

STAMP/STPA기반 하나로 연구용원자로 운영 프로세스 모델링 및 평가

Operational Process Modelling and Analysis for HANARO Research
Reactor based on STAMP/STPA

KAERI

Korea
Atomic Energy
Research Institute



한국원자력연구원
Korea Atomic Energy Research Institute



제 출 문

한국원자력연구원장 귀하

이 보고서를 2020년도 “원자력시스템 리스크 안전 목표 최적 평가/관리 기술개발” 과제 세부과제 “원자력 신형 안전시스템 리스크 평가 기반기술 개발”의 기술보고서로 제출합니다.

2020년 6월 2일

과제명 : 원자력 신형 안전시스템 리스크 평가 기반기술 개발

주 저 자 이상훈
공 저 자 신성민
박진균



요 약 문

I. 제 목

STAMP/STPA기반 하나로 연구용원자로 운영 프로세스 모델링 및 평가

II. 연구개발의 목적 및 필요성

하나로는 1995년 첫 임계에 도달한 이후로 핵연료 및 재료의 조사 실험, 동위원소 생산, 중성자 빔을 이용한 연구 및 분석에 이용되고 있다. 하지만 최근 연구용 원자로 관련 규제가 강화되면서 본 규제를 만족하기 위한 장기간의 재가동 준비, 엄격해진 불시정지 조건에 따라 불시정지 빈도가 높아지면서 운영률이 감소하였다. 본 연구에서는 하나로의 안정적 운영과 활용을 위한 불필요한 불시정지를 최소화하기 위해 STAMP/STPA(System Theoretic Accident Model and Process/Systems-Theoretic Process Analysis) 방법론에 기반하여 하나로 연구용원자로의 운영 프로세스를 모델링하고 원자로 불시정지 유발 Unsafe Control Action(UCA)을 도출하여 향후 원자로 불시정지 최소화에 활용될 수 있는 기초자료를 개발하고자 한다.

III. 연구개발의 내용 및 범위

본 연구에서는 최근 10년간 연도별 불시정지 현황을 바탕으로 원자로 불시정지를 많이 발생시켰던 냉중성자원(CNS, Cold Neutron Source) 계통을 하나로 불시정지 시범 분석 대상으로 선정하였다. CNS계통으로 인한 하나로 불시정지는 CNS 수소계통 고압력 또는 저압력 신호로 인해 발생하므로 CNS계통의 운영 프로세스 모델링은 이 두 불시정지 신호의 발생을 유발하는 상황 및 조건을 분석 범위로 한다. 본 연구에서 수행된 STPA 분석절차는 1) 계통 친숙화, 2) 계통 운영 자료 분석, 3) 계통 STPA모델 개발, 4) 계통 UCA 도출 및 검토의 과정에 따라 수행되었다.

IV. 연구개발결과

본 연구에서는 CNS계통에 대해 개발된 STPA모델(Control Structure)을 토대로 운전원의 수동 운전 혹은 조작 및 제어컴퓨터의 자동 운전이 요구되는 수소계통, 진공계통, 원자로제어계통에 대해 UCA분석을 수행하였으며, 각 계통에 정의된 총 51개의 Control

Action 목록에 대해 총 127개의 UCA들이 도출되었다. 도출된 UCA의 타당성을 평가하기 위해 각 UCA들에 대해 하나로 운전원 및 전문가 자문을 통해 평가지표에 따른 검토를 수행하였으며 실제 하나로 불시정지 사례들과의 비교분석을 수행하였다. 도출된 UCA를 기존의 정지 이력을 비교하여 본 결과, 1건의 원자로 불시정지 사례가 STPA결과를 통해 파악된 UCA와 일치하는 것으로 확인되었다.

V. 연구개발결과의 활용계획

본 연구에서 STPA 방법론을 통해 도출된 UCA는 시스템 비정상적인 행위를 포함하여 운전절차서, 인적 오류에 이르는 운전원 관련 위험요인들을 모델에 포함하여 분석할 수 있어, 원자로 안전성 분석뿐만 아니라 재가동을 위한 기초분석자료 용도로도 활용할 수 있을 것으로 기대된다.

본 연구에서는 UCA 도출까지를 분석범위로 설정하였는데, 더 나아가 각 UCA 발생원인(Causal Factor Analysis)을 추가적으로 분석할 시 보다 체계적인 보완요건을 도출할 수 있을 것이다. 이를 위해 본 분석에서 수행된 STPA 분석절차 및 결과물은 FMEA와 상호보완적으로 연계될 수 있다. STPA는 기계적 요소와 더불어 인적오류에 이르는 제어 신호의 이상특성을 다양하게 정의하고 그 이상신호가 전체시스템에 전파되는 과정을 체계적으로 분석하게 된다. 이후 보다 안전한 시스템 및 대응체계 구축을 위해 이상신호 발생의 원인을 파악할 필요가 있는데, 중요 UCA로 평가된 항목들의 발생원인 파악에 FMEA 결과가 활용될 수 있다. 또한, 기존의 Control Structure에 추가적인 요소들(현장 운전원, 운전원간 지시체계 등)을 모델링 할 시, 더 구체적이고 포괄적인 운영 프로세스 분석이 가능할 것으로 기대된다.

SUMMARY

I. Project Title

Operational Process Modelling and Analysis for HANARO Research Reactor based on STAMP/STPA

II. Objective and Importance of the Project

After HANARO research reactor reached first criticality at 1995, it has been used for various research purposes such as nuclear fuel and material testing, isotope production, neutron beam research. However, its operation rate has been reduced as it experiences frequent spurious trip and long overhaul to meet enhanced regulatory requirements. In this research, in order to minimize the unnecessary spurious trip for the safe operation of HANARO research reactor, the operational process of HANARO reactor is modelled based on STAMP/STPA(System Theoretic Accident Model and Process/Systems-Theoretic Process Analysis) framework and the unsafe scenarios which could cause spurious reactor trip are derived.

III. Scope and Contents of Project

Based on the yearly reactor trip statistics, the cold neutron source(CNS) system which caused most of the spurious reactor trip during last decade was selected as a pilot system. Since spurious reactor trip due to CNS system is caused by the CNS hydrogen system high pressure or low pressure trip signals, the scope of this research is limited to deriving the unsafe scenario which may cause these trip signals. The analysis steps conducted in this research include 1) system familiarization, 2) Review on documentations regarding system operation, 3) system STPA model development, 4) system unsafe control action(UCA) analysis.

IV. Result of Project

In this research, the control structure for CNS system is developed and UCAs for

hydrogen system, vacuum system, and reactor control system are derived which requires automatic operation by control computer or manual operation or intervention by human operator in HANARO main control room(MCR). As a result, 127 UCAs are derived for 51 control actions in control structure of CNS system. To demonstrate the effectiveness of the proposed framework, the derived UCAs were compared with the actual spurious trip causal analysis reports. As a result, all reactor trip histories were included in the derived UCAs. The UCA result can be coupled with the failure mode and effect analysis(FMEA) where the root cause of UCAs can be found using FMEA process and results.

V. Proposal for Applications

The proposed framework enables the analysis on the human operator related hazards regarding the operation procedure and human error, so the result can be used not only for system safety analysis but also the basis for reducing the overhaul period of HANARO research reactor.

Although the scope of this study is limited to UCA analysis for CNS system, by conducting the causal factor analysis utilizing FMEA result, the improvements for the components having high risk potentials can be systematically derived and implemented. In addition, if the operator modeling of the current version of control structure for CNS system is improved by introducing various information (tasks of field operator, operators' command line), more detailed operation process and hazard analysis can be conducted.

CONTENTS

SUMMARY	5
 Chapter 1. Introduction	15
Section 1. Research Background and Necessity	17
Section 2. Research Purpose	18
Section 3. Research Scope	19
Section 4. Contents Configuration	19
 Chapter 2. STAMP/STPA Overview	21
Section 1. Theoretical Basis	23
1. System Theory	23
2. STAMP Concept Understanding	26
Section 2. STPA Analysis Method	27
1. STPA Concept	27
2. STPA Analysis Procedures	27
A. Accident/Hazard Definition	28
B. Control Structure Schematization	28
C. Unsafe Control Action Derivation	31
D. Causal Scenario Derivation	32
Section 3. Nuclear Domain Applications	33
1. USA Darlington NPP Reactor Protection System	35
2. Digital I&C System for MSIV Control	38
 Chapter 3. HANARO Operational Process Modeling	43
Section 1. Analysis Steps	45
Section 2. System Familiarization	46
1. Hydrogen System	47
2. Vacuum System	49
3. Helium Refrigeration System	50
4. Gas Blanket System	52

5. Cooling Water System	54
6. Air Compression System	56
7. Instrumentation and Control System	57
Section 3. Review on System Operation Procedures	59
Section 4. System STPA Model Development	68
1. Accident/Hazard Definition	68
2. Control Structure Development	70
Section 5. System UCA Derivation and Review	83
1. System UCA Derivation	83
2. UCA Importance Analysis based on expert elicitation	110
 Chapter 4. HANARO Operational Process Analysis	 123
Section 1. Comparison study with HANARO Reactor Trip Record	125
Section 2. Coupling with FMEA Results of CNS System	127
 Chapter 5. Conclusion	 129
 Chapter 6. References	 133
 Appendix	 137
[Appendix 1] Introduction and Manual for RMStudio	139
 BIBLIOGRAPHIC INFORMATION SHEET	 156

목 차

요약문	3
제1장 서론	15
제1절 연구 배경 및 필요성	17
제2절 연구 목적 및 범위	18
제3절 연구 방법론	19
제4절 내용 구성	19
제2장 STAMP/STPA 개요	21
제1절 방법론의 이론적 기초	23
1. 시스템 이론	23
2. STAMP 개념 이해	26
제2절 STPA 분석 방법론	27
1. STPA 개념	27
2. STPA 분석 절차	27
가. 사고 및 위험 정의	28
나. Control Structure 도식화	28
다. Unsafe Control Action 도출	31
라. Causal Scenario 도출	32
제3절 원자력 분야 STPA 적용 사례	33
1. 미국 Darlington 원전 원자로정지계통 분석 사례	35
2. 원전 디지털보호계통 안전성 분석 사례	38
제3장 하나로 운영 프로세스 모델링	43
제1절 분석 절차	45
제2절 계통 친숙화	46
1. 수소계통	47
2. 진공계통	49
3. 헬륨냉동계통	50
4. 가스블랭킷계통	52

5. 냉각수계통	54
6. 압축공기계통	56
7. 계측제어계통	57
제3절 계통 운영 자료 분석	59
제4절 계통 STPA모델 개발	68
1. 사고 및 위험 정의	68
2. Control Structure 개발	70
제5절 계통 UCA 도출 및 검토	83
1. 계통 UCA 도출	83
2. 전문가 자문을 통한 UCA 중요도 분석	110
제4장 하나로 운영 프로세스 평가	123
제1절 하나로 정지이력 비교분석	125
제2절 CNS계통 FMEA결과와의 연계	127
제5장 결론	129
제6장 참고문헌	133
부 록	137
[부록 1] RMStudio 프로그램 소개 및 사용법	139
서지정보양식	155

