KOSDI
ISSN : 1976-2208 (Print)
ISSN : 2671-5287 (On-line)
www.sodi.or.kr

Journal of the Society of Disaster Information
Vol. 16, No. 4, pp. 784-795, December 2020
https://doi.org/10.15683/kosdi.2020.12.31.784

Original Article

재해경감활동계획 수립에 위험 시나리오 도출을 위한 STPA기법 도입

Introduction of the STPA Mechanism to Derivation of Risk Scenarios for Establishment of Disaster Reduction Activity Plans

김상덕[1] · 이석형[2] · 김창수[3]*
Sang Duk Kim[1], Seok Hyung Lee[2], Chang Soo Kim[3]*

[1]PhD. Course, Department of Interdisciplinary Program of Information Systems, Pukyeong National University, Busan, Republic of Korea
[2]PhD. Course, Department of Interdisciplinary Program of Information Systems, Pukyeong National University, Busan, Republic of Korea
[3]Processor, Department of Interdisciplinary Program of Information Systems, Pukyeong National University, Busan, Republic of Korea

*Corresponding author: Chang Soo Kim, cskim@pknu.ac.kr

ABSTRACT

Purpose: This study intends to review the risk assessment procedures specified in the corporate disaster management standard. **Method:** The requirements for each stage of risk assessment stipulated in the corporate disaster management standard were identified, the case of application of the organization'A' and the partner companies were reviewed, and the risk assessment procedure in line with the requirements was reviewed. **Result:** It was reviewed that it was necessary to clearly define the method and procedure for deriving risk scenarios, which are the requirements of the corporate disaster management standard, and to introduce a standardized procedure for deriving risk scenarios. **Conclusion:** A method of deriving risk scenarios was implemented by applying the STPA technique based on the system theory for power generation fuel supply and demand, and it was suggested that the STPA technique be reflected in corporate disaster management standards as a risk scenario derivation technique for the establishment of a disaster reduction activity plan.

Keywords: Corporate Disaster Management Standard Risk Scenario. Risk Assessment. STPA. Risk Assessment for Fuel Supply and Demand Business. Establishment of Disaster Reduction Activity Plan

요 약

연구목적: 본 연구는 기업재난관리표준에 규정하고 있는 위험평가 절차에 대하여 연구하고자 한다. **연구방법:** 기업재난관리표준에 정하고 있는 위험평가 단계별 요구사항을 파악하고, 'A'기관과 협력사의 적용사례를 검토하였으며 요구사항에 맞는 위험평가 절차를 도출하였다. **연구결과:** 기업재난관리표준의 요구사항인 위험 시나리오 도출 방법과 절차에 대하여 명확히 정의하고, 위험 시나리오 도출을 위한 표준화된 절차 도입이 필요한 것으로 검토되었다. **결론:** 발전 연료수급업무에 대하여 시스템 이론에 기반한 STPA 기법을 적용하여 위험 시나리오를 도출하는 방법을 구현하였으며, 모든분야의 핵심업무에 대한 위험 시나리오 도출에 적용할 수 있도록, STPA 기법을 재해경감활동계획 수립을 위한 위험 시나리오 도출 기법으로 기업재난관리표준에 반영할 것을 제시하였다.

핵심용어: 기업재난관리표준, 위험 시나리오, 위험평가, STPA, 연료수급업무 위험평가, 재해경감활동계획 수립

Received | 10 November, 2020
Revised | 11 December, 2020
Accepted | 28 December, 2020

서 론

연구개요

재난관리를 통한 재해경감활동을 지원하기 위한 정부의 정책이 확대되고 있고, 재난예방을 위한 재해경감활동에 관한 연구가 활발하게 진행되고 있다. 재해경감활동을 위한 계획은 경영현황분석과 이해관계자 및 법적 규제적 요구사항을 이해한 후, 업무영향 분석결과 도출된 핵심업무에 대한 위험평가를 시행하고 그 결과들을 반영하여 수립하게 되고, 위험평가는 핵심업무에 위험요인(자연재난, 사회재난 등)이 어떻게 작용하여 위험이 전개될지를 인식하는 위험 시나리오를 도출하고 위험의 원인을 분석하는 절차로 시행된다(기업재난관리표준, 행정안전부).

재해경감활동계획 수립 절차를 정하고 있는 기업재난관리표준(5.3)에 의하면 "조직이 우선적으로 수행해야 하는 업무와 프로세스, 시스템, 정보, 인력, 자산, 아웃소싱협력업체와 그들을 지원하는 자원운용에 있어 중단 위험을 식별"하여 위험평가를 시행하도록 규정하고 있으나 구체적인 방법에 대하여 정하지 않고 있어 현장에서의 실질적인 적용은 집행하는 주체에 따라 지극히 주관적인 방법으로 적용하거나 생략되는 경향이 있다.

위험평가에 있어서 첫 번째 절차인 위험 시나리오 도출이 누락없이 적합하게 시행되어야 다음단계인 위험분석과 위험평가를 진행하게 되고, 재난을 예방·대비·대응·복구하기 위한 계획을 수립하는 절차를 이어 진행 할 수 있으므로, 그 절차를 규정하고 있는 기업재난관리표준에 위험 시나리오 도출을 위한 업무 절차가 구체적인 요구사항으로 포함되어 있어야 표준에 의하여 작성되는 재해경감활동계획의 신뢰성과 작동성을 담보하고 지속적으로 유지 발전시켜 나갈 수 있을 것이다.

