원자력 발전소 I&C 시스템의 안전성 분석을 위한 신기술 적용 사례

건국대학교 ▌이동아 · 김의섭 · 유준범

1. 서 론

최근 원전, 항공, 철도 등과 같은 안전필수시스템(Safety Critical System)의 사고로 인한 피해가 심각해지고 있다. 그 예로, 2011년 3월에 발생한 후쿠시마(福島) 제1원전의 사고로 인하여 방사성물질이 대기와 바다로 방출되었다[1]. 이로 인해 일본 정부는 원전 반경 20km 지역을 경계구역으로 지정하여 출입금지 구역으로 설정하였고, 20,000여 명의 사고 복구 작업종사자와 243,000여 명의 지역 주민들을 대상으로 피폭선량 평가가 이루어졌다[2]. 또한 2008년 산둥성(山東省)에서 발생한 열차사고로 인하여 72명이 사망하고 416명이 부상을 입는 등의 큰 피해를 입혔다[3].

이처럼 사고의 피해가 커지면서 안전필수시스템의 안전성에 대한 요구가 높아지고 있다. 특히 원자력 분야는 후쿠시마 사고 이후 원전 운영국들이 공통적으로 안전성 점검에 착수하는 등의 움직임을 보였다[4,5]. 주요 운영국 중 일본과 EU 등은 원전운영을 재검토하고 독일과 스위스 등은 원전 완전 폐지하는 것으로 정책의 방향을 변화시켰다. 미국과 프랑스 등의 국가는 정책을 유지하지만 안전한 원전 개발에 많은 노력을 기울이고 있다.

원자력 분야의 I&C(Instrumentation and Controls) 시스템에 대한 안전성 분석(Safety Analysis; 또는 위험성 분석: Hazard Analysis)을 위하여 다양한 기법들이 적용되어 왔다. Fault Tree Analysis(FTA)[6]와 Failure Mode and Effect Analysis(FMEA)[7], HAZard and OPerability Analysis(HAZOP)[8] 등이 대표적으로 사용되는 기법들이다. 위와 같은 기법들은 약 50년 전에 개발된 기법으로서 많은 산업분야에서 사용하였고, 여러 인증기관에서 시스템의 안전성 분석을 위한 수단으로 요구하고 있다. 하지만, 현재 사용하거나 개발 중인 시스템들은 위 기법들이 개발되던 시기의 시스템들과는 비교할 수 없을 정도로 규모가 크고 복잡해졌다. 그로 인하여 한계점들이 드러나고 있다.

최근 MIT의 Nancy G. Leveson 교수는 시스템을 표현하는 새로운 모델인 System-Theoretic Accident Model and Processes(STAMP)와 STAMP로 표현된 시스템의 안전성을 분석하는 기법인 System-Theoretic Process Analysis(STPA)를 제시하였다. 기존 기법들을 이용해 STAMP로 표현된 시스템의 안전성을 분석할 수 없기 때문에 STPA를 개발하였다. STPA의 주된 목적은 소프트웨어를 포함한 설계의 오류나 컴포넌트 사이의 상호작용에서의 사고, 사람에 의해 발생한 사고 등을 밝혀내기 위함이다.

본 논문에서는 기존의 안전성 분석 기법과 새로운 기법인 STPA를 소개하고, STPA를 원자력 발전소 I&C 시스템 중 일부에 적용해 본 사례를 소개한다. 또한, 새로운 기법과 기존 기법과의 차이를 보이고 새로운 기법의 장점들을 소개하며, 새로운 기법의 동향에 대해 살펴본다.

2. 안전성 분석 기법

2.1 기존 안전성 분석 기법

2.1.1 FTA

FTA(Fault Tree Analysis)는 Bell 연구소의 H. A. Watson에 의해 Minuteman 미사일 발사 컨트롤 시스템에 관한 연구를 진행하면서 처음 고안되었고, Boeing 사의 Dave Haasl에 의해 Minuteman 미사일 시스템 전체에 적용되었다. 1965년에 System Safety Conference에 해당 논문이 소개되면서 면서 세계적으로 관심을 받기 시작했다[10]. 그 후, 현재까지 다양한 분야(항공우주,

† 본 연구는 "지식경제부의 지원 및 한국원자력연구원의 안전등급 제어기기 엔지니어링 도구 성능개선 기술개발사업(KETEP-2010-T1001-01038)"과 "원자력계측제어 적합성평가, 감시 및 대응 체계 구축" 사업의 지원으로 연구한 결과로 수행되었음.