표 목차

표 1. 하나로 불시정지 현황 (2010~2019년)	18
표 2. Control Structure의 구성 요소	29
표 3. 위험을 유발할 수 있는 UCA의 4가지 전형적인 유형	31
표 4. 안전 분야에서의 STPA 적용 현황	34
표 5. High LogN Power 트립 관련 UCA 도출 예시	36
표 6. Darlington SDS의 UCA-1에 대한 원인 분석	37
표 7. 원전에서 발생할 수 있는 사고 및 위험 정의	39
표 8. ESF-CCS SIAS 개시신호의 UCA 분석 결과	40
표 9. 공정계통 비정상상태에 의한 원자로 정지변수	58
표 10. 하나로 CNS계통 운전절차서 목록	59
표 11. 하나로 CNS-진공계통 운전절차서 분석 결과	61
표 12. 하나로 CNS계통 관련 운전원 및 제어컴퓨터 운전절차 목록	63
표 13. 하나로 CNS계통 관련사고 및 위험 목록 정의	69
표 14. Control Structure내 CNS계통간의 제어(Control Action) 목록	70
표 15. Control Structure내 CNS계통간의 반응(Feedback) 목록	75
표 16. CNS계통 UCA 분석 결과 예제	84
표 17. 전문가 검토 결과 평가지표 O로 평가된 UCA 목록	111
표 18. 전문가 검토 결과 평가지표 X로 평가된 UCA 목록	112
표 19. 하나로 CNS계통 STPA모델 결과와 정지이력의 비교분석	126
표 20. CNS 진공계통 FMEA분석 결과 예제	128

그림 목차

그림 1. 연도별 하나로 운전일수 및 불시정지횟수	17
그림 2. 해석적 분해(좌) 및 시스템 이론(우)에 기반한 접근의 차이	25
그림 3. 기존 위험분석 기법과 STPA의 연관성 및 차이점	25
그림 4. STAMP/STPA 분석 절차	28
그림 5. 제어 루프의 일반적 구성	29
그림 6. 다양한 형태의 Control Structure	30
그림 7. Causal Scenario 유형	32
그림 8. Darlington SDS Control Structure - 운전원(좌) 및 시스템(우)	35
그림 9. 공학적안전설비-기기제어계통(ESF-CCS) 구성도	38
그림 10. ESF-CCS를 포함한 원자로보호계통의 Control Structure	39
그림 11. ESF-CCS의 UCA-1에 대한 원인 분석 결과	41
그림 12. 하나로 원자로 불시정지 STPA 분석 절차	45
그림 13. 하나로 CNS 공정계통 흐름도	47
그림 14. 하나로 CNS-수소계통 계통도	48
그림 15. 하나로 CNS-진공계통 계통도	49
그림 16. 하나로 CNS-헬륨냉동계통(냉동박스) 계통도	51
그림 17. 하나로 CNS-헬륨냉동계통(헬륨압축기) 계통도	51
그림 18. 하나로 CNS-가스블랭킷계통(질소 블랭킷) 계통도	53
그림 19. 하나로 CNS-가스블랭킷계통(헬륨 블랭킷) 계통도	53
그림 20. 하나로 CNS-냉각수 계통(1차 순환계통) 계통도	55
그림 21. 하나로 CNS-냉각수 계통(2차 순환계통) 계통도	55
그림 22. 하나로 CNS-압축공기계통 계통도	56
그림 23. 하나로 CNS-계측제어계통 구성도	58
그림 24. 하나로 CNS계통 관련 사고-위험간 관계 정의	70
그림 25. 하나로 CNS계통 Control Structure	82
그림 부록 1-1. RMStudio STPA 프로젝트 생성	140
그림 부록 1-2. RMStudio STPA 프로젝트 실행	140
그림 부록 1-3. RMStudio STPA 프로젝트 이름 및 설명 설정	141
그림 부록 1-4. RMStudio Models 탭	142
그림 부록 1-5. RMStudio Control Structure 모델링	143

그림 부록 1-6. RMStudio Control Structure 개발 예시	143
그림 부록 1-7. RMStudio Analysis 탭	144
그림 부록 1-8. RMStudio Loss 설정	145
그림 부록 1-9. RMStudio Hazard 설정	146
그림 부록 1-10. RMStudio Loss-Hazard 관계 설정	147
그림 부록 1-11. RMStudio Keywords 설정	148
그림 부록 1-12. RMStudio Keywords 템플릿 설정	148
그림 부록 1-13. RMStudio UCA 식별	149
그림 부록 1-14. RMStudio Reporting - Loss/Hazard 분석 결과 예시	150
그림 부록 1-15. RMStudio Reporting - UCA 분석 결과 요약 예시	151
그림 부록 1-16. RMStudio Reporting - Control Action별 UCA 분석 결과 예시	152
그림 부록 1-17. RMStudio Reporting - Loss Scenario 분석 결과 예시	153





제 1 장

서론

제1절 연구 배경 및 필요성

제2절 연구 목적 및 범위

제3절 연구 방법론

제4절 내용 구성

KAERI



제1장 서론

제1절 연구 배경 및 필요성

하나로는 1995년 첫 임계에 도달한 이후로 핵연료 및 재료의 조사 실험, 동위원소 생산, 중성자 빔을 이용한 연구 및 분석에 이용되고 있다. 하나로 초반 운전주기에는 1주일을 기준으로 3~4일 운전 / 2~3일 정지를 반복하였으며, 통상 4주 운전 후 2주 정지 원칙으로 연간 200일 운전을 이어왔다. 반면 원자로 정상운전 주기 이외에도 계통 건전성을 손상시키는 비정상 현상이 감지될 시 원자로를 자동 혹은 수동으로 불시 정지하게 되는데, 그림 1은 1995년 이후 원자로 불시정지 현황을 보여준다[1].

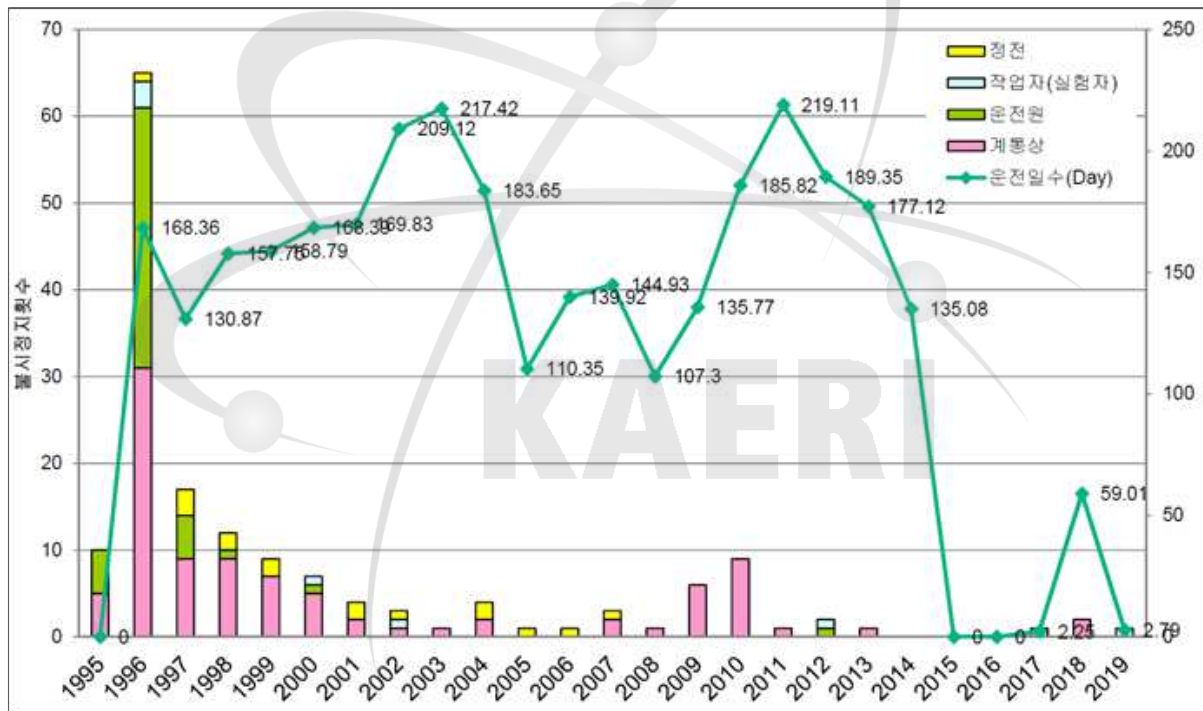


그림 1. 연도별 하나로 운전일수 및 불시정지횟수

운전 초창기를 제외하고는, 2009~2010년 노내 핵연료 조사시험 장치와 냉중성자원(CNS; Cold Neutron Source) 설비 설치 및 시운전 과정에서 불시정지 횟수가 다소 증가추세를 보였지만, 이후에는 꾸준히 감소하는 추세를 보여 왔다. 하지만 최근 다시 다소 증가하는 추세를 보인다. 이는 최근 연구용 원자로 관련 규제가 강화되면서 본 규제를 만족하기 위한 장기간의 재가동 준비, 엄격해진 불시정지조건에 따라 불시정지 빈도가 높아지면서 운영률이 감소한 것이다. 주어진 환경 하에서 하나로의 안정적 운영과 활용

을 위해 불필요한 불시정지를 최소화할 필요가 있다. 이에 본 연구는 하나로 운영 프로세스를 모델링하여 원자로 불시정지 시나리오의 기초자료를 도출함으로써, 향후 원자로 불시정지 최소화에 기여하고자 한다.

제2절 연구 목적 및 범위

표 1은 최근 2010-2019년 원자로보호계통(RPS, Reactor Protection System)과 원자로제어계통(RRS, Reactor Regulating System)에 의한 불시정지 연도별 현황[2]을 보여 준다[2]. 표 1에서 볼 수 있듯이, 총 18건의 불시정지 중 7건이 CNS 수소계통 압력 이상으로 인해 발생함을 알 수 있다. 특히, 2018년 12월 CNS 수소 압력 불안정으로 인한 원자로 수동정지 이후, 그 원인파악 및 연구원 조치 등으로 수개월간 재가동을 하지 못하여 운영률이 크게 저하된 상황이다.

여건상, 본 연구에서 하나로 전반의 모든 계통을 분석하기에는 어려움이 있는바, 위와 같은 배경에 근거하여 CNS계통을 하나로 불시정지 시범 분석 대상으로 선정하였다. CNS계통으로 인한 하나로 불시정지는 두 가지 신호, 즉 CNS 수소계통 고압력, CNS 수소계통 저압력 신호로 인해 발생한다. 따라서 CNS계통의 운영 프로세스 모델링은 이 두 불시정지 신호의 발생을 유발하는 상황 및 조건을 그 분석 범위로 한다.