연구방법

최근 재난이 복합화되고 발생빈도가 높아져서 재난으로 인한 피해가 증가하는 경향이고, 재난관리의 패러다임 변화로 재난예방활동의 중요성에 대한 많은 연구결과가 있음에도 불구하고, 작동성을 담보할 수 있는 재난관리단계별 재해경감활동계획 수립의 기초자료가 되는 위험 시나리오 도출기법 적용이 표준화되지 않고 있다.

본 연구에서는 기업재난관리표준에 규정하고 있는 위험평가 절차에 대하여 연구하였으며, 'A'기관과 협력사의 적용사례를 비교 분석하여 기업재난관리표준 요구사항에 맞는 위험평가 절차를 도출하였다. 기업재난관리표준 요구사항의 현장 적용 현황 파악을 위한 'A' 기관의 발전업무구조도와 핵심업무 분석에서 업무연속성 확보를 위한 중요한 구성요소인 연료업무가 핵심업무 선정에서 누락된 것과 위험평가에서 위험 시나리오 도출과정이 생략된 것을 확인할 수 있었다. Fig. 3.발전업무구조도에서 같은 업무그룹으로 되어 있는 연료업무와 연료취급설비 업무 중에서 연료취급설비만 핵심업무에 포함되는 점에 착안하여 연료업무에 대하여 STPA(System Theoretic Process Analysis) 기법으로 위험 시나리오를 도출하여 연료업무에 대한 많은 위험을 인식할 수 있었고, 재해경감활동계획 수립의 절차에 있어서 신뢰성을 담보하기 위하여 재해경감활동계획 수립절차를 표준화한 기업재난관리표준에 STPA기법을 위험 시나리오 도출 기법으로 도입하는 안을 제시한다.

이론적 배경

위험 시나리오 도출 방법 비교 및 문제점

위험평가 절차

기업재해경감활동계획 수립 기준에 의하면 위험평가 절차에 대하여 아래(Fig. 1)와 같이 정하고 있다.

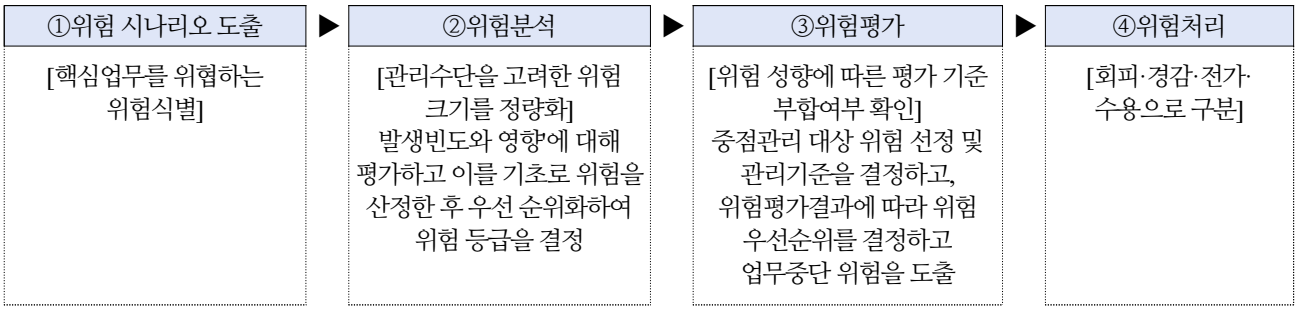

Fig. 1. Risk assessment procedure

위험 시나리오 도출에 관한 요구사항과 적용사례 비교

재해경감활동 관련 규범에 재해경감활동계획을 수립하는 절차로 위험 시나리오별 위험분석과 위험평가(Fig. 1)를 통하여 처리 우선순위를 정하도록 하고 있으나, 위험평가 첫 번째 단계인 위험 시나리오 도출 절차를 생략하거나, 관련자 브레인스토밍에 의하여 시나리오를 도출하는 등 핵심업무에 대한 시나리오 도출 절차가 각양각색이다.

Table 1의 A기관의 사례에 의하면 기업재난관리표준에서 정하고 있는 핵심업무에 대한 위험 시나리오 도출 절차는 생략하고, 핵심업무 지원을 위한 8대 소요자원(인적자원 등) 또는 재난 위험요인(자연재난, 사회적 재난)에 대한 위험 시나리오 도출을 통해 재해경감활동계획을 수립하였다.

Table 1. Application examples for corporate disaster management norm requirements

기업재난관리 규범(요구사항)	A기관/협력사(적용사례)
○ 기업재난관리표준(5.3) 프로세스, 시스템, 정보, 인력, 자산, 아웃소싱협력업체와 그들을 지원하는 자원운용에 있어 중단 위험을 식별 ○ 기업재해경감활동계획 수립 기준 (5.3) 핵심업무에 영향을 미치는 위험의 종류 식별 및 핵심업무를 유지하는 자원에 큰 피해를 미칠 가능성이 있는 위험요인(사회재난, 자연재난 등)식별 ○ 행안부 대행교재[1] (p290) 비전 및 전략과 프로세스 분석, 워크샵과 인터뷰, 손실사건 데이터 분석, 설문지 조사를 통해 위험요인 실현시 중단될 수 있는 핵심업무 위험 시나리오 도출	○ 핵심업무에 대한 위험 시나리오 도출절차는 생략하고, 위험요인에 대한 위험 시나리오 도출 ○ 핵심업무에 대하여 브레인스토밍에 의한 위험 시나리오 작성 →핵심업무 소요자원(8개) 기초로 중단시나리오 정의 →소요자원 시나리오별 위험평가 실시