철도, 원자력 등)에서 오랫동안 지속적으로 사용되어지고 있는 방법이다.

FTA는 연역적, 하양식(Top-down approach)특징을 가지고 있는 분석방법으로써, 분석이 필요한 시스템의 장애를 최상위 사상(Top event)으로 설정하고, 시스템의 실패를 발생시킬 수 있는 내부 요인을 논리적 관계로 연결한다[11]. 이를 통해 최상위 사상을 일으킬 수 있는 기본 사상(정상적 사상, 문제를 품고 있는 사상)들의 조합을 통해 문제를 분석하게 된다.

FT(Fault tree)는 기호(표 1)와 게이트(표 2)를 이용하여 시각적으로 표현(그림 1)되기 때문에 다른 안전성 분석 기법에 비해 상대적으로 적용과 이해가 쉽고, 최

표 1 FTA에 사용되는 기호

기호	내용
사상 (Event)	개개의 사상 보통 결함사상을 표시 논리기호의 입력 또는 출력
기본사상 (Basic Event)	더 이상 전개하지 않는 기본적 사상 논리기호의 입력 논리기호의 출력은 되지 않음
전입 (In) 전출 (Out)	동일한 FT속에서 내용이 같은 타 부분과의 사이에 전이를 나타내는 기호로서 삼각형의 상부에 선이 나오는 경우는 타 부분에서의 전입을 의미하고 측면에 선이 나오는 경우는 타 부분으로의 전출을 나타낸다.
부전개사상 (Undeveloped Event)	정보부족에 의해 분석되지 않거나 또는 분석의 필요가 없는 생략현상을 나타내는 기호이다.

표 2 FTA에 사용되는 논리 게이트

기호	내용
AND 게이트	하위사건을 모두 만족하는 경우에 사용하는 논리 게이트
OR 게이트	하위사건 중 어느 하나라도 만족하면 사용하는 논리 게이트

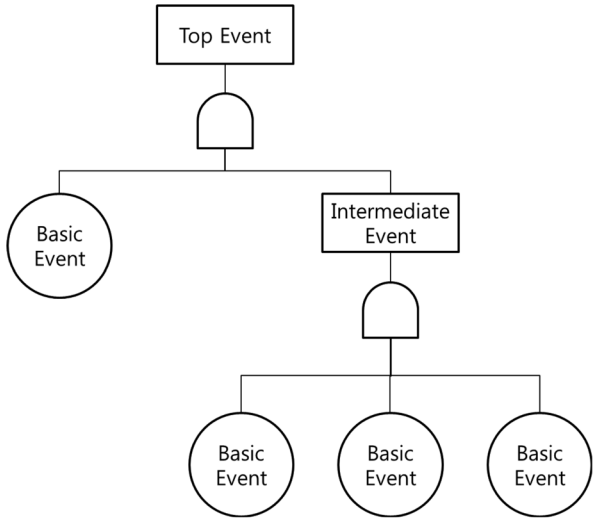

그림 1 Fault Tree 예시

상위 사상까지의 path와 이를 이루고 기본 사상들의 관계 파악에도 용의하다. 하지만, FTA는 하나의 fault tree에 하나의 재해만을 분석 할 수 있기 때문에 시스템이 발생시킬 수 있는 모든 재해를 분석하기 위해서는 많은 시간과 노력이 필요할 수 있으며, 사상간 순차적 처리와 같은 시간적 요소 고려하기 어렵다는 단점이 있다.

2.1.2 FMEA

FMEA(Failure Mode and Effect Analysis)는 1949년대 U.S. military에서 정형정인 분석을 하기 위해 처음 개발되었으며, 1960년대 우주산업과, 1970년대 자동차 산업에서 사용되면서 점차 다양한 분야에 사용되기 시작했다[12]. 1990년대 들어서는 ISO 9000, QS 9000 등의 품질보증시스템과 6-Sigma 등에서 품질 및 개선을 위한 필수적인 기법으로 인식되고 있다.

FMEA는 product와 process의 문제가 일어나기 전에 체계적으로 찾고 예방하고자 하는 방법이다[13]. 귀납적, 상향식(Bottom-UP approach) 특징을 가지고 있는 분석 방법으로써, 시스템의 잠재적인 고장 모드를 찾고, 해당 고장 모드가 전체 시스템의 신뢰성에 얼마나 영향을 미치는가를 평가하게 된다. 시스템 구성 요소의 고장발생 빈도(Occurrence)와 시스템에 대한 영향도(Severity), 시스템 사용자의 고장발생 발견 가능성(Detection) 등을 평가하여 각 구성 요소 고장의 위험 순위(Risk Priority Number, RPN)를 정하게 된다. 시스템 디자인시 해당 요소들을 고려함으로써, 보다 신뢰성 있는 시스템의 개발이 가능하게 된다.