표 1. 하나로 불시정지 현황 (2010~2019년)

연도	RPS 자동 정지	RRS 자동 정지	수동정지	주요원인
2010	0	9	0	CNS 기포발생(4), I&C, 제어봉(2), 펌프오일, 반사체
2011	1	0	0	수조고방사선, 백색비상
2012	1	1	0	수조고방사선, 인적오류
2013	0	1	0	CNS 수소 압력
2014	0	0	1	Bio-D 전원 단자 소손
2015	하나로 내진 보강공사			
2016				
2017	0	0	1	수조고온층
2018	0	1	1	정지제어봉, CNS 수소 압력
2019	0	1	0	CNS 수소 압력, 작업자 오류
계	2	13	3	

제3절 연구 방법론

CNS 수소 압력 비정상에 의한 원자로 불시정지는 수소계통에 존재하면서 수소 압력에 직접적으로 영향을 미치는 기기의 고장에 의해 발생할 수 있다. 하지만 보다 포괄적인 분석을 위해, 기기 또는 관련 계통간의 상호작용, 인적 요인과의 상호작용, 그리고 환경과 같은 시스템 외적인 요인까지 통합적으로 고려한 분석이 필요할 것으로 판단된다.

이에 2012년 미국 MIT대학의 Leveson교수가 제안한 위험 분석 방법인 STAMP/STPA(System-Theoretic Accident Model and Process/System-Theoretic Process Analysis)기법[3]을 적용하고자 한다. 이는 FTA/ETA(Fault Tree Analysis/Event Tree Analysis), FMEA(Failure Mode and Effect Analysis), HAZOP(Hazard and Operability Study) 등 전통적 위험분석 방법과는 다르게, 사고가 시스템을 구성하는 요소(기기 및 인적요소 등) 간 제어문제에 의해 발생할 수 있다는 관점에서, 시스템을 모델링 하고 사고를 분석하는 프로세스이다. 따라서 수많은 기기 및 인적 요소로 구성된 복잡한 계통도 추상화하여 분석가능하다. STAMP/STPA기법은 국외에서는 미국, 일본 등을 중심으로 항공, 자동차, 원자력 분야에서 적용되고 있으며, 특히 미국 NRC(Nuclear Regulatory Commission), EPRI(Electric Power Research Institute)는 해당 방법론을 원전 디지털 계통 위험 분석에 활용한 사례가 있다[4, 5].

제4절 내용 구성

본 보고서의 내용 구성은 제 2장에서 STAMP/STPA에 대한 이론부터 일반적인 소개를 다루며, STAMP/STPA모델을 작성하는 방법, STPA를 수행하는 단계별 프로세스, STPA를 원자력 분야에 적용한 예제들을 소개한다. 제 3장에서는 하나로 연구용원자로의 운영 프로세스 및 관련 위험요소들을 분석하기 위해 STPA모델을 개발하고 분석을 수행한 연구내용을 기술한다. 제 4장에서는 개발된 STPA모델에서 도출된 CNS계통에 대한 안전하지 못한 제어 행위(UCA; Unsafe Control Action)들에 대해 기존 하나로 불시정지 사례들과와의 비교분석을 수행한 결과를 기술하며, 그 결과를 통해 STAMP/STPA의 적용가능성 및 향후 개선방향을 기술한다. 제 5장에서는 결론을 기술한다.



제2장

STAMP/STPA 개요

제1절 방법론의 이론적 기초

제2절 STPA 분석 방법론

제3절 원자력 분야 STPA 적용 사례

KAERI



제2장 STAMP/STPA 개요

FTA/ETA, HAZOP, FMEA 등의 기존 전통적 위험분석 기법은 약 50년 전 시스템 내 소프트웨어의 비중이 적고 현재 시스템에 비해 비교적 단순한 구조의 시스템을 대상으로 개발된 위해도/위험 분석 기법들이다. 이러한 기법들은 시스템의 오동작을 발생시키는 구성요소를 식별해 해당 요소를 대체하거나 보완한다면 사고 예방 및 해결이 가능하다는 전제를 기반으로 한다. 과거 시스템들은 분리 관계가 명료하여 독립적인 분석이 가능했으며, 구성요소 간 상호작용 또한 단순하였기 때문에 안전에 영향을 미치는 특정 기기 결함이나 사건을 식별하는 방식으로 위험분석이 가능했다. 하지만, 점차 디지털 기반의 전기전자제어시스템이 증가하면서 소프트웨어의 비중이 높아지고 시스템이 복잡해지게 되어 기존 방법론으로는 위험분석에 많은 한계점이 존재해왔다. 특히 시스템의 복잡성으로 인해 시스템 내 결함을 식별하기가 어려워졌을 뿐만 아니라 시스템들 간 또는 시스템-외부요소(사람, 정책, 환경 등)간의 여러 상호작용으로 시스템에 기능상 문제가 없다 할지라도 복합적인 요인에 의해 예기치 못한 사고가 발생할 수 있기 때문이다.

이러한 점을 극복하기 위해 미국 MIT대학의 Leveson교수 연구팀은 시스템 이론(System Theory)에 기반한 STAMP/STPA라는 위험분석 방법을 제안한 바 있다[3]. STAMP/STPA방법론은 사고 원인의 확장 모델을 기반으로 한 새로운 위해도 분석 기법이며 소프트웨어, 하드웨어, 운전원 등이 포함된 복잡한 시스템에 대한 위험 분석이 가능하며 이를 기반으로 CAST(Causal Analysis based on Systems Theory), STPA-SEC(System-Theoretic Process Analysis for Security) 등 다양한 분석 기법이 개발되어 자동차, 항공과 같은 중요 안전 분야의 시스템 분석에 활발히 적용되고 있다.

제1절 방법론의 이론적 기초

1. 시스템 이론

STPA는 시스템 이론에 기초하며 이론적 수학적 기초에 대한 이해가 거의 필요하지 않으며 직관적 이해에 도움이 된다. 시스템 이론은 제2차 세계대전 이후에 건설되고 있는 시스템의 복잡성이 증가하는 것을 다루기 위해 개발되었다. 이러한 시스템에서 개별적인 상호작용하는 구성요소의 분리 및 분석은 각 요소들의 행동이 명백하지 않은 방식으로 결합되기 때문에 시스템 전체에 대한 결과를 왜곡할 수 있다.

STAMP/STPA방법론의 기초가 되는 시스템 이론의 이해를 돕기 위해, 이와 대조되는 기존의 해석적 분해의 개념 및 전제를 살펴본다. 기존의 해석적 분해에 따른 접근은 시

시스템을 구성요소(Component)로 나누고 사고(Accident)는 구성요소의 실패로 인해 발생한다는 가정 하에, 각 구성요소의 실패 확률을 개별적으로 계산한 다음 분석 결과를 시스템 신뢰성 수치를 계산할 때 결합한다. 또는 시스템의 실패를 유발할 수 있는 직접적 또는 논리적 고장 이벤트의 체인을 식별하고, 각 이벤트의 확률을 이벤트 체인의 발생 확률로 결합한다. FMEA, FMECA(Failure Modes, Effects, and Criticality Analysis), FTA/ETA, FHA(Fault Hazard Analysis), HAZOP 기법이 이러한 접근법의 예시들이다. 이와 같은 접근에는 아래 전제를 내포하고 있다.

- 각 구성요소 또는 서브시스템은 독립적으로 동작한다. 이벤트가 모델링되는 경우, 이벤트는 바로 앞뒤의 이벤트를 제외하고는 독립적이다.
- 구성요소의 개별적 동작이 전체에서 동작하는 것과 동일하다.
- 구성요소 및 이벤트는 피드백 루프 및 기타 간접 상호작용에 영향을 받지 않는다.

전통적인 해석적 분해에 따른 접근은 대부분의 전기기계 시스템의 유형에 대해서는 여전히 유효하다. 하지만 소프트웨어에 의해 기능하거나 인적요인을 포함하는 시스템 구성요소의 복잡한 상호작용에 의해 기능하는 시스템의 경우, 그 시스템의 모든 잠재적 동작을 예측, 이해, 보호하는데 있어서 분석적 접근방식이 더 이상 유효하지 않을 수 있다. 이와 대조되는 시스템 이론은 아래와 같은 특징을 가진다.

- 시스템을 부분들의 합으로서가 아닌 전체로서 취급한다.
- 주요 관심사는 개별 구성요소의 합이 아닌, 구성요소가 상호작용할 때 나타나는 속성인 "발현(Emerge)" 속성이다.
- 시스템 위험요소는 시스템 구성요소간의 관계, 즉 상호 작용에 의해 발생한다.

여기서 발현 속성이란 시스템 구성요소가 독립적으로 있을 때는 확인할 수 없지만, 각 구성요소가 시스템 전체의 일부로써 상호작용할 때에 비로소 발생하는 속성을 말한다. 시스템 내 개별구성요소의 거동 및 구성요소간의 상호작용이 발생하는 경우, 안전, 보안, 유지보수성 및 운전가능성과 같은 시스템의 주요 특성을 제어하려면 개별 요소들의 거동 및 상호작용을 제어해야 한다. 이러한 발현속성으로 인해, 심지어 구성요소의 고장이 발생하지 않고 설계된 대로 기능하더라도, 그 상호작용으로 인해 시스템차원에서 위험한 상황이 발생할 수 있음을 감안한다. 아래 그림 2는 기존의 해석적 분해에 따른 접근 및 시스템 이론에 기반한 접근의 차이를 보여준다. 그리고 각각의 이론적 배경에 따른 위험 분석 방법론들의 연관성 및 차이는 그림 3과 같이 표현될 수 있다.