재해경감활동계획 수립을 위한 위험 시나리오 도출 기법 표준화를 위하여 위험평가 기법의 특성을 검토한 결과(Table 2) 기존의 전통적 위험평가 기법은 현재의 시스템보다 규모가 작고 단순하며 하드웨어를 기반으로 동작하는 당시(1960~70년) 시스템의 특성을 반영하여 개발되었고, 특정 위험에 영향을 미치는 고장이나 오류를 찾아내거나 반대로 특정 고장이나 오류에 의해 발생 할 수 있는 위험 또는 사고를 밝혀 내는 것에 초점을 두고 있다. 최근 시스템들은 기능과 구성이 복잡해짐에 따라 사고의 발생 원인을 특정 컴포넌트나 기능의 문제로 규정하기 어려워졌다. 시스템의 복잡성으로 인해 시스템 내 문제의 결함를 식별하기가 어려울 뿐만 아니라, 시스템들 간 또는 시스템과 외부 요소들(사람, 정책, 환경 등) 간의 다양한 상호작용으로 시스템에 기능상 문제가 없다 할지라도 복합적인 요인에 의해 예기치 못한 사고가 발생할 수 있기 때문이다. 이에 기존의 전통적 위험평가 기법과는 다른 새로운 관점의 위험평가 방법이 필요하게 되었으며, 2012년에 STPA가 발표된 이래 항공 자동

차 등 안전 필수도메인을 중심으로 STPA에 대한 연구와 활용이 꾸준히 확산되고 있다(Ministry of Science and Technology Information and Communication, 2018).

Table 2. Review of characteristics by risk assessment technique

구분	전통적 위험평가 기법				시스템이론 기반 프로세스 분석
	FTA	ETA	FMEA	HAZOP	STPA
개발시기	1961년	1970년대	1949년	1970년대	2012년
평가방법	정량/정성적	정량/정성적	정량/정성적	정성적	정성적
위험식별	불가능	불가능	일부가능	가능	가능
특성	○ 하드웨어 기반 : 현재의 시스템보다 규모가 작고 단순하며, 하드웨어를 기반으로 동작하는 1960-70년도 당시 시스템의 특성에 적합 ○ 고장, 사고 분석 : 기술 기계적 고장이나 오류를 찾아내거나, 반대로 특정 고장이나 오류에 의해 발생 할 수 있는 위험 또는 사고를 밝혀 내는 것에 초점				○ 위험이 시스템과 시스템 또는 구성요소들 간 제어 문제에서 발생함을 기본전제로 하는 프로세스 분석 (시스템 : 하드웨어, 소프트웨어, 인력, 사회조직, 제도 등 다양한 요소로 구성)

출처 : Ministry of Science and Technology Information and Communication(2018)

STPA/STAMP

STAMP(System Theoretic Accident Model and Processes)는 시스템의 위험원인을 분석하기 위해 시스템 이론(System Theoretic Approach)을 적용한 모델이다. 시스템 이론은 이벤트 사이의 복잡한 관계를 분석하여 해당 이벤트가 왜 발생했는지를 파악할 수 있게 해주는 방법이다. STPA는 STAMP에 기반한 위험원인 분석 기법으로, 시스템 컴포넌트에 문제가 없더라도 컴포넌트간의 상호작용에 의해 사고가 발생할 수 있다는 점을 고려하여 위험원인을 도출한다.

STPA 기반 위험분석은 시스템을 제어 관계 관점에서 분석하고, 해당 제어 관계 중 위험을 유발할 수 있는 부적절한 제어를 식별하는 방식으로 이루어진다. 사고 정의에서 시작하여 원인 시나리오 도출을 수행하는 하향식 분석 체계를 가지며 크게 4단계(Fig. 2)로 구성된다.

Fig. 2. Risk scenario analysis system

선행연구

재난 예방 및 대비계획 수립절차 표준화를 통한 재난 예방활동 강화

발달된 기술을 적용한 데이터 및 기술기반 예측역량의 지속적인 발굴노력을 통한 재해경감활동이 우리가 나아가야 할 바람직한 재난관리활동이며(Kim et al., 2019), 과거의 경험이나 수집된 예측정보분석을 통하여 재난으로 발전될 수 있는 위험요인을 개선하기 위해 자원을 투입하는 등 재난의 예방·대비중심으로 재난관리 패러다임이 바뀌고(Ministry of Public Administration and Security, 2008) 있다.

재해에 광범위하게 노출되는 사후복구 중심의 전통적인 재난관리를 예측 및 관측기술로 예측·취약성평가·저감활동 등 프

로세스별 재해위험을 통합적으로 관리하는 재난의 예방·대비 중심으로 재난관리의 패러다임을 적극적으로 변화시키기 위하여 제시한 '재난 예방활동강화를 위한 재해경감활동관리체계 모델 제안(Kim et al., 2019)'에서 재난 예방 및 대비계획 수립절차를 표준화하여 기업재난관리표준에 추가할 것을 제시하고 있다.

선행연구에서 재난관리단계를 고려하는 종합적인 재난관리의 필요성과 재해경감활동계획 수립에 있어서 재난관리단계별 계획의 문서화 필요성 등이 연구되었지만, 후속연구로서 실효성 있는 재난관리단계별(예방·대비·대응·복구)계획 수립의 기초자료가 되는 핵심업무의 중단을 위협하는 위험 시나리오 도출 절차를 표준화하고자 하는 본 연구의 목적은 기존의 선행연구와는 차이점이 있다.