FMEA의 결과물은 하나의 시스템 기능 별 도표의 형태로 나타내게 된다. 이 도표에는 각 요소가 발생시킬 수 있는 잠재적 실패들과 그 실패로 인해 생기는 영향들이 기록되어 있으며, 영향도, 확률, 발생 빈도, 위험도 우선순위 등으로 평가를 한 결과들이 첨가되어 있다. 많은 FMEA의 도표가 제시되고 있고, 그 중 하나의 예시는 표 3과 같다.

2.1.3 HAZOP

HAZOP(Hazard and Operability analysis)은 1960년도 중반 화학 분야에서 연구되기 시작했고, 1970년도에 디

표 3 FMEA의 worksheet 예시

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

표 4 HAZOP의 Worksheet 예시

Failure Mode and Effects Analysis										
System:		Subsystem:				Mode/Phase:				
No.	Item	Function/ Purpose	Parameter	Guide Word	Consequence	cause	Hazard	Risk	Recommendation	Comments

자인에 있을 수 있는 일탈을 찾는 방법에 대한 정형화된 이론이 나왔다[14]. 이후 Lawley에 의해 자세히 기술 되었고 현재 여러 산업분야에서 다양하게 사용되고 있다.

HAZOP은 사고가 설계 또는 운용상에서 의도한 것에서 벗어났을 때 발생하는 것을 가정하고 설계에서 예상한 운용을 하였을 경우 일어날 수 있는 모든 가능한 일탈(Deviation)상황과 그와 관련된 위해 요소를 찾으려고 하는 것이다[15]. 이러한 일탈을 체계적으로 누락없이 검토하고자 공정변수(Process parameter)와 가이드워드(Guide words)를 조합하고, 이를 통해 실제 의도에서 벗어나는 공정상의 이탈을 구성하고 이에 대하여 여러 분야의 경험을 가진 구성원이 난상토론(Brainstorming)을 수행한다.

분석과정에서 시스템에 대한 효율적인 검토를 하기 위하여 시스템 설계의 일정구간을 분할(Study node)하여 단계적으로 설비 오작동이나 운전 조작 실수 등 위험성(Hazard) 및 운전성(Operability)을 평가한다. HAZOP의 결과물은 표 4와 같은 형태로 나타나게 된다.

2.2 STAMP/STPA

System-Theoretic Accident Model and Process(STAMP)는 사고의 인과 관계를 분석하는 모델로서, 안전 제약사항(Safety Constraints)과 계층형 제어 구조(A Hierarchical Safety Control Structure), 프로세스 모델(Process Models)이라는 세 가지 개념에 기반을 둔 새로운 모델이다. 그림 2는 STAMP에서 제시하는 기본적인 형태의 계층형 제어구조를 나타낸다. 이 모델은 시스템의 개발과 운영에 관여하는 모든 요소들을 포함함으로써 시스템을 요소 전체가 상호작용하는 하나의 커다란 시스템으로 표현한다. 상위의 요소는 컨트롤러로서 하위의 요소를 제어해 안전 제약사항이 지켜지도록 하며, 컨트롤러는 제어를 위해 프로세스 모델을 가진다.

System-Theoretic Process and Alaysis(STPA)는 STAMP 모델의 안전성 분석을 위해 새롭게 제시된 안전성 분석기법이다. 4단계의 절차를 통해 안전성 분석을 수

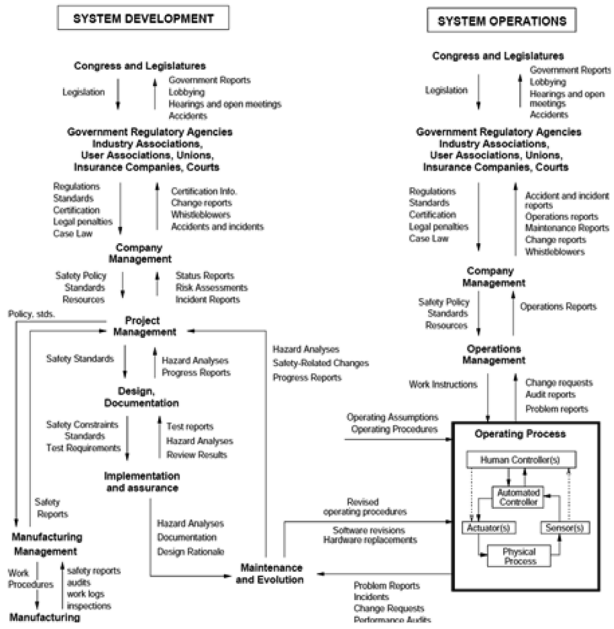

그림 2 STAMP가 제시하는 Sociotechnical Control Structure의 일반 모형[9]

행하게 되며, 그 절차는 다음과 같다.