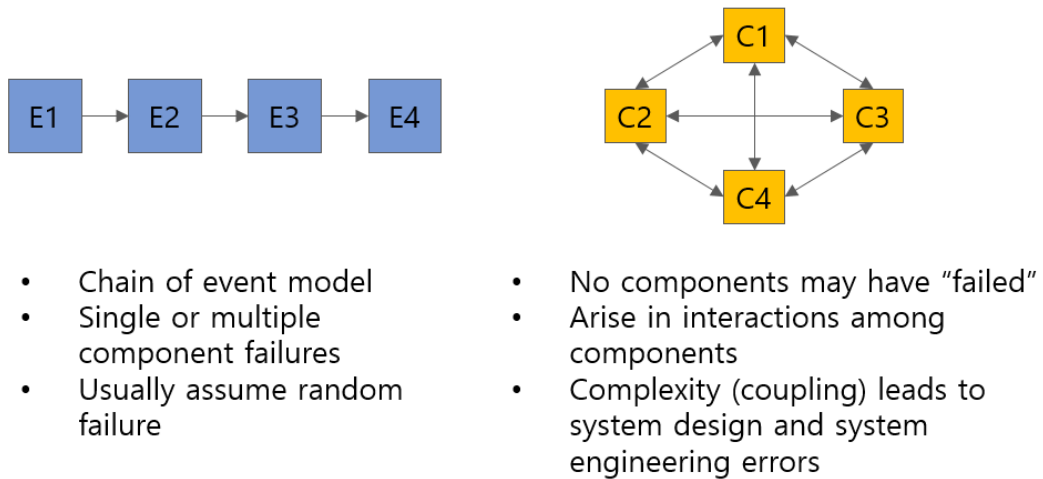


그림 2. 해석적 분해(좌) 및 시스템 이론(우)에 기반한 접근의 차이

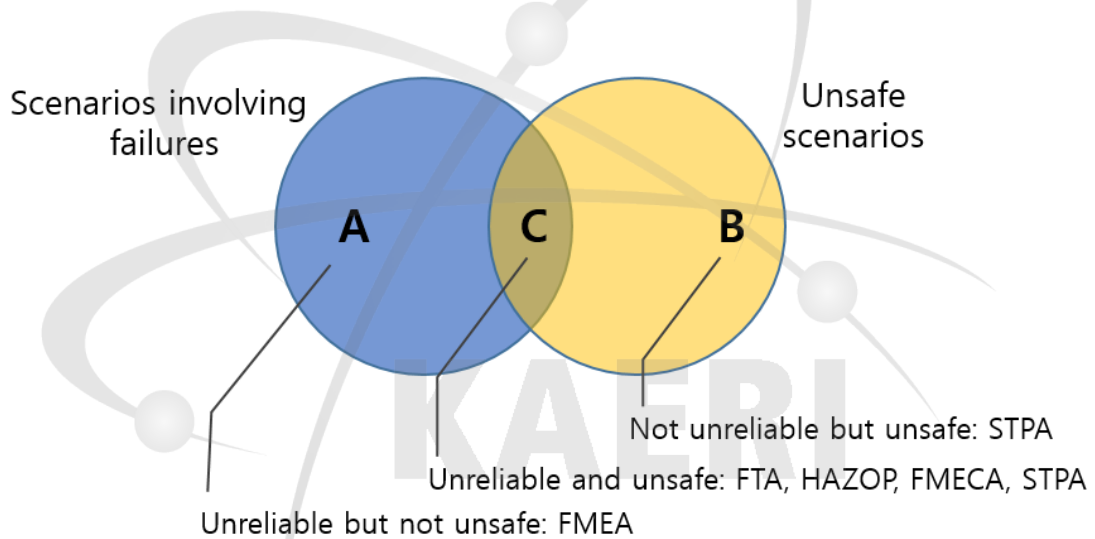


그림 3. 기존 위험분석 기법과 STPA의 연관성 및 차이점

전통적인 위해도/위험 분석 기법에 비해 STAMP/STPA기법이 가지는 특징 및 장점은 다음과 같이 정리할 수 있다.

- 이전에 운용에서만 발견되었던 미지의 고장 및 사고 위험을 시스템 개발주기 초기에 식별하여 제거하거나 완화할 수 있으며 이는 의도된 기능 및 의도하지 않은 기능 모두를 포함한다.
- 기존의 위험 분석 방법과는 다르게, 시스템 개발 생명주기 중 초기 요건 (Requirement) 및 설계(Design)단계에서도 STPA분석을 시작할 수 있어 안전 요구사항 및 제약사항 등을 식별할 수 있으며 이를 시스템 아키텍처와 설계에 이용하

여 개발 중 또는 운용 중에 결함이 확인될 때 수반되는 비용을 줄일 수 있다.

- 상세한 설계 결정이 이루어짐에 따라 STPA분석을 개선하여 상세한 설계 결정에 활용할 수 있으며 시스템 설계 사항에 대한 추적성을 쉽게 유지할 수 있으며 시스템 유지보수성을 개선할 수 있다.
- STPA는 소프트웨어 및 인간 운전원을 분석대상에 포함시켜 위험분석 과정에서 모든 잠재적 인과 요인이 포함되도록 보장한다.
- STPA는 대규모의 복잡한 시스템에서 기존 위험분석 방법에서 누락되거나 찾기 어려운 시스템 기능에 대한 분석이 수행되도록 보장한다.

2. STAMP 개념 이해

STAMP는 시스템 이론에 기반한 사고 분석 모델 및 프로세스로서 STPA의 이론적 토대를 제공한다. STAMP는 FTA/ETA, FMEA와 같은 분석 기법이라기보다는 거시적 관점에서 사고의 원인을 구조화하고 식별하는 관점과 절차를 제시하는 모델이자 프로세스이다. STAMP에서 사고의 원인을 바라보는 관점은 기존의 위험분석 기법에서 제시하는 관점과 차이가 있다. 기존의 분석 기법은 특정 기능이나 기기의 결함, 동작 실패, 특정 사건에서 사고가 기인한다고 보지만 STAMP는 사고의 발생 원인을 단순히 특정 사건이나 기능 실패의 문제로 바라보지 않고 시스템을 구성하는 기기간 제어문제(control problem)에서 사고가 발생한다고 본다. 또한 STAMP에서는 사고의 원인이 시스템 그 자체뿐 아니라, 시스템과 관련된 인적 자원, 사회적 · 구조적 구조, 제도·정책 등 복합적 작용에서 비롯될 수 있다고 본다. 예를 들어, 사고를 분석할 때는 ‘왜 시스템 동작이 실패했고 동작 실패가 어떻게 사고로 이어지게 되었는가’의 관점에 국한하기 보다는 ‘사고가 일어나지 않도록 방어하거나 그 영향을 최소화할 수 있는 적절한 제어(control)가 왜 이루어지지 않았는가 또는 왜 부적절한 제어가 일어났는지’와 같은 관점에서 분석을 수행한다. STAMP는 STPA, CAST, 위험 선행지표의 식별 및 관리, 조직위험분석 등 보다 강력한 위험분석 도구의 창출을 가능하게 한다. 특히 오늘날 널리 사용되는 STAMP기반 툴은 STPA와 CAST가 있으며 STPA는 위험을 제거하거나 제어할 수 있도록 시스템 개발 중 사고의 잠재적 및 미확인 위험요소들을 분석하는 사전 예방적 분석 방법이다. STAMP의 주요 특징은 다음과 같이 요약될 수 있다.

- 안전을 고장 방지의 문제가 아닌 동적 제어문제로 취급된다.
- 상향식이 아닌 하향식 접근으로, 복잡한 시스템의 표현도 가능하다.
- 사고 및 기타 손실에 대한 인과관계 요인으로써, 소프트웨어, 인간, 조직, 안전문화 등을 모두 하나의 모델에 포함한다.

제2절 STPA 분석 방법론

1. STPA 개념

STPA는 STAMP를 기반으로 하는 위험분석 기법으로 시스템 생명주기 전 과정에 걸쳐 존재하는 잠재적인 위험과 발생 원인을 시스템의 상위 수준에서 분석하는 새로운 기법이다. STPA는 시스템의 안전(safety)을 확보하기 위해서는 시스템이 안전 제약사항(safety constraint)을 지킬 수 있도록 제어(control)해야 한다는 관점을 가진다. 즉 STPA는 위험(Hazard)을 특정 기능의 실패나 기기 오류 문제로 인식하기보다는 시스템과 시스템 또는 구성요소들 간 제어 문제(control problem)에서 발생함을 전제로 한다. 여기서 시스템 구성요소는 하드웨어나 소프트웨어와 같은 시스템뿐 아니라 인력, 사회 조직, 제도 등으로 다양할 수 있다.

STPA기반 위험분석은 시스템을 제어 관계 관점에서 분석하고 해당 제어 관계 중 위험을 유발할 수 있는 부적절한 제어를 식별하는 방식으로 이루어진다. 사고 정의에서 시작하여 원인 시나리오(Causal Scenario)도출을 수행하는 하향식 분석 체계를 가진다. 또한, 분석 과정에서 안전 제약사항(safety constraint)과 안전 요구사항(safety requirement)을 도출할 수 있다. 안전 제약사항이란 위험을 발생시키지 않도록 하기 위한 시스템 수준의 요건을 의미하며 안전 요구사항은 시스템 구성요소 수준의 요건을 의미한다.

2. STPA 분석 절차

STPA의 수행단계는 그림 4와 같이 크게 4단계로 수행된다. 분석 대상과 관련한 사고(Loss) 및 위험(Hazard)을 정의하는 1단계, Control Structure를 도식화하는 2단계, 안전하지 못한 제어 행위(UCA)를 도출하는 3단계, 원인 요소(Causal Factor)와 원인 시나리오(Causal Scenario)를 도출하는 4단계로 이루어진다.

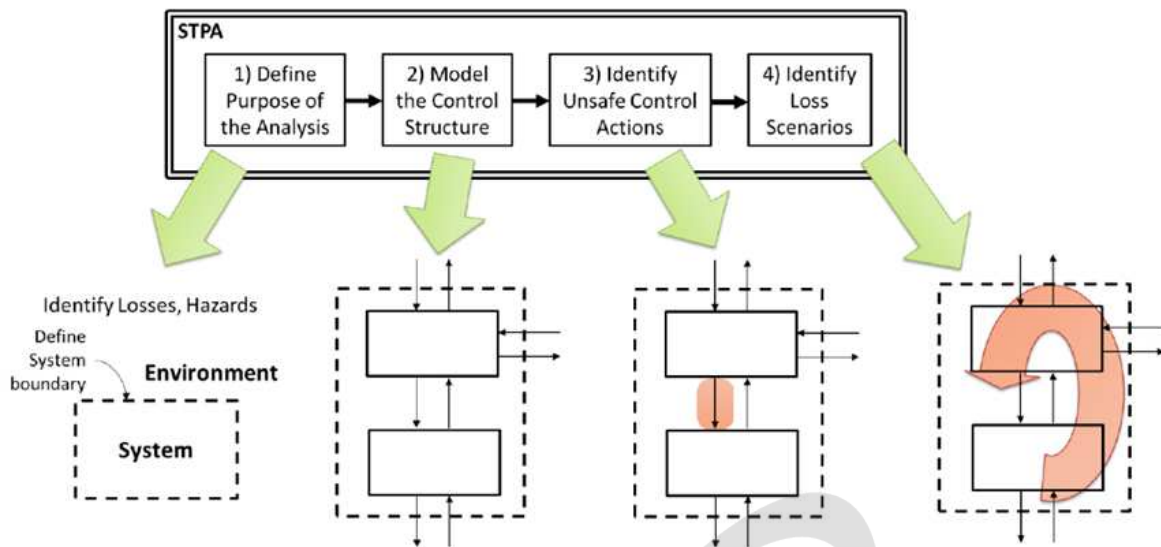


그림 4. STAMP/STPA 분석 절차

가. 사고 및 위험 정의

어떤 분석방법이든, 그 분석의 목적을 분명히 정의하는 것이 중요하다. STPA도 마찬가지인데 이와 관련하여 2가지 정의, 즉 사고 (Loss 또는 Accident)와 위험(Hazard)의 정의를 요구한다. 여기서 사고란 인적 손실 및 상해, 재산의 피해, 환경의 오염, 미션의 실패 등 다양한 성격의 정의가 있을 수 있다. 다만 위험과 구분되는 특징으로 시스템 차원에서 통제할 수 있는 범위를 넘어선 것을 의미한다.