발전소 연료수급 업무에 대한 STPA 기반의 위험 시나리오 도출

발전업무구조도의 구성요소별 핵심업무 검토

발전소는 해외에서 수입한 연료를 사용하여 보일러에서 생산된 고온 고압의 수증기로 터빈을 돌려 전기를 생산하여 변전소로 송전한다. 발전설비는 Fig. 3과 같이 다양한 기술이 적용된 종합플랜트 설비로서 전기 생산 프로세스에 내재되어 있는 위험 시나리오 도출 작업의 체계적인 수행을 위해서는 기능별 구성요소(Block)를 정확하게 인식하여 업무구조도를 정의하는 것이 중요하다.

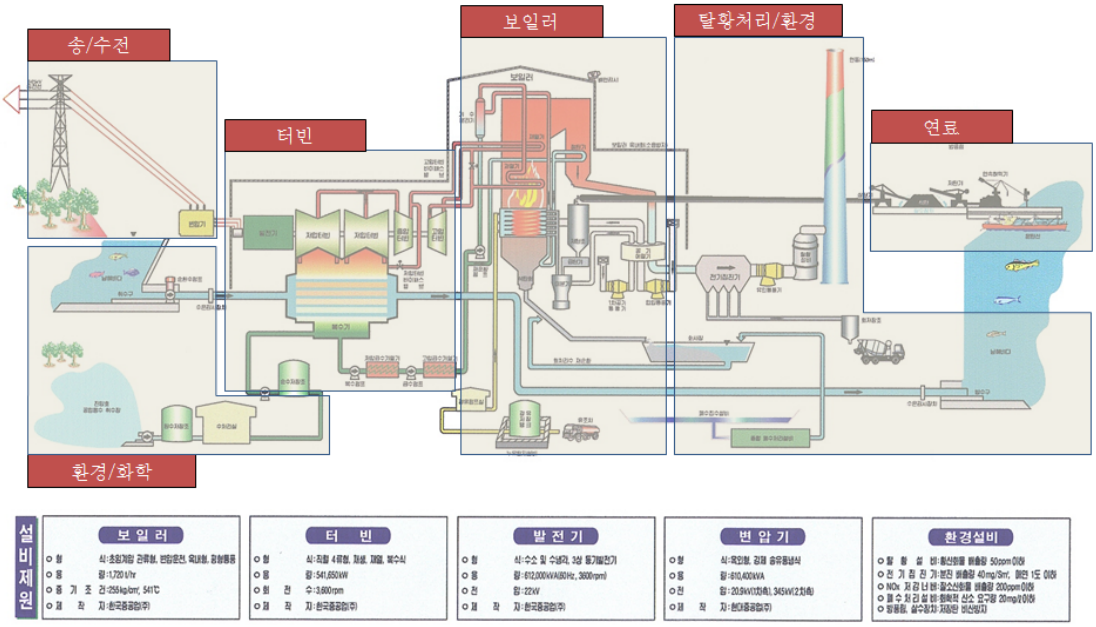

Fig. 3. Power generation business structure diagram

Fig. 3. 발전업무구조도는 전기를 생산하는 주요 구성요소를 구조화 한 것으로서, 업무영향분석(BIA)으로 도출된 핵심업무와 비교한 결과 일부 구성요소와 핵심업무가 불일치하는 부분이 존재한다. Table 3에 따르면 발전업무구조도의 구성요소에는 표기되지 않았으나 핵심업무에 포함된 '발전설비 운전조작'과 '전력거래' 요소는 발전업무 전체에 연관된 구성요소이

며, 업무구조도에 구성요소로 표기되어 있으며 업무중단에 영향을 끼치는 핵심적인 구성요소인 '연료'는 핵심업무 선정시 누락된 것으로 검토되었다.

Table 3. Contents of core business selection by component of the power generation business structure

구성요소	핵심업무(23)		위험 시나리오	
[발전설비 운전·조작]	Unit 기동·정지·출력 증·감발 운전조작	(1)		포괄적인 내용으로 Fig.3 발전업무구조도에서 누락
[전력거래]	전력거래운영	(1)		
[연료취급설비]	상탄 설비 운영	(1)		'연료' 구성요소에 포함
연료	[없음]	(0)	없음	핵심업무에서 누락
환경/화학	공업용수취수 계통 등	(3)		
보일러	보일러 설비 등	(6)		
환경	탈황 운영	(1)		
터빈	터빈 보조설비 등	(8)		
송/수전	송/수전 설비 관리 등	(2)		

A기관과 구내 상주 협력사의 위험 시나리오 도출 사례 비교

A기관 및 구내 상주협력사의 위험 시나리오 도출 사례를 검토한 결과(Table 4)에 의하면 A기관은 핵심업무를 위협하는 위험 시나리오 도출과정을 생략하고 브레인스토밍으로 도출된 5개 위험요인에 대한 재해경감활동계획을 수립하였으며, 협력사는 위험 시나리오를 도출하였으나 위험분석등 다음단계의 업무에 활용하지 않고 핵심업무에 소요되는 자원의 중단 시나리오에 대한 재해경감활동계획을 수립하였다.