(1) 시스템의 위험 상황을 설정
(2) 시스템의 Control Structure 도출
(3) (STPA 단계 1) 시스템을 위험한 상황으로 만들 수 있는 잠재적인 부적절 Control을 밝혀냄
(4) (STPA 단계 2) STPA 단계 1에서 밝혀낸 부적절 Control이 어떤 경우에 일어나는지 밝혀냄

STPA는 시스템을 위험으로 이끄는 원인을 밝혀내는 기법이다. 따라서 STPA를 수행하기 위해서는 시스템의 위험을 정의할 수 있어야 하며 Control Structure를 사전에 그릴 수 있어야 한다. 시스템의 기능 제어도나 요구사항, 시스템 위험, 안전 제약사항 등을 사용해 시스템의 위험을 정의하고 Control Structure를 그릴 수 있다.

STPA의 첫 단계에서 시스템을 위험으로 이끄는 부적절한 제어를 밝혀낸다. 이는 다음과 같은 4가지 분류로 나뉘게 된다.

(1) 안전을 위해 필요한 제어가 제공되지 않는 경우
(2) 제어가 제공되어 위험을 일으키는 경우
(3) 제어가 너무 이르거나 늦게, 혹은 잘못된 순서로 제공되는 경우
(4) 제어가 너무 일찍 멈추거나 너무 오래 제공되는 경우

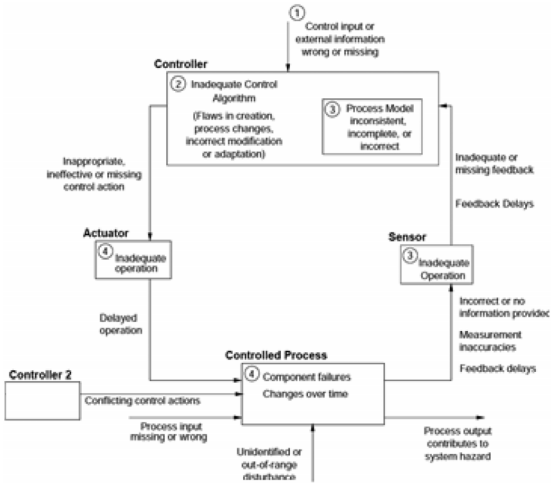

그림 3 STPA가 제시하는 위험을 일으킬 수 있는 원인 요소의 일반적인 형태[9]

네 가지 위험한 제어에 대하여 밝혀낸 후, 위험한 제어들을 일으킬 수 있는 원인을 찾아낸다. 그림 3은 원인의 일반적인 형태를 네 가지로 나타낸 그림이다.

(1) 외부로부터 들어오는 제어나 정보가 잘못 되거나 없어짐
(2) 제어 알고리즘이 올바르지 않음
(3) 제어를 위한 프로세스 모델이 잘못 되거나 정보를 제공하는 센서가 잘못 된 경우
(4) 제어되는 프로세스가 실패하거나 제어를 수행하는 개체가 실패 경우

3. 신기술 적용

3.1 적용 대상

KNICS[16] 프로젝트의 일부로 개발된 공학적안전설비-기기제어계통[1]은 원전에서 일어날 수 있는 설계기준사고[2]시 발전소보호계통[3]과 방사선감시계통[4]으로부터 신호를 받아 공학적안전설비계통 기기를 작동시키며 공학적안전설비 관련 기기를 포함한 모든 안전관련 기기의 제어기능을 수행한다. 또한 공학적안전설비-기기제어계통은 운전원으로부터의 수동작동 신호에 의해서도 기능을 수행한다.

본 논문에서는 새로운 기법을 이용한 안전주입에 대한 위험성 분석을 수행하였다. 공학적 안전설비-기기제어계통은 안전주입작동[5]과 격납용기살수작동[6] 등을 포함한 8가지의 기능을 수행한다. 이 중, 안전주입은 원자로의 온도를 낮추기 위해서 붕산을 포함하고 있는 비상 냉각수를 원자로에 제공한다. 이 기능이 제대로 작동하지 않으면 높은 압력으로 인해 원자로가 손상을 입을 수 있다. 해당 기능은 아래의 사고 발생 시 동작한다.