반면 위험은 시스템의 단일 또는 집합적 상태 및 조건으로써, 최종적으로 사고로 이어질 수 있지만 시스템차원에서 여전히 통제 가능한 영역의 것을 의미한다. 1단계에서는 사고와 위험의 정의를 통해 시스템의 경계가 어디까지인지, 사고로 이어질 수 있는 시스템의 상태에는 무엇이 있는지 등의 근본적인 내용을 다룬다. 예로 들어, 원전의 경우 사고에 영향을 미칠 수 있는 요인은 원자로정지시스템의 제어문제, 도시 위치, 풍향, 풍속 등 다양하다. 이 때 도시 위치나 풍향, 풍속과 같은 요인은 시스템 엔지니어가 제어할 수 없는 부분이므로 위험분석 범위에서 주로 제외된다.

나. Control Structure 도식화

Control Structure는 시스템을 그림 5와 같이 컨트롤 루프 형태를 띄어 제어의 관점으로 주체(Controller), 객체(Controlled Process), 제어(Control Action), 반응(Feedback)으로 구성된다. 각 구성요소에 대한 설명은 표 2와 같다. 여기서 Controller는 Controlled Process를 컨트롤하기 위한 내부 알고리즘과 Process Model을 포함한다.

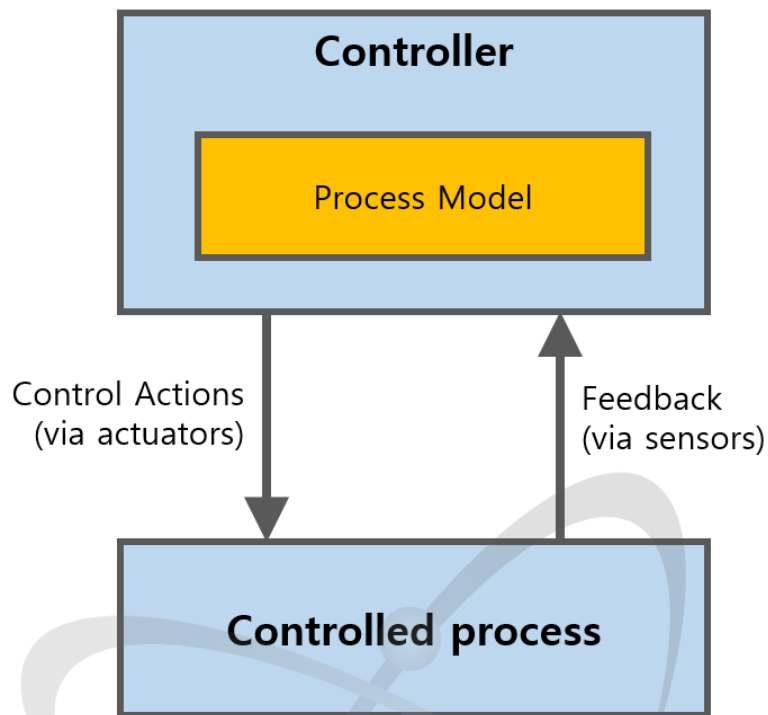


그림 5. 제어 루프의 일반적 구성

표 2. Control Structure의 구성 요소

구성요소	설명
Controller	제어명령을 내리는 주체로서 사람, 소프트웨어, 기기, 절차 등을 포함.
Controlled Process	제어 대상 객체
Process Model	Controller가 제어명령을 내리는데 판단의 근거가 되는 다양한 정보
Control Action	Controller가 내리는 제어명령
Feedback	제어명령을 이행한 결과, Controlled Process의 상태를 나타는 정보

기본적으로 Control Structure는 계층적 구조(Hierarchical Structure) 특성을 기반으로 한다. Control Structure를 도식화 할 때 범위를 단순히 하드웨어와 소프트웨어로 구성된 시스템으로 한정하지 않고 시스템 프로세스나 운영 프로세스 시스템 개발 또는 운영에 영향을 미치는 지침과 같은 사회적 측면, 운영자나 관련 조직 등 인적 측면을 모두 포함할 수 있다. 즉 Control Structure는 시스템 개발(System Development) 측면과 시스템 운영(System Operation) 측면을 모두 포함할 수 있다. 예로 들어 시스템 설계나 개발 공

정과 같은 개발 측면의 문제가 위험을 유발할 수도 있지만 안전 운전 사항을 준수하지 않거나 운전자 미숙 또는 실수, 시스템 성능 저하와 같은 운영 측면에 의해서도 위험이 발생할 수 있다. Control Structure는 대개 매우 추상적인 수준에서 시작하며, 시스템에 대한 보다 자세한 정보를 표현하기 위해 반복적으로 구체화되며 그림 6과 같이 다양한 형태의 시스템을 표현할 수 있다. Control Structure의 주요 특징은 다음과 같다.

- Control Structure는 물리적 블록다이어그램이나 계통도와 같은 물리적인 모델 (physical model)이 아니며 기능을 중심으로 도식화한 것이다.
- Control Structure는 항상 실행 가능한 모델이나 시뮬레이션 모델이 아니다. Control Structure는 인적 요소와 같은 종종 실행 가능한 모델을 포함하지 않는 구성요소들을 포함한다. 예로 들어, 필요한 실행 명령이 전달되지 않을 수 있으며, 부적절한 명령이 전달되거나, 실행 명령을 받은 객체가 주어진 명령을 이행하지 않을 수 있다고 가정한다.
- Control Structure에 도식화되는 Control Action이나 Feedback은 실제로 실행되는 명령어를 의미하기 보다는 두 객체간의 송수신되는 정보를 의미한다.
- Control Structure는 시스템의 복잡성 문제를 해결하기 위해 시스템을 추상화하여 표현한다. 예로 들어, 시스템의 구성요소를 버튼, 스위치, 레버 등으로 나열하기보다는 기기들을 기능에 따라 추상화하고 객체간 Control Action이나 Feedback도 개념적으로 추상화하여 단순화할 수 있다.

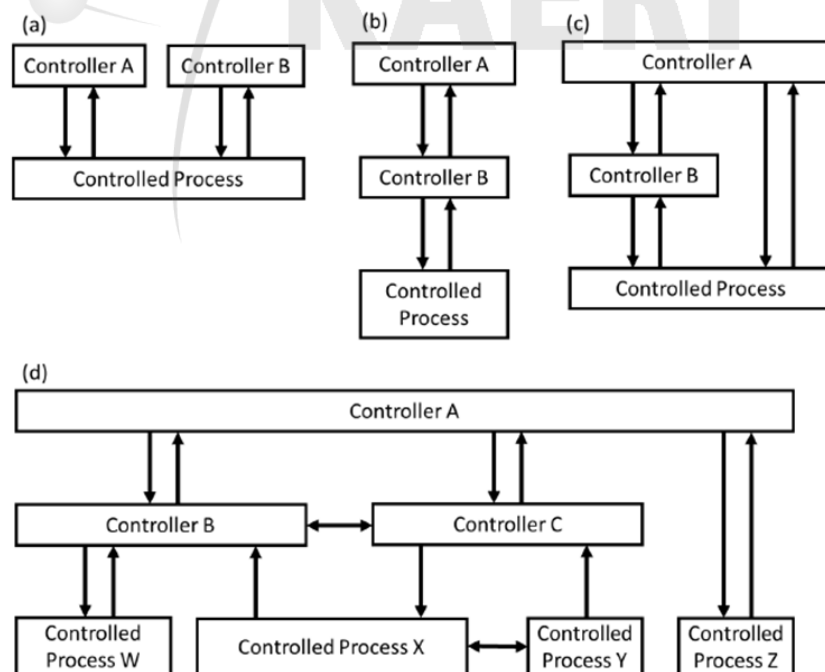


그림 6. 다양한 형태의 Control Structure

다. Unsafe Control Action 도출

세 번째 단계는 시스템의 기능을 수행하기 위한 일종의 개시신호(activation signal)인 Control Action을 분석하여, 첫 번째 단계에서 정의된 사고 또는 위험으로 이어질 수 있는지를 검토하는 것이다. Unsafe Control Action(UCA)은 시스템의 위험을 유발할 수 있는 Control Action의 불안전한(unsafe) 형태를 의미한다. 2단계에서 정의한 모든 Control Action이 UCA 도출의 대상이 되며 분석의 목적과 범위에 따라 특정 Control Action만을 대상으로 UCA를 도출할 수도 있다. Control Action에서 UCA를 도출하기 위해서는 크게 1) Controller가 Control Action을 제공하는 형태와 2) 해당 Control Action이 행해지는 특정 상황 또는 조건(Context)이 필요하다. 첫째로 Control Action이 불안전할 수 있는 형태는 표 3과 같이 주로 크게 4가지 유형으로 분류되지만 시스템 및 적용 분야에 따라 UCA 유형의 변경 및 확장이 가능하다.

표 3. 위험을 유발할 수 있는 UCA의 4가지 전형적인 유형

유형	설명
Not providing causes hazard	〈Controller〉가 〈Control Action〉을 제공하지 않아서 위험이 발생할 수 있음.
Providing causes hazard	〈Controller〉가 〈Control Action〉을 제공하여 위험이 발생할 수 있음.
Too late, too soon, out of order	〈Controller〉가 〈Control Action〉을 제공하였으나, 너무 늦게 또는 너무 빨리, 또는 잘못된 순서로 제공하여 위험이 발생할 수 있음.
Stopped too soon, Applied too long	〈Controller〉가 〈Control Action〉을 너무 이른 시점에 제공이 종료되거나 너무 오랫동안 제공하여 위험이 발생할 수 있음

시스템의 위험은 단순히 표 3의 Control Action 제공 형태에 따라 발생하지 않으며, Control Action이 제공되는 시점의 시스템 및 시스템의 주변 환경 조건에 따라 위험이 발생할 수 있다. 이러한 정보를 Context로 정의하고 4가지 타입의 Control Action을 조합하여 UCA를 도출한다. Context는 Control Action을 제공하는 Controller의 Process Model과 밀접한 관련이 있다. 전 단계에서 Process Model이 정의되었다면 해당 정보를 토대로 고려할 수 있는 모든 환경 조건들의 경우를 Context로 작성하는 것이 가능하다.