Table 4. Examples of risk scenarios(Fig. 1. Apply 'classification' according to the risk assessment procedure)

구분	재해경감활동계획서 (A기관, 2018)	재해경감활동계획서 (A기관 협력사, 2019)
① 위험 시나리오 도출	(보고서 없음)	- 구성원 브레인스토밍에 의한 중단 위험 시나리오(203개) 를 도출하고, 위험지수(발생빈도, 영향력, 위험점수)로 처리 필요한 위험 시나리오 38개 도출
(위험 요소 식별)	- 자연재난(10)인적재난(8) 사회재난(4) 기타재난(3) ※ 국내외 위험분류 자료 참조하고, 설문조사(브레인스토밍)	- 태풍/강풍, 홍수, 지진, 산사태, 화재/폭발, 붕괴, 유틸리티중단, 파업, 전염병, 기계고장, 부도, 컴퓨터 바이러스 등 ※ 국내외 위험분류 자료 참조하고, 설문조사(브레인스토밍)
② 위험 분석	- 화재, 극한, 오조작, 태풍, 지진 등 5개 중점관리대상 위험요소 선정 ※ 위험특성(발생확률, 평균대응기간), 주요영향(업무마비기간, 예측가능기간, 영향범위), 영향평가(인적피해, 재난피해)에 대하여 구성원 설문 시행	- 8대 업무(인력, 차량 및 수송, 정보 및데어터, ICT시스템, 건물, 유틸리티, 설비/장비/소모품, 협력업체.공급업체) 중단 시나리오와 위험요소 Mapping → 8대 업무 중단시나리오와 핵심업무(161개) 소요자원과 Mapping
③ 위험평가	-재난발생빈도×위험크기= 상중하로 우선순위 결정	- 재난발생빈도×위험크기= 상중하로 우선순위 결정

본 연구는 위험평가 절차에 해당하는 위험 시나리오 도출 절차를 시행하지 않고 있는 A기관의 전력생산과정을 구조화한 발전업무구조도에서 업무중단에 중요한 영향을 끼치는 구성요소이나 핵심업무로 선정되지 않은 연료업무에 대하여

STPA(System Theoretic Process Analysis)기법을 적용하여 위험 시나리오를 도출하고, 재해경감활동관리계획 수립절차를 표준화한 기업재난관리표준에 STPA기법을 위험 시나리오 도출기법으로 도입하는 방안을 제안한다. 이는 재해경감활동계획 수립의 기초자료가 되는 위험 시나리오 도입절차가 중요하여 기업재난관리표준에 위험 시나리오 도출방법을 반영하도록 개정하는 것이 필요하기 때문이다.

연료수급업무에 대한 위험 시나리오 도출

사고 및 위험 정의

○ 사고 정의

시스템에 발생할 수 있는 사고를 정의한다. 사고종류로는 인명손실 또는 부상, 재산손실, 환경오염 뿐만 아니라 중요 정보 손실 또는 유출, 목표 달성 실패, 명성 손실 등 통제할 수 없는 요인을 포함 할 수 있다. Table 5의 사고정의에 있어서 시스템 이해관계자들은 분석하고자 하는 사고 범위를 정의해야 하며, 해당 사고는 추적이 용이하도록 ID를 부여한다(Ministry of Science and TechnologyInformation and Communication, 2018).

Table 5. Definition of possible incidents

구분		내용
사고 (Accident)	A1	전기 생산 중단
	A2	환경오염
	A3	과다한 체선료 발생 손실
	A4	불법사건 연루로 회사 이미지 훼손

○ 시스템 수준 위험 정의

위험분석을 위해서는 먼저 대상 시스템을 선정하고 시스템 범위를 정의할 필요가 있다. 시스템 범위는 설계나 운영관리 등을 통해 제어(Control)가 가능한 부분을 범위로 정의하는 것이 좋다. 제어가 불가능한 부분을 위험분석 범위에 포함하면 관리할 수 있는 수단을 사실상 마련할 수 없기 때문이다. 위험분석 대상범위를 정의한 후에는 위험을 정의한다. Table 6의 위험 정의는 사고를 일으킬 수 있는 시스템 상태 및 조건을 식별하는 것을 의미한다(Ministry of Science and Technology Information andCommunication, 2018).

Table 6. Risk definition

구분		내용	관련사고
위험 (Hazard)	H1	광산지역 기후이변(태풍 등) 발생	A1
	H2	해상 선박화물(유연탄 등) 화재 발생	A1.A2
	H3	해상 기후이변으로 기일내 수송 불가	A1
	H4	하역 항만 사고 및 노조파업	A1.A2.A3
	H5	마약류 밀반입 등 불법사건 연루	A3.A4

○ 시스템 수준 안전 제약사항(Safety constraints) 도출

Fig. 4의 시스템 수준 안전 제약사항은 Table 6 '위험정의'에서 정의한 위험과 대응되는 개념으로서 사고나 손실을 막기 위한 시스템의 상태유지 및 실행해야 함을 의미한다.

Accident Hazard Safety Constraint Table / Accident Hazard Safety Constraint Table

A...	Accident	H...	Hazard	Saf...	Safety Constraint
A1	전기 생산 중단	H1	광산지역 기후이변(태풍 등) 발생	SC1	광산지역 기후 상황을 감안한 납품 일정 설정
A1	전기 생산 중단	H2	해상 선박화물(유연탄 등) 화재 발생	SC2	유연탄 자연발화 예방 기술이 적용된 선박 배선
A1	전기 생산 중단	H3	해상 기후이변으로 기일 내 수송 불가	SC3	수송로 기후 상황을 감안한 수송 일정 설정
A1	전기 생산 중단	H4	하역 항만 사고 및 노조 파업	SC4	타 발전사 협약 체결을 통한 대체 항만 확보
A2	환경오염	H5	해상 선박화물(유연탄 등) 화재 발생	SC5	유연탄 자연발화 예방 기술이 적용된 선박 배선
A2	환경오염	H6	하역 항만 사고 및 노조 파업	SC6	타 발전사 협약 체결을 통한 대체 항만 확보
A3	과다한 체선료 발생 손실	H7	하역 항만 사고 및 노조 파업	SC7	타 발전사 협약 체결을 통한 대체 항만 확보
A3	과다한 체선료 발생 손실	H8	마약류 밀반입 등 불법 사건 연루	SC8	불법사건 차단을 위한 유관기관 공조 및 선원 교육,선적과정 모니터링 강화
A4	불법사건 연루로 회사 이미지 훼손	H9	마약류 밀반입 등 불법 사건 연루	SC9	불법사건 차단을 위한 유관기관 공조 및 선원 교육,선적과정 모니터링 강화

Fig. 4. Derivation of system-level safety constraints

제어구조도 정의

제어구조도는 Control loop 형태를 띠며 제어의 관점으로 주체(Controller)와 객체(Controlled Process) 그리고 제어(Control Action)와 반응(Feedback)으로 구성된다(Ministry of Science and Technology Information and Communication, 2018).