(1) 원자로냉각재상실사고(Loss of Coolant Accident)
(2) 이차측 열제거원(급수) 상실(2ry Heat Sink Loss)
(3) 증기관 또는 급수관 파열
(4) 제어봉집합체 인출사고(Rod Ejection Accident)

3.2 적용 결과

3.2.1 위험 설정

STPA를 이용한 위험성 분석은 대상 시스템의 위험을 밝혀내는 것으로부터 시작한다. SIAS는 원자로에서 일어나는 특정 사고 시, 원자로의 온도를 낮추기 위해서 비상 냉각수를 제공하는 동작을 한다. 이 동작이 제대로 수행되지 않을 때, 원자로는 손상을 입게 된다. 따라서 SIAS의 위험은 다음과 같다.

"원자로에 사고 발생 시 SIAS가 정상 작동하지 않아 원자로가 손상된다."

이 단계에서 시스템의 안전 제약사항을 정의할 수 있다.

"원자로에 사고 발생 시 SIAS는 반드시 정상 작동해야 한다.."

3.2.2 Control Structure 도출

그림 4는 STPA를 수행하기 위하여 SIAS에 대한 control structure를 나타내고 있다. Control structure를 그리는 주된 목적은 상위 개체들(Controllers)과 하위 개체들(Controlled Processes)의 관계를 명확히 하기 위함이다. SIAS의 안전성 분석을 위한 control structure는 8개의 개체들(Operator, MCR/RSR, IPS, ESF-CCS, ESF-AFS, PPS, Sensors, Reactor)로 구성되어 있다.

Operator는 ESF-CCS를 MCR/RSR에 있는 작동 스위치를 이용해 수동 작동시킬 수 있으며, 작동 시 MCR/RSR에 있는 화면을 통해 원자로나 ESF-CCS의 상태에

1) ESF-CCS: Engineered Safety Features- Components Control System
2) DBE: Design Basis Events
3) PPS: Plant Protection System
4) RMS: Radiation Monitoring System
5) SIAS: Safety Injection Actuation Signal
6) CSAS: Containment Spray Actuation Signal

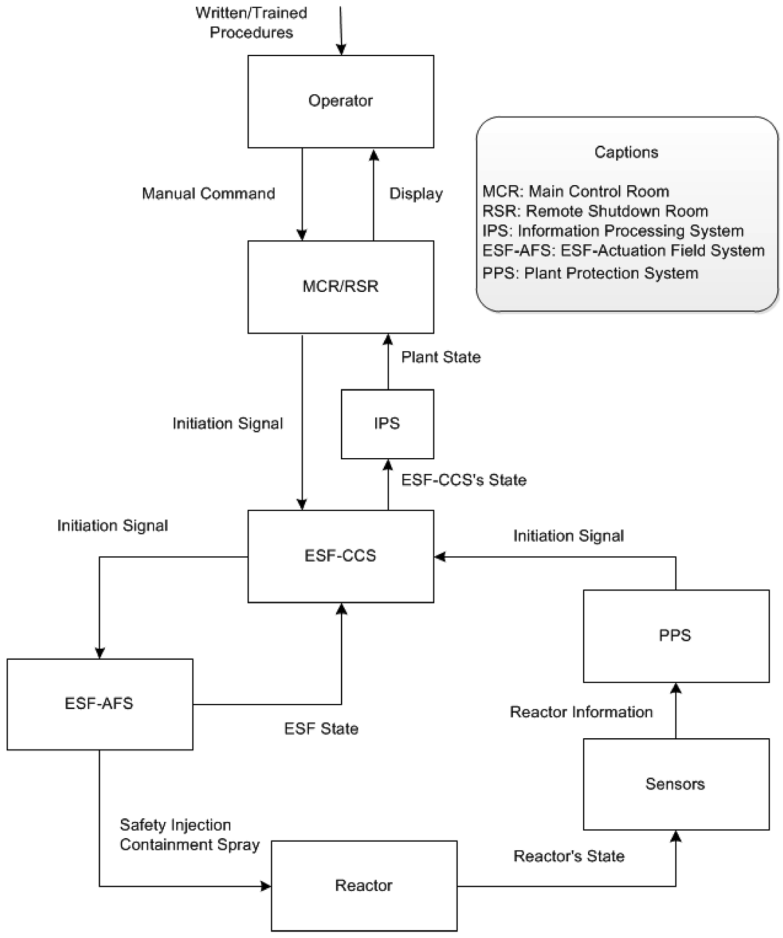

그림 4 SIAS의 안전성 분석을 위한 Control Structure

대한 정보를 얻을 수 있다. 또한 ESF-CCS는 PPS에서 얻어지는 작동변수의 값을 통해서 작동하는데, 이 때 PPS는 원자로의 상태를 감지하는 Sensors로부터 정보를 얻어 작동변수를 제어한다. 제어 정보를 받은 ESF-CCS는 벨브나 펌프에 해당하는 ESF-AFS에 작동 신호를 전달해 벨브를 열거나 펌프를 작동시키는 등의 동작을 수행하도록 제어한다.