라. Causal Scenario 도출

네 번째 단계에서는 세 번째 단계에서 도출된 위험을 유발할 수 있는 UCA가 왜 발생하는 지에 대한 원인들(Causal Factors)을 분석한다. 이 과정을 통해 도출되는 사고 시나리오는 잘못된 피드백, 부적절한 요구사항, 설계 오류, 구성요소 고장 및 기타 요인이 어떻게 UCA를 야기하고 궁극적으로 위험 및 사고로 이어지는지, 그리고 올바른 Control Action이 제공되었음에도 불구하고 어떠한 이유로 시스템 기능이 정상적으로 수행되지 않을 수 있는지를 설명한다.

원인들은 Control Structure를 기반으로 직관적으로 도출할 수 있으며 그림 7과 같이 크게 두 가지 유형으로 분류할 수 있다. 첫째는 Control Action이 왜 불안전하게 제공되었는지 (Controller가 UCA를 제공한 원인이 무엇인지)를 도출하는 것이며, 두 번째는 제공한 Control Action이 부적절하게 수행되거나 수행되지 못한 것에 대한 원인을 도출하는 것이다. 이러한 원인들을 토대로 원인 시나리오를 작성한다.

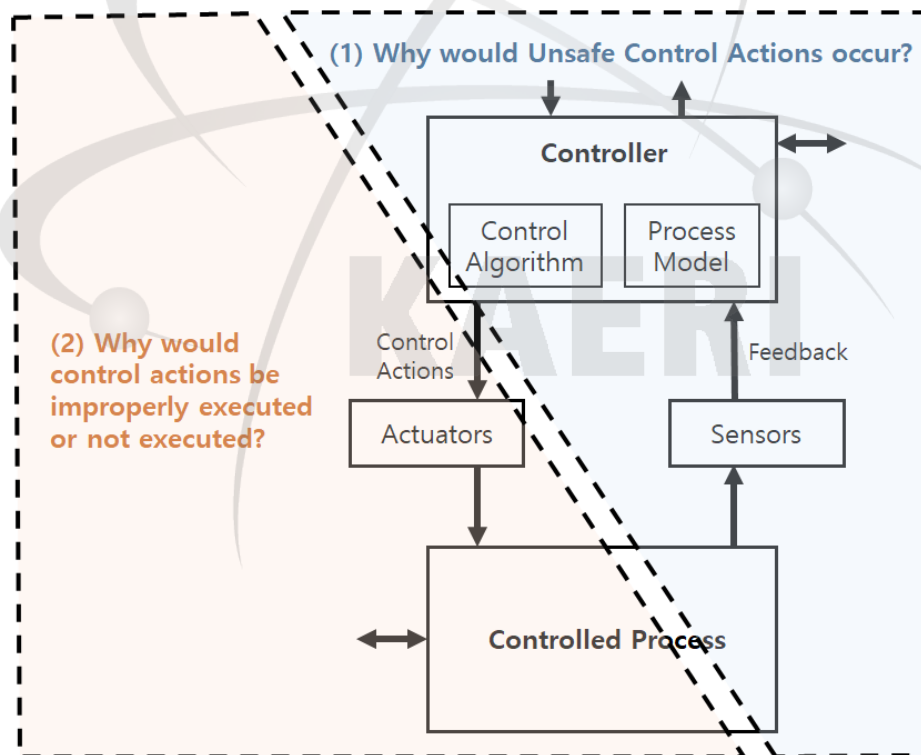


그림 7. Causal Scenario 유형

그림 7의 (1) Why would unsafe control actions occur에 존재하는 UCA 유발 원인은 Controller 자체에 존재할 수 있으며, Controller가 받는 Feedback에 존재할 수도 있다. Controller 자체에 존재하는 원인은 Controller의 고장, 부적절한 알고리즘 또는 Process

Model 등이 있으며 Feedback에 존재하는 원인은 Controlled Process로부터 받는 정보가 부적절한 경우나 필요한 정보를 받지 못하는 경우 등이 있다. 또한 사고는 UCA의 수행으로 발생도리 수도 있지만 Control Action이 부적절하게 수행되거나 수행되지 않은 경우에도 발생할 수 있다. 즉 Controller와 Controlled Process 사이에서 Control Action을 전달하는 Control Path와 Control Action이 수행되는 Controlled Process에서 그 원인을 찾아낼 수 있다. 예로 들어, Control Path는 단순 Actuator로 구성되거나 Control Action을 전송하기 위한 네트워크로 구성되는데, 여기서 Actuator가 Control Action을 수신하지 못하거나 잘못된 Control Action을 수신하는 경우에는 통신 지연, 데이터 전송 오류가 생길 수 있다. Actuator가 응답하지 않거나 잘못된 응답을 하는 경우는 Actuator의 물리적 오류, 전원문제, 성능저하 등이 그 원인이 될 수 있다.

제3절 원자력 분야 STPA 적용 사례

해외에서는 미국, 일본 등을 중심으로 항공, 자동차, 의료, 원자력 등 분야에서 STPA를 도입된 바 있다. 표 4는 다양한 분야에 적용된 STPA분석 사례를 나타낸다. 미국 SAE International 항공 표준인 ARP 4761A 개정판에 STPA가 추가될 예정이며 자동차 기능 안전 표준 ISO 26262 Rev. 2에 STPA가 위험분석 기법으로 포함될 예정이다. 미국의 NHTSA(National Highway Traffic Safety Administration), EPRI, FDA(US Food and Drug Administration)에서도 안전성 분석에 STPA를 적용한 연구 결과들을 발표하고 있으며, 일본의 차량 시스템 표준화 단체 JASPAR(Japan Automotive Software Platform and Architecture)에서도 자율주행차 안전성 분석에 STPA 적용 계획을 발표한 바 있다. 특히 STAMP/STPA방법론을 원자력 분야에 적용한 사례들은 아래와 같다.

표 4. 안전 분야에서의 STPA 적용 현황

분야	주요 내용
항공	<ul style="list-style-type: none"> ○ SAE International Aircraft and Systems Development and Safety Assessment Committee(S-18) 표준위원회는 ARP 4761A의 PASA(Preliminary Aircraft Safety Assessment) 및 PSSA(Preliminary System Safety Assessment)에 STPA를 적용하는 방안을 검토 중임[6]. ○ ASTM(American Society for Testing and Materials) F44.50위원회에서 WK60748(New Guide for Application of System-Theoretic Process Analysis to Aircraft) 표준을 개발 중임[7]. ○ FAA에서 Software Assurance Approaches, Considerations, and Limitations 보고서를 통해 STPA를 활용한 Software Hazard 분석 방법을 제시함[8].
자동차	<ul style="list-style-type: none"> ○ SAE International은 GM, Ford, Nissan 등 11개의 자동차 회사가 참여하는 STPA Recommended Practice Task Force를 구성하였으며 ISO 26262 Rev. 2에서 STAMP/STPA를 위험분석 기법으로 포함할 예정임. ○ GM은 STPA를 활용한 v-Model을 개발하여 자사의 Safety Process에 적용 중임. ○ 미국 NHTSA는 STPA를 적용한 차량시스템 위험분석 방법을 연구하여 관련보고서[9]를 발간함. ○ 일본의 차량 시스템 표준화 단체 JASPAR는 일본 정보기술진흥원(IPA/Sec)과 함께 자율주행차의 안전성 분석 방법으로 STPA 적용 계획을 발표함[10].
원자력	<ul style="list-style-type: none"> ○ 미국 전력연구소 EPRI는 2013년부터 일찌감치 STPA기법에 주목하여 FTA/ETA, FMEA 등 기존 위험분석 기법과 STPA를 연계한 안전성 분석 방안을 연구하여 HAZCADS프로젝트에 적용한 바 있다[4].
의료	<ul style="list-style-type: none"> ○ 미국 FDA에서는 의료 기기 UI 소프트웨어의 요구사항을 도출하기 위해 STPA기법을 적용하는 방안을 발표함[11].

1. 미국 Darlington 원전 원자로정지계통 분석 사례

원자력 발전소는 안전에 치명적 영향을 미치는 시스템이기 때문에 개발 단계부터 FTA/ETA, FMEA 등을 활용해 위험분석을 수행하도록 하고 있다. 최근 원전에 컴퓨터 기반의 제어시스템 도입이 증가하면서 그 구성과 로직이 복잡해짐에 따라 기존 위험분석 기법을 이용해 분석을 수행하는데 어려움을 겪고 있다. 이에 캐나다 OPG(Ontario Power Generation)은 Darlington 발전소의 원자로 제어 시스템을 대상으로 STPA를 적용하고 그 효용성을 분석한 연구 사례가 존재한다[12].

Darlington 원전에서는 컴퓨터를 기반으로 원자로를 자동 정지시키는 Darlington Shutdown System(SDS)를 보유하고 있고 Darlington SDS는 SDS1과 SDS2로 이중화 구조로 구성되어 있으며, 각 시스템은 3채널로 구성되어 있다. SDS1과 SDS2는 기본적으로 원자로 정지 기능을 수행하지만, SDS1은 코발트 제어봉을 이용한 정지 방식, SDS2는 액체독물질 주입 방식에 의한 정지방식으로 동작하는 독립적인 시스템이다. SDS1 원자로 정지 시스템은 크게 트립 컴퓨터, 원자로 등의 상태를 감지/전송하는 센서, 증폭기와 트랜스미터, Watchdog, 중계기 등으로 구성된다. 원자로에는 원자로 상태 정보를 수집할 수 있는 다양한 센서들이 설치되어 있으며, 센서들이 수집한 정보들은 아날로그 신호로서 증폭기와 트랜스미터에 의해 트립컴퓨터에 전달된다. 트립컴퓨터는 각 채널에서 트립 로직 Controller 역할을 수행하는데 원자로에 이상이 발생했다고 판단하는 경우 채널 트립을 발생시킨다. 이 때 선출 로직 서브시스템은 3개 채널로부터 수신한 트립신호를 비교하여 2-out-of-3 트립 로직으로 최종 원자로 정지를 결정한다.