'Fig. 5. 연료수급 제어구조도'의 하위 구성요소(Component)인 공급업체에 대하여 제어구조도(Fig. 6)를 구현해 보았는데 하위 계층의 구성요소(Component) 뿐만 아니라 모든분야의 업무절차에 대한 각각의 제어구조도를 정의할 수 있다.

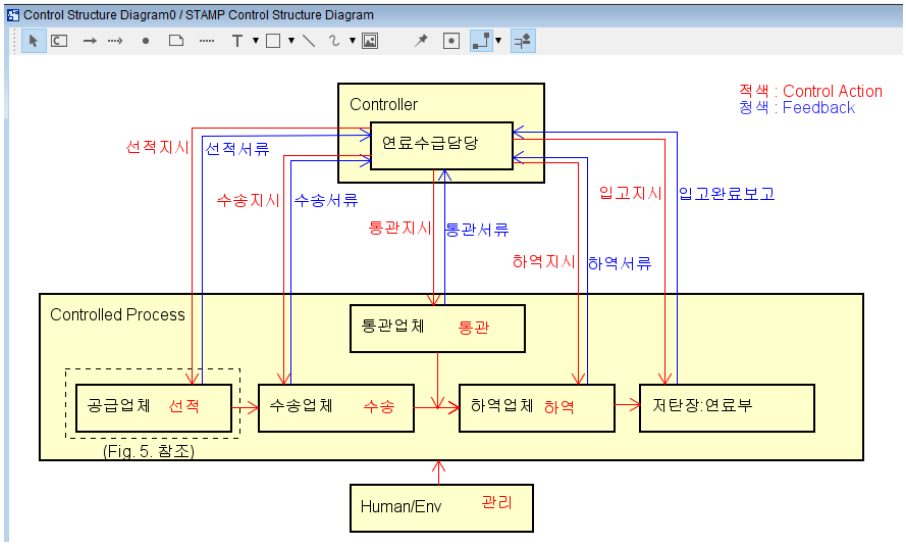

Fig. 5. Fuel supply and demand control structure diagram

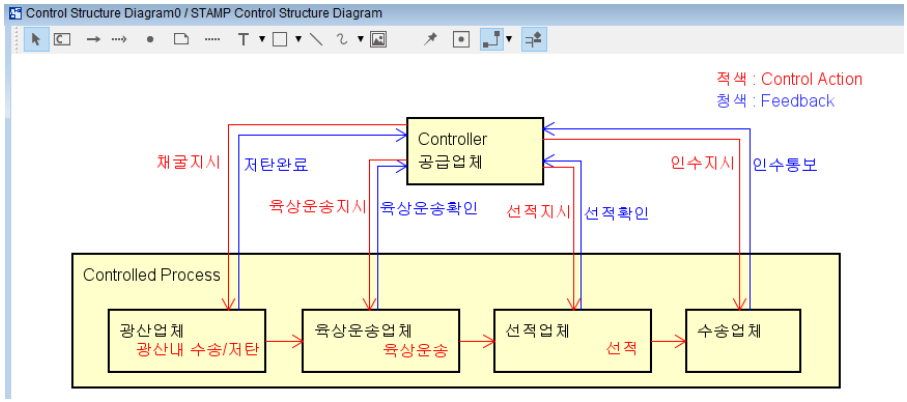

Fig. 6. Supplier's control structure diagram

Unsafe Control Action 도출

제어구조도에서 식별한 Control Action인 계약의 이행을 지시하는 선적/수송/하역/통관지시와 관련된 UCA를 식별하는 단계이다. Table 7의 CA에 대한 ① 계약조건 불 이행 ② 계약조건 이행 ③ 계약이행을 너무 늦게 또는 일찍 이행 ④ 계약이행을 부족하게 또는 과다하게 이행과 같이 4가지 유형에 따라 위험을 식별한다(Ministry of Science and Technology Information and Communication, 2018).

Table 7. Unsafe Control Action

No	CA	Not Providing	Providing causes hazard	Too early/Too late	Stop too soon / Applying too long
1	선적지시	(UCA2-N-1) 미선적 [SC1][SC3]	해당없음	(UCA2-T-1) 선적지연 [SC1][SC3]	해당없음
2	수송지시	(UCA4-N-1) 수송실패 [SC2][SC3][SC5]	해당없음	(UCA4-T-1) 수송지연 [SC2][SC3][SC5]	해당없음
3	통관지시	(UCA6-N-1) 통관실패 [SC8][SC9]	해당없음	(UCA6-T-1) 통관지연 [SC8]	해당없음
4	하역지시	(UCA8-N-1) 하역불가 [SC4][SC6][SC7]	해당없음	(UCA8-T-1) 하역지연 [SC4][SC6][SC7]	해당없음

HCF(Hazard Casual Factor) 식별

UCA(Table 7)를 유발할 수 있는 위험원인요소를 식별한다. Table 8의 HCF는 위험원인요소이며, Hint Word는 위험원인요소별로 15가지 유형으로 구분되고, 해당 요소로 인해 고려해볼 수 있는 시나리오를 정리하였다.