이 중 PPS에 의한 자동 SIAS 작동에 대하여 세부적인 분석을 하기 위해 control structure를 관련된 요소들만으로 구성한 버전을 생성하였다(그림 5). PPS는 3.

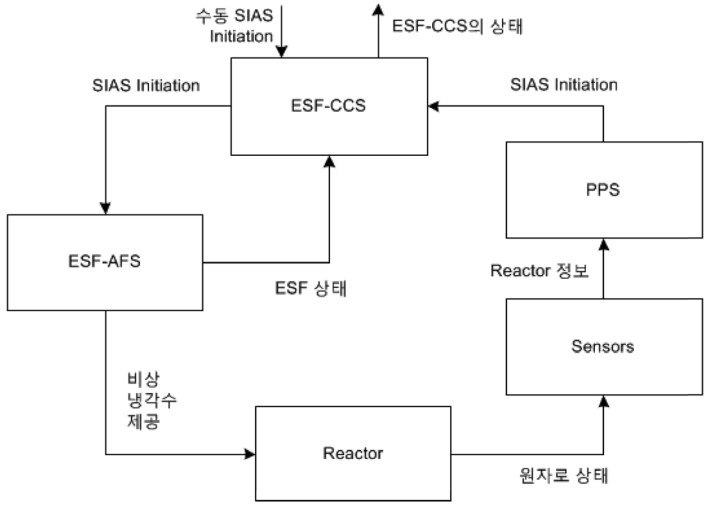

그림 5 PPS에 의한 자동동작 SIAS를 분석하기 위한 control structure

표 5 PPS에 의한 자동 SIAS동작의 위험 요소 분석 결과

Control Action	제공되지 않는 경우	제공되어 위험한 경우	타이밍이 맞지 않거나 순서가 올바르지 않아 위험한 경우	일찍 멈추거나 오래 지속되는 경우
SIAS Initiation	• LOCA 발생 시 SIAS 개시 신호가 제공되지 않음(a1) • 이차측 열제거원(급수) 상실 사고 발생 시 SIAS 개시 신호가 제공되지 않음(a2) • 증기관 또는 급수관 파열 시 SIAS 개시 신호가 제공되지 않음(a3) • 제어봉집합체 인출사고 시 SIAS 개시 신호가 제공되지 않음(a4) • 수동 SIAS 개시신호 발생 시 SIAS 개시 신호가 제공되지 않음(a5)	위험하지 않음	• LOCA발생 시 SIAS 개시 신호 발생 시간이 너무 오래 걸림(c1) • 이차측 열제거원(급수) 상실 사고 발생 시 ESF-CCS의 SIAS 개시 신호 발생 시간이 너무 오래 걸림(c2) • 증기관 또는 급수관 파열 시 SIAS 개시 신호 발생 시간이 너무 오래 걸림(c3) • 제어봉집합체 인출사고 시 SIAS 개시 신호 발생 시간이 너무 오래 걸림(c4) • 수동 SIAS 개시신호 발생 시 SIAS 개시 신호 발생 시간이 너무 오래 걸림(c5)	SIAS 개시 신호가 비상 냉각수가 충분히 공급되지 전에 멈춤(d1)

의 3.1에 명시한 4가지 사고 발생 시 반드시 SIAS작동을 위한 신호를 ESF-CCS로 제공해야 하며, 해당 작동 신호의 전달이 정상적으로 이루어지지 않았을 경우 원자로는 손상을 입을 수 있다.

3.2.3 부적절한 Controls 분석

시스템에 대한 위험과 control structure가 준비되면 STPA의 첫 단계를 수행할 수 있다. STPA의 첫 단계는 네 가지 부적절한 control actions을 찾는 것으로부터 시작된다.