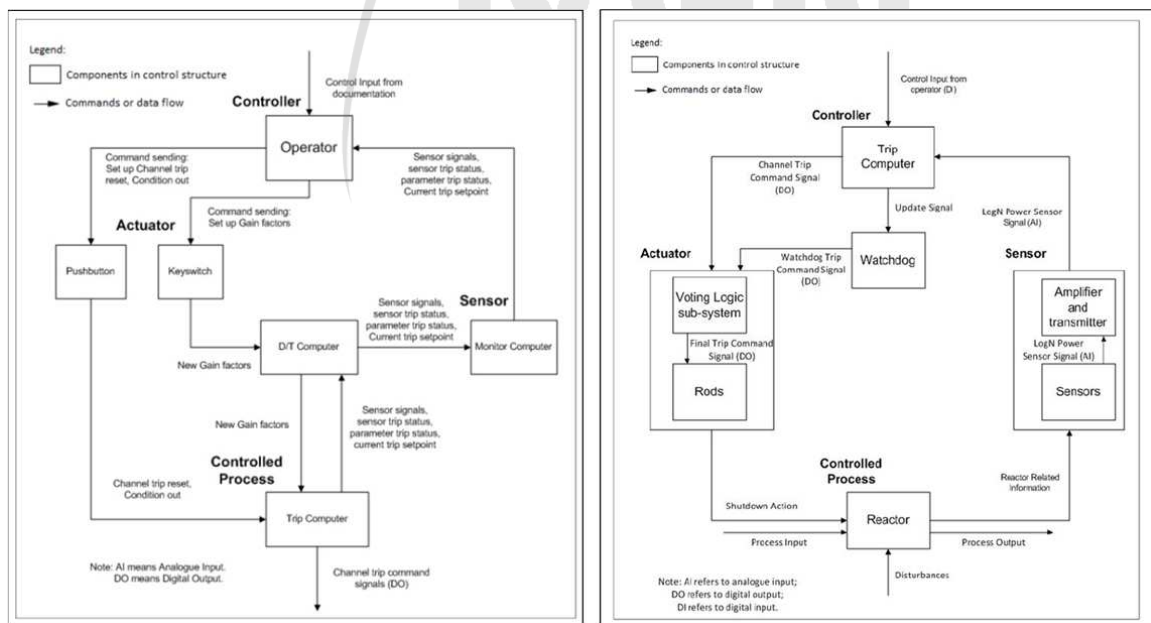


그림 8. Darlington SDS Control Structure - 운전원(좌) 및 시스템(우)

Darlington 원자로 제어시스템의 Controller는 크게 두 가지(운전원과 시스템)이 존재하며 그림 8과 같다. Controller가 운전원인 경우 Control Structure는 Controller(운전원), 액추에이터(Push button, Key switch), 센서(Monitor, Computer), Controlled Process(D/T 컴퓨터, 트립 컴퓨터)로 구성된다. Controller가 시스템인 경우, Control Structure는 Controller(트립 컴퓨터, Watchdog), 액추에이터(선출 로직 서브시스템, 제어봉), 센서(센서, 증폭기, 트랜스미터), Controlled Process(원자로) 등으로 구성된다. 그림 8의 Control Structured에서 트립 컴퓨터는 원자로의 이상상태가 판단된 경우 채널 트립 신호를 발생시키며 Watchdog의 경우도 업데이트 실패로 타임아웃이 발생하는 경우 트립 신호를 발생시킨다. 본 연구보고서에는 Control Structure 도식화 단계에서 식별한 Control Action들 중 High LogN Power 트립과 관련된 두 가지 Control Action에 대해 Unsafe Control Action을 표 5와 같이 도출하였다.

표 5. High LogN Power 트립 관련 UCA 도출 예시

Control Action	Not providing causes hazard	Providing causes hazard	Too soon, too late, out of order	Stopped too soon, applied too long
TC_Trip on High LogNPower	High LogN Power가 setpoint를 초과 시, 트립 컴퓨터가 채널 트립 명령 전송에 실패함 (UCA-1)	“TC_Trip on High LogN Power” 명령 대신 “WD_trip on High LogN Power” 명령이 전송됨. (Not Hazard)	High Log N Power가 setpoint 이하일 때 트립 컴퓨터가 파라미터 트립을 명령함 (UCA-2)	원자로가 채널 트립 시그널을 수신하지 못한 상태에서 너무 빨리 “TC_Trip on High LogN Power” 명령이 종료됨. (UCA-3)
WD_Trip on High LogNPower	time-out이 발생하였지만 Watchdog에서 WD_Trip 전송에 실패함 (UCA-4)	“WD_Trip on High LogN Power” 명령 대신 “TC_Trip on High LogN Power” 명령이 전송됨. (Not Hazard)	Watchdog이 time-out이 발생하지 않았음에도 WD_trip을 전송함 (UCA-5)	원자로가 채널 트립 신호를 수신하지 못한 상태에서 WD_Trip이 너무 빨리 중지됨 (UCA-6)

위 결과에서 알 수 있는 바와 같이 일부 UCA는 실제 발생할 수 있더라도 위험을 초래하지 않는 경우(Not Hazard)로 분류되며 이후 단계에서는 위험을 초래할 수 있는 UCA만을 대상으로 발생 가능한 원인을 분석하였다. 본 연구보고서에서는 2절에서 소개한 바와 같이 다양한 원인들을 기반으로 UCA의 발생에 기여할 수 있는 원인을 표 6과 같이 분석하였다. 본 연구는 STPA가 기존의 전통적 기법, 특히 FMEA와 비교하여 어떠한 효과성이 있는지 분석하기 위해 STPA 위험분석 결과와 기존 FMEA 분석과 비교 평가하였다. 그 결과 FMEA에서 식별하지 못했던 위험, Failure mode 등 STPA분석을 통해서만 도출될 수 있는 위험요소들이 추가적으로 식별됨을 확인한 바 있다.

표 6. Darlington SDS의 UCA-1에 대한 원인 분석

구분	내용		
Controller → Controlled Process	트립 컴퓨터 → 원자로		
Control Action	TC_Trip on High LogN Power		
UCA	(UCA1) High LogN Power가 setpoint를 초과 시, 트립 컴퓨터가 채널 트립 명령 전송에 실패함		
Control Loop	발생원인 (Causal Factor)		
트립 컴퓨터	운전원으로부터 잘못된 명령 수신 혹은 누락	운전절차서 오류 또는 누락	
	부정확한 컨트롤 알고리즘 동작	Calibrated LogNPower 신호가 매우 낮음	알고리즘 모듈(소프트웨어) 오류
	기기 하드웨어 동작 실패	트립 컴퓨터 DO/AI/DI 입출력 실패	DO/AI/DI 카드 오류
트립 컴퓨터 ↔ 센서	부정확한 피드백	피드백되는 AI신호가 너무 낮음	전송 채널 오류
트립 컴퓨터 ↔ 액추에이터	채널 트립 명령 누락	채널 트립 명령 상실	전송 채널 오류
센서	센서/증폭기 동작 오류	부정확한 원자로 상태 신호(AI) 생성	센서/증폭기 오류
	트랜스미터 동작 오류	원자로 상태 신호(AI) 손실	트랜스미터 오류
액추에이터	액추에이터 동작 오류	제어봉의 부적절한 동작으로 채널 트립 실패	제어봉 기기 오류
액추에이터 ↔ 원자로	제어봉 제어 지연	채널 트립 신호 지연	전송 채널 오류

2. 원전 디지털보호계통 안전성 분석 사례

국내 한국원자력연구원에서는 원전 보호계통을 구성하는 공학적안전설비-기기제어계통(ESF-CCS; Engineered Safety Features-Component Control System)의 안전성 분석에 STAMP/STPA 기법을 적용하고 기존 기법들과의 차이를 밝히는 연구가 진행된 바 있다. 그림 9는 ESF-CCS 구성도를 나타내며 8가지 기능(SIAS: 안전주입 작동, CIAS: 격납용기격리 작동, MSIS: 주증기격리 작동, CSAS: 격납용기 살수 작동, AFAS: 보조급수 작동, CREVAS: 주 제어실 비상환기 작동, FHEVAS: 핵연료취급지역 비상환기 작동, CPIAS: 격납용기 퍼지 격리 작동)을 수행한다. 해당 연구에서는 이 중 SIAS를 대상으로 STPA기법을 적용하여 안전성 분석을 수행한 바 있다[13].

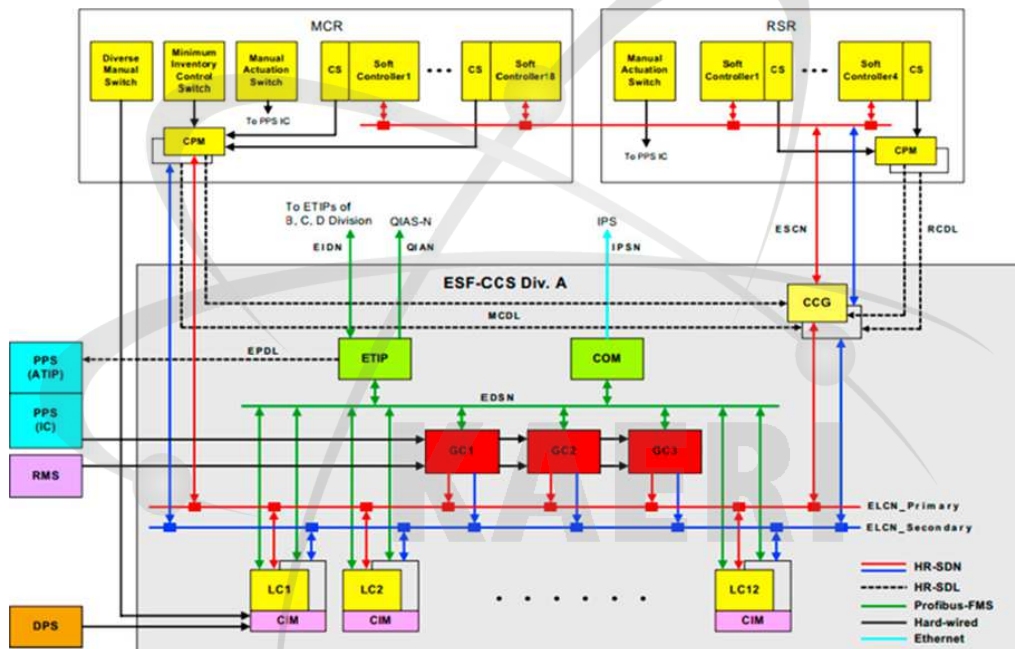


그림 9. 공학적안전설비-기기제어계통(ESF-CCS) 구성도

안전성 분석을 수행하기 위해 원전에서 발생할 수 있는 사고 및 위험을 표 7과 같이 정의하였다. 여기서 사고 A-1과 A-2는 심각한 인명 피해나 환경오염 등의 결과를 초래하고 이 사고는 위험 H-1과 H-2에 의해 발생할 수 있다. 사고 A-3는 원자로가 손상되어 막대한 경제적 손실을 가져올 수 있는 사고이며 이는 위험 H-3, H-4, H-5에 의해 발생할 수 있다. ESF-CCS에 의해서 동작하는 기능 중 SIAS는 원자로보호계통 중 가장 중요한 기능 중 하나로써 냉각재상실사고와 같은 사고 발생 시 노심냉각에 필요한 비상 냉각수를 공급하는 계통이다. ESF-CCS는 안전주입을 작동시키기 위해 다양한 계통간 제어정보 및 상태정보에 의해서 개시여부를 판단한다. 그림 10은 ESF-CCS의 기능 및 구성기기를 바탕으로 개발된 Control Structure를 나타낸다.