Table 8. Risk scenario by risk factor

ID	HCF	Hint Word	Scenario
HCF2-N-1-1	광산지역 기후이변(우기, 폭우, 싸이클론)으로 광산 및 운송로 침수	(10)	광산 및 운송로 침수로 수송 불가
HCF2-N-1-2	석탄운송로 철도사고	(10)	철도사고로 수송 불가

Table 8. Risk scenario by risk factor (Continue)

ID	HCF	Hint Word	Scenario
HCF2-T-1-1	광산지역 기후이변(우기, 폭우, 싸이클론)으로 광산 및 운송로 침수	(10)	광산 및 운송로 침수로 육상운송이 늦어져 선적 지연
HCF2-T-1-2	석탄 운송로 철도사고	(10)	철도사고로 육상운송이 늦어져 선적 지연
HCF4-T-1-1	해상 기후이변으로 선박 정상운행 불가	(10)	해상 기후이변으로 수송 지연
HCF8-T-1-1	항만 시설 고장(경미한 고장)	(10)	항만시설 수리기간 동안 하역 지연
HCF8-T-1-2	항만 이상기후(고파랑 등)	(10)	항만 해역 고파랑으로 하역 지연
HCF8-T-1-3	항만 조노 파업	(10)	항만노조 파업으로 하역 지연
HCF4-N-1-1	해상 선박 화재 발생	(8)	해상선박화재로 선적화물(유연탄등) 소실
HCF4-N-1-2	선박침몰	(8)	선적화물(석탄) 침몰
HCF6-N-1-1	원산지 위조	(12)	원산지 위조로 통관거절(북한산 석탄)
HCF6-T-1-1	마약류 밀반입 연류	(8)	불법사건 연류로 통관 보류
HCF8-N-1-1	항만시설 소손 및 중대한 고장	(10)	항만시설 사용 불가로 일정기간 하역 불가
HCF8-N-1-2	항만 노조 장기 파업	(10)	항만노조 장기파업으로 하역 불가

※ (8)부적절하거나 비효율적이거나 누락된 제어 조치. (10)미확인 또는 범위를 벗어난 소동. (12)부적절한 actuator 작업

대책(Countermeasure)

발전업무구조도에 구성요소로 표기되어 있고 업무중단에 영향을 끼치는 핵심적인 구성요소임에도 재해경감활동계획 수립을 위한 핵심업무 선정에서 누락된 '연료'수급업무에 대하여 위험 시나리오 도출 절차를 진행한 결과 Fig. 7에 따르면 전기

Countermeasure Table / Countermeasure Table

HC...	HCF	...	Countermeasure	UCA	Co...	...
HCF2-N-1-1	광산지역 기후이변(우기, 폭우, 싸이클론)으로 광산 및 운송로 침수	M1	1. 선적 개시노력 촉구(TO. 미선적 공급사) 또는 선적가능한 대체탄 선적 방안 협의 2.타 계약물량 선적일정 조정(TO.타 공급사) 또는 근거리탄 긴급 구매 3. 선적일정 조정하여 배선 조치지시(TO.수송선사) 4. 유사탄종 물량 교환(swap) 를 통한 재고 선 확보 및 추후 반환 협의 추진(TO.타 발전사) 5. 발전소 : 탄종 혼소율 조정 및 연소 대응방안 협의로 비축재고 사용 최적화	(UCA2-N-1) 미선적 [SC1][SC3]	연료 수급 담당	
HCF2-N-1-1	광산지역 기후이변(우기, 폭우, 싸이클론)으로 광산 및 운송로 침수	M2	빠른 복구 및 선적 개시노력 및 선적가능한 대체탄 선적 방안 강구	(UCA2-N-1) 미선적 [SC1][SC3]	공급 업체	
HCF2-N-1-2	석탄운송로 철도사고	M1	1. 선적 개시노력 촉구(TO. 미선적 공급사) 또는 선적가능한 대체탄 선적 방안 협의 2.타 계약물량 선적일정 조정(TO.타 공급사) 또는 근거리탄 긴급 구매 3. 선적일정 조정하여 배선 조치지시(TO.수송선사) 4. 유사탄종 물량 교환(swap) 를 통한 재고 선 확보 및 추후 반환 협의 추진(TO.타 발전사) 5. 발전소 : 탄종 혼소율 조정 및 연소 대응방안 협의로 비축재고 사용 최적화	(UCA2-N-1) 미선적 [SC1][SC3]	연료 수급 담당	
HCF2-N-1-2	석탄운송로 철도사고	M2	빠른 복구 및 선적 개시노력 및 선적가능한 대체탄 선적 방안 강구	(UCA2-N-1) 미선적 [SC1][SC3]	공급 업체	
HCF2-T-1-1	광산지역 기후이변(우기, 폭우, 싸이클론)으로 광산 및 운송로 침수	M3	1. 선적지연 해결노력 협의 및 선적지연 예상기간 및 발전 정지 영향 파악(TO.공급사) 2. 타 발전사와 물량교환 또는 필요시 긴급구매	(UCA2-T-1) 선적지연 [SC1][SC3]	연료 수급 담당	

※ 14개의 HCF에서 18개의 Countermeasure를 도출할 수 있었다.

Fig. 7. Countermeasures against risk factors

생산중단·환경오염 등의 사고로 이어질 수 있는 14개의 위험원인요소에 의한 14개의 위험 시나리오를 도출하고 그에 대한 18개의 대책(Fig. 1의 ④위험 처리)을 수립할 수 있었다.