네 가지 종류의 부적절한 controls을 찾아내기 위하여 표를 이용하였다. 표 5는 PPS에 의한 자동 SIAS동작의 위험요소 분석 결과이다. PPS가 제공하는 SIAS Initiation이 제공되지 않는 경우와, 제공되어 위험한 경우, 올바르지 않은 순서에 제공되 위험한 경우, 너무 빨리 멈추거나 너무 늦게 멈추는 경우에 대하여 분석을 한 결과이다. 표는 올바르지는 않지만 위험한 상황을 만들어내지 않는 제어에 해당하는 controls은 포함하지 않는다. 또한 SIAS가 제공되면 금전적인 손실이 크지만, 원자로가 손상돼 방사능 물질이 나오는 더 큰 위험상황을 피할 수 있어 포함시키지 않았다.

3.2.4 원인 도출

STPA의 두 번째 단계는 첫 번째 단계에서 찾아낸 부적절한 control actions의 원인을 찾아내는 것이다. 그림 6은 표 5의(a1)에 대한 원인 분석 결과를 control structure그림 상에 표현한 것으로서, 그림 3의 일반적인 형태의 원인 분류를 참고하여 분석한 결과이다. Controller인 ESF-CCS가 내부적인 논리에 의한 오류로 SIAS 개시신호를 제공하지 못하는 경우를 비롯해 시스템과

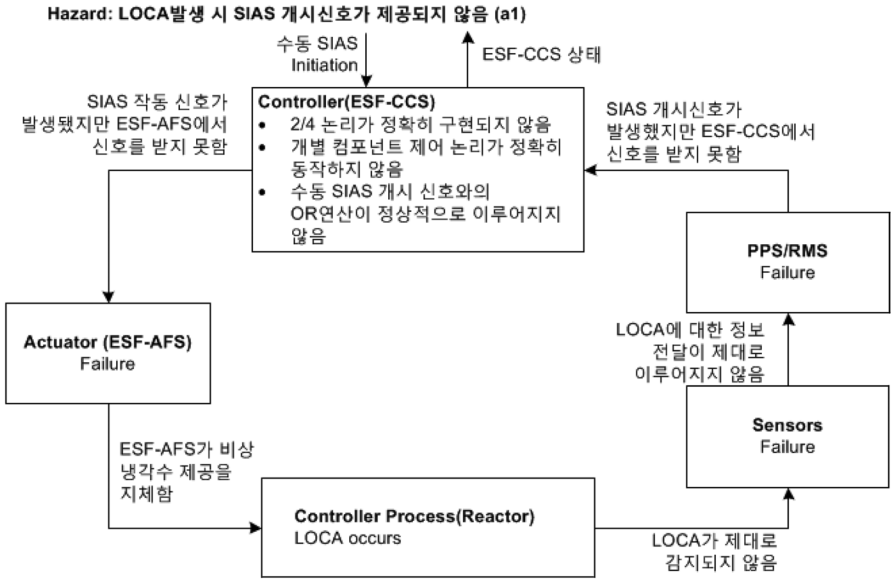

그림 6 부적절한 control(a1)에 대한 원인 분석 결과

시스템 간의 제어나 피드백 전달에서 발생할 수 있는 오류, 시스템 자체에서 발생할 수 있는 고장이나 실패에 대한 결과를 포함하고 있다.

3.3 기존 기법과 비교

STAMP에 기반을 둔 안전성 분석 기법인 STPA는 기존에 존재하지 않던 새로운 분석 기법으로써 위험에 대한 분석을 여러 시스템이나 개체들이 복합적으로 엮여 있는 시스템을 하나의 분석 대상으로 보는 것이 특징이다. 여러 시스템이 상호작용하며 하나의 시스템을 이루고, 그 상호작용에서 시스템을 위험으로 만들 수 있는 원인들이 발생한다는 개념을 바탕으로 분석하는 기법이다. 기존의 기법인 FTA나 FMEA 등은 실패에 대한 정의를 하고, 실패가 일어날 수 있는 경우를 확률이나 확률의 조합으로 나타낸다는 특징을 가진다. 기존 기법들과 STPA는 시스템과 위험을 바라보는 차이가 존재하기 때문에 그 결과도 차이가 있음을 알 수 있다.

4. 결 론

2013년에 개최된 STAMP Conference[17]에서는 미국을 포함한 전세계 11개국에서 다양한 주제를 통해 새로운 안전성 기법에 대한 관심을 보이고 있다. 특히, 원자력이나 항공, 자동차 등의 산업분야 뿐만이 아니라 조직이나 기업 문화에 대한 분석을 통해 안전성 분석을 시도하려는 연구들이 눈에 띄었다. 안전에 대한 노력이 공학이나 과학적인 접근뿐만이 아닌 다양한 분야가 통합을 이뤄나간다는 특징을 파악할 수 있다.

