를 대상으로 하였다.

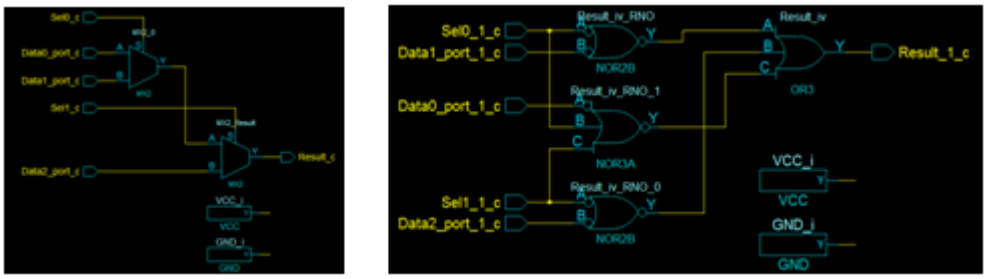

Figure 10. 3to1 Multiplexer 라이브러리 사용 디자인(좌) HDL 로 직접 작성한 디자인(우) 그림

<Figure 10>은 첫 번째 실험 결과 중 3to1 multiplexer 에 대해라이브러리를 사용한 디자인과(좌), 직접 HDL 을 작성 하여 라이브러리를 사용하지 않은 디자인(우)

의 합성 결과에 대해 각각 나타낸 그림이다. <Figure 10> 결과 'Smart Design'의 라이브러리를 사용한 코드는 기본 게이트인 MX2 2 개를 사용한 반면 Verilog 로 작성된 디자인은 NOR, OR 등의 게이트를 이용하여 합성 되었다. 비교를 통해 'Synplify Pro'는 3to1 multiplexer 에 대해서 합성 과정에서 'Smart Design' 의 라이브러리를 사용하지 않음을 알 수 있다. 다른 라이브러리에 대해서도 같은 실험을 수행 하였다.

Table 2 실험 결과 비교

Logic	Smart Design(사용)	Verilog(미사용)
3to1 Mux	2 개 (2to1 mux 2)	9 개 (NOT 5, NOR3 1, NOR2 2, OR3 1)
Decoder	6 개 (NOT 2, AND 3, NOR 1)	8 개 (NOT 4, NOR 4)
4 bit Adder	11 개 (AND 7, XOR3 3, XOR2 1)	15 개 (AND 6, OR 2, XOR3 3, XOR2 1, NOT 2, NOR 1)
Incrementer	6 개 (AND3 1, AND 1, XOR 3, NOT 1)	9 개 (AND3 1, XOR 3, NOT 3, NOR 2)

<Table 2> 는 실험 결과에 대해 비교 예제의 일부로 3to1 mux 와 adder, decoder, incrementer 라이브러리에 대해 비교한 예제 이다. 각각의 모듈들에 대해 비교해 본 결과 사용하는 게이트의 종류와 개수가 다름을 확인 할 수 있었다. 다른 모듈들도 4 개의 로직과 마찬가지로 사용하는 게이트들의 차이점이 존재함을 확인 하였다. 결과적으로 Synplify Pro 에 대해서는 IP Core library 를 합성과정에서 임의로 사용하지 않는 것을 확인 할 수 있다.

8.0 Reference

[1] KEPCO E&C,건설 원전 CGI Dedication, 제 18 회 원자력안전정보기술회의, 2015

[2] 10CFR50 B

[3] Electric Power Research Institute, "Plant Engineering : Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications(NP-5652)"

[4] TR-102260

[5]Electric Power Research Institute, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications(TR-106439)"

[6] Electric Power Research Institute, "Guideline for Sampling in the Commercial-Grade Item Acceptance Process", 1999

[7] Electric Power Research Institute, "Guidelines for the Technical Evaluation of Replacement Items in Nuclear Power Plants", 1989

[8] Electric Power Research Institute, "Plant Support Engineering : Guidelines for the Technical Evaluation of Replacement Items in Nuclear Power Plants, Rev1", 2006

[9] NUREG/CR-6421, "A Proposed Acceptance Process for Commercial Off-the-Shelf(COTS) Software in Reactor Applications.

[10] Electric Power Research Institute, "Plant Engineering : Guideline for the Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Application", 2013

[11] KINS/RG-N17.12, "안전성관련품목 대체사용을 위한 일반규격품의 품질검증"

[13] Jong Gyun Choi, Dong Young Lee, "Development of RPS trip logic based on PLD technology", Nuclear Engineering and Technology, Vol. 44, Num 6. Pp 697-708, 2012

[14] 이동아, 유준범, 최종균, "원자력 발전소의 FPGA 기반 계측제어 시스템을 위한 통합 소프트웨어 개발 환경", 정보과학회지 제 32 권 제 12 호, p36-43, 2014. [3] FPGA 기반 DIGITAL I&C

[15] Jaeyeob Kim, Eui-Sub Kim, Junbeom Yoo, Young Jun Lee, Jong-Gyun Choi, "An Integrated Software Testing Framework for FPGA-based Controllers in Nuclear Power Plants", Nuclear Engineering and Technology (Submitted)

[16] Eui-Sub Kim, Junbeom Yoo, Jangyeol Kim, "A VIS-based Correctness Verification Technique for Commercial FPGA Logic Synthesis," Software Testing, Verification and Reliability. (Submitted)

[17] Microsemi Libero SoC, "http://www.microsemi.com/products/fpga-soc/design-resources/design-software/libero-soc"

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