A기관 연료수급업무에 대한 위험 시나리오 도출에 STPA 기법 적용 결과 분석

업무구조도 정의를 통하여 위험 시나리오 도출 대상인 핵심업무의 적정 선정

전력 생산 중단에 중요한 영향을 끼치는 구성요소중에서 핵심업무에서 누락된 연료수급업무에 대하여 위험 시나리오 도출절차를 진행한 결과 4개의 '발생가능한 사고'가 정의 되었고, 5개의 '시스템 수준의 위험'이 정의되는 등 연료수급업무가 발전업무의 연속성확보를 위한 중요한 구성요소임을 확인할 수 있었다.

Fig. 3과 같이 다양한 기술이 적용되는 전기 생산 프로세스에 내재되어 있는 위험 시나리오 도출 작업의 체계적인 수행을 위해서는 기능별 구성요소(Block)를 정확하게 인식하여 '업무구조도를 정의'하는 절차가 위험 시나리오 도출 대상인 핵심업무 누락을 최소화하는 중요한 절차가 됨을 확인하는 기회가 되었다.

위험 시나리오는 재난관리 단계별 계획 작성의 기초자료로 활용

본 연구는 위험 시나리오 도출을 위해 STPA기법을 적용하여 'Fig. 2. 위험 시나리오 분석 체계'에서 정하는 순서에 따라 위험 분석 절차를 진행함으로서 업무연속성 확보에 영향을 주는 위험요소 누락을 최소화 할 수 있는 위험평가 절차를 정립해 나갈 수 있는 방법을 제시하고 있다.

재해경감활동계획은 경영현황과 업무영향분석을 통해 핵심업무를 도출하고 핵심업무의 중단 위험에 대한 위험평가 결과를 반영하여 수립되는데, 연료수급업무에 대한 위험평가의 첫 번째 절차인 핵심업무의 중단을 위협하는 위험 시나리오 도출에 시스템 이론 기반의 STPA 기법(사고정의·위험정의·제어구조도 정의·불안전한 제어행위·위험원인요소 정의)에 의한 시나리오 도출 절차를 적용하여 14개의 위험 시나리오를 도출할 수 있었고 18개의 대책을 강구할 수 있었다(Table 8, Fig. 7).

적합하게 도출된 위험 시나리오에 대한 위험평가 결과는 선행연구인 '재난 예방활동강화를 위한 재해경감활동관리체계 모델(Kim et al., 2019)'에서 제안한 재난관리 단계별(예방·대비·대응·복구) 재해경감활동계획의 기초자료로 활용되어 실효성 있는 계획 수립에 기여할 수 있을 것으로 기대된다.

결 론

재해경감활동계획 수립 절차를 정하고 있는 기업재난관리표준과 기업재해경감활동계획 수립 기준, 기업재난관리사 교재(대행분야, 행정안전부)를 분석한 결과 위험요인 실현시 중단될 수 있는 핵심업무에 대한 위험 시나리오를 도출하도록 규정하고 있으나, 구체적인 방법이나 프로세스에 대하여 정하지 않고 있어, 시스템 이론에 기반한 STPA 기법을 재해경감활동계획 수립을 위한 위험 시나리오 도출 기법으로 기업재난관리표준에 반영할 것을 제안하였다.

기존의 기업재난관리 제반 규범과 A기관/협력사의 사례, 전통적인 위험평가기법, 최근에 MIT공대에서 개발하여 확산되고 있는 STPA기법을 비교 분석하였으며, STPA기법을 A기관 연료수급업무에 적용한 결과 ①업무구조도를 통하여 업무중단에 영향을 끼치는 핵심업무를 확인 할 수 있었고, ②구체적으로 정의된 제어구조도를 바탕으로 핵심업무를 위협하는 많은

위험을 식별할 수 있었으며, ③위험이 왜 발생하게 되었는지에 대한 위험원인요소 및 위험 시나리오를 더 구체적으로 도출할 수 있었다.

핵심업무를 위협하는 위험 시나리오 도출은 재해경감활동계획 수립에 있어서 가장 기초적이고 필수 절차에 해당하므로 STPA기법과 같이 시스템에 의하여 위험 시나리오를 도출하는 방안을 도입하여 표준화하고 지속적으로 유지 개선해 나가야 할 것이다.

References

[1] 'A' Institution (2018). Disaster Reduction Activity Plan, Busan.

[2] Criteria for establishing corporate disaster reduction activity plans (Ministry of Public Administration and Security note No.2014-83)

[3] Enterprise Disaster Management Standard (Ministry of Public Administration and Security note No.2017-1)

[4] Kim, S.D., Kim, C.S. (2019). "A proposal of the disaster mitigation activity management system model for strengthen disaster prevention activities." Journal of the Society of Disaster Information, Vol. 15, No. 4, pp. 502-513.

[5] Ministry of Science and Technology Information and Communication (2018). Guide to risk analysis using STPA. Seoul, Korea.

[6] Ministry of Public Administration and Security. Disaster Relief activity practical teaching material, Seoul.

[7] Ministry of Public Administration and Security (2008). A Study on Functional Enhancement of the National Security Planning, Seoul.

[8] Nancy G. Leveson, John P. Thomas. (2018). STPA HANDBOOK. Boston. USA.

[9] Partner of Agency 'A' Institution. (2018). Disaster Reduction Activity Plan, Busan.

[10] Power Plant Cooperation Headquarters (2016). Fuel Business Manual.

[11] STAMP WORKBENCH : https://www.ipa.go.jp/english/sec/reports/20180330.html