본 논문에서는 새로운 안전성 분석 기법인 STPA를 이용해 원전에서 사용하는 공학적안전설비-기기제어계통의 일부 기능을 분석하였다. 분석 결과에 대하여 원자력 분야의 전문가는 기존 기법들과 시스템과 시스템의 위험을 바라보는 관점이 다름을 확인할 수 있었다. 또한 위험을 일으킬 수 있는 원인의 범위가 서로 다르기 때문에 새로운 기법의 적용에 대한 타당성도 인정하였다.

시스템이 완전히 안전하기 위해서는 개발 자체를 하지 않는 것이 답이라는 말이 있을 정도로 안전을 보장하기란 매우 어려운 일이다. 안전성 분석이나 평가와 같은 분야의 전문가들은 안전이라는 것을 보장할 수는 없지만 안전하기 위한 최대한의 노력을 기울이는 것이 최선이라는 같은 목소리를 내고 있다. 따라서 높은 수준의 안전성이 필요한 원자력과 같은 분야의 시스템에 대해서는 안전성 분석 기법이 타당하고 적용가능하다면 그 기법을 적용하여 안전성을 높이는 것이 정답일 것이다.

참고문헌

[1] http://en.wikipedia.org/wiki/Fukushima_Daiichi_nuclear_disaster

[2] “후쿠시마 원전 사고 분석”, 한국원자력학회 후쿠시마위원회, 2013

[3] http://en.wikipedia.org/wiki/2008_China_Railways_train_T195_accident

[4] 홍정석, 이영준, 이영철, “후쿠시마 사고 이후 원자력 정책과 R&D 동향 및 주요 이슈”, 과학기술 및 연구개발사업 동향브리프 2012-05, 한국과학기술기획평가원, 2012

[5] 이석호, “후쿠시마 원전사고 이후 해외 원자력정책 주요 동향”, 세계 에너지시장 인사이트 제11-07호, pp 9-19, 에너지경제연구원, 2011

[6] W. E. Vesely, N. H. Roberts, “Fault Tree Handbook”, Government Printing Office, 1987

[7] D. H. Stamatis, “Failure Mode and Effect Analysis: FMEA from Theory to Execution”, ASQ Quality Press, 2003

[8] http://en.wikipedia.org/wiki/Hazard_and_operability_study

[9] Nancy G. Leveson, “Engineering a Safer World: Systems Thinking Applied to Safety”, MIT Press, 2012

[10] C. A. Ericson, “Fault tree Analysis-A History“ Proceedings of the 17th International System Safety conference, 1999

[11] http://en.wikipedia.org/wiki/Fault_tree_analysis#cite_note-1

[12] C. A. Ericson, “Hazard analysis techniques for system safety”, Wiley-Interscience, 2005.

[13] R. E. McDermott, R. J. Mikulak, M. R. Beauregard, “The basics of FMEA”, Productivity Press, 2008.

[14] a Dunjó, Jordi, et al. “Hazard and operability(HAZOP) analysis. A literature review”, Journal of Hazardous Materials Vol.173, No.1, pp.19-32, 2010

[15] 이영준, 권기춘, 이장수, 김장열, 차경호, 천세우, 손한성, “HAZOP을 이용한 안전등급 제어기기 운영체제의 안전성분석”, 한국정보과학회 가을 학술표논문집 Vol.31, No.2, 2004

[16] KNICS, Korea Nuclear Instrumentation & Control System R&D Center, http://www.knics.re.kr/

[17] http://psas.scripts.mit.edu/home/2nd-stampstpa-workshop-2013/

약 력

이 동 아

2010 건국대학교 컴퓨터공학과 학사
2012 건국대학교 컴퓨터공학과 석사
2012~현재 건국대학교 컴퓨터공학과 박사과정
관심분야 : 소프트웨어 공학, 안전성 분석, 정형기법
E-mail : ldalove@konkuk.ac.kr

김 의 섭

2012 건국대학교 컴퓨터·정보통신공학과 학사
2012~현재 건국대학교 컴퓨터·정보통신공학과 석사과정
관심분야 : 소프트웨어 공학, 안전성 분석, 정형기법
E-mail : atang34@naver.com

유 준 범

2005 KAIST 전자전산학과 전산학전공 박사
2008 삼성전자주식회사 통신연구소 책임연구원
2008~현재 건국대학교 컴퓨터공학과 부교수
관심분야 : 소프트웨어 공학, 안전성분석, 정형기법
E-mail : jbyoo@konkuk.ac.kr