표 7. 원전에서 발생할 수 있는 사고 및 위험 정의

ID	Accidents
A-1	A nuclear power plant system injures or kill people
A-2	A nuclear power plant system pollutes environment
A-3	A reactor is damaged
ID	Hazards
H-1	Radioactive materials leaks out of a reactor
H-2	Radioactive materials leaks out of a plant
H-3	Pressure of a reactor is abnormal
H-4	Temperature of a reactor is abnormal
H-5	Safety functions work on a reactor being normal

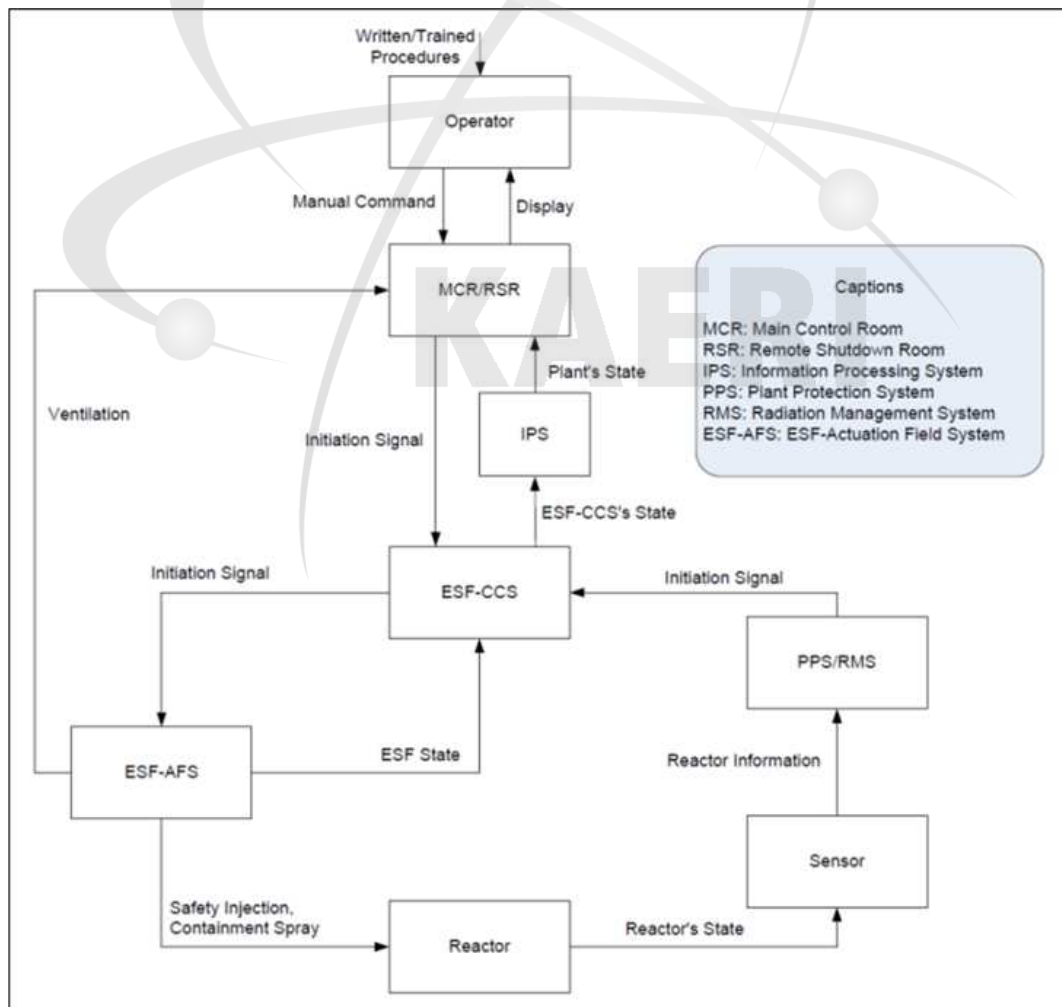


그림 10. ESF-CCS를 포함한 원자로보호계통의 Control Structure

ESF-CCS는 두 가지 제어신호에 의해서 작동된다. 첫째는 설계기준사고 시 원자로보 호계통과 방사선감시계통으로부터 공학적안전설비 구동신호를 받아 동작한다. 둘째는 운 전원으로부터 수동 작동신호를 받아 동작한다. ESF-CCS의 기능 중 SIAS는 RPS로부터 취득되는 가압기 저압력이나 격납용기 고압력 감지에 의해 자동 동작하거나 운전원에 의 해 수동 동작한다. 본 연구보고서에는 SIAS 개시신호가 위험을 초래할 수 있는 경우를 다음과 같이 5가지 경우로 나누어 분석을 수행했으며 그 결과 표 8과 같은 UCA 목록을 밝혀냈다.

- SIAS 개시가 필요할 때 개시되지 않은 경우
- SIAS 개시가 필요하지 않은 경우에 개시된 경우
- SIAS 개시가 필요한 시점보다 너무 이른 시간에 발생한 경우
- SIAS 개시가 필요한 시점보다 너무 늦게 발생한 경우
- SIAS 개시가 너무 이른 시간에 종료된 경우

표 8. ESF-CCS SIAS 개시신호의 UCA 분석 결과

Control Action	Reactor Status		Unsafe Control Actions				
	Pressurizer Pressure	Containment Pressure	Not provided	Provided	Too early	Too late	Stopped too soon
SIAS Initiation by RPS	Normal ($\diamond 1.762$ psia)	Normal (< 1.9 psig)		H-5	H-5	H-5	
		High (≥ 1.9 psig)	H-1 (UCA-1), H-2, H-3			H-1	H-1
	Low (≤ 1.762 psia)	Normal (< 1.9 psig)	H-1, H-2, H-3			H-1	H-1
		High (≥ 1.9 psig)	H-1, H-2, H-3			H-1	H-1

표 8에서 밝혀낸 UCA들 중 UCA-1에 대해 해당 UCA가 발생할 수 있는 원인을 그림 11과 같이 분석한 바 있다. 예를 들어 격납용기의 압력상태가 0.13 kg/cm² 이상일 때 RPS는 자동으로 SIAS 개시를 ESF-CCS에 전송해야하지만 제어 로직 오류, 피드백 신호 오류 등의 원인에 의해 개시 신호가 전달되지 않을 수 있다.

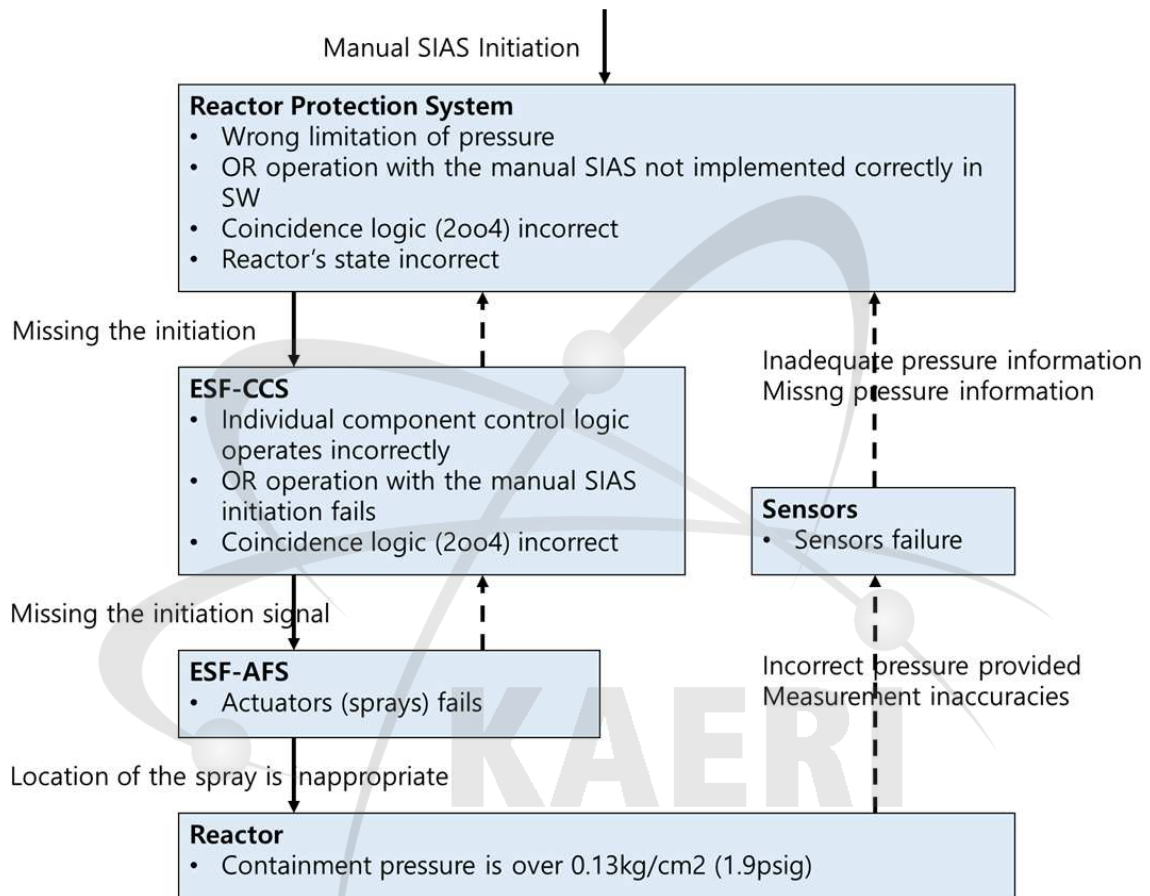


그림 11. ESF-CCS의 UCA-1에 대한 원인 분석 결과



제3장

하나로 운영 프로세스 모델링

제1절 분석 절차

제2절 계통 친숙화

제3절 계통 운영 자료 분석

제4절 계통 STPA모델 개발

제5절 계통 UCA 도출 및 검토



제3장 하나로 운영 프로세스 모델링

제1절 분석 절차

본 연구의 목적은 STAMP/STPA 체계를 토대로 하나로 CNS계통 운영 프로세스를 모델링하고, 해당 모델을 기초로 원자로 불시정지를 유발할 수 있는 UCA를 도출하는 것이다. 도출된 UCA는 하나로 CNS계통 및 계통 운영 프로세스의 안전성을 개선하는데 기초자료로 활용될 수 있다. 본 연구에서 수행된 STPA 분석절차는 그림 12에 정리된 바와 같이 1) 계통 친숙화, 2) 계통 운영 자료 검토, 3) 계통 STPA 모델(Control Structure) 개발, 4) 계통 UCA 도출 및 검토의 과정에 따라 수행되었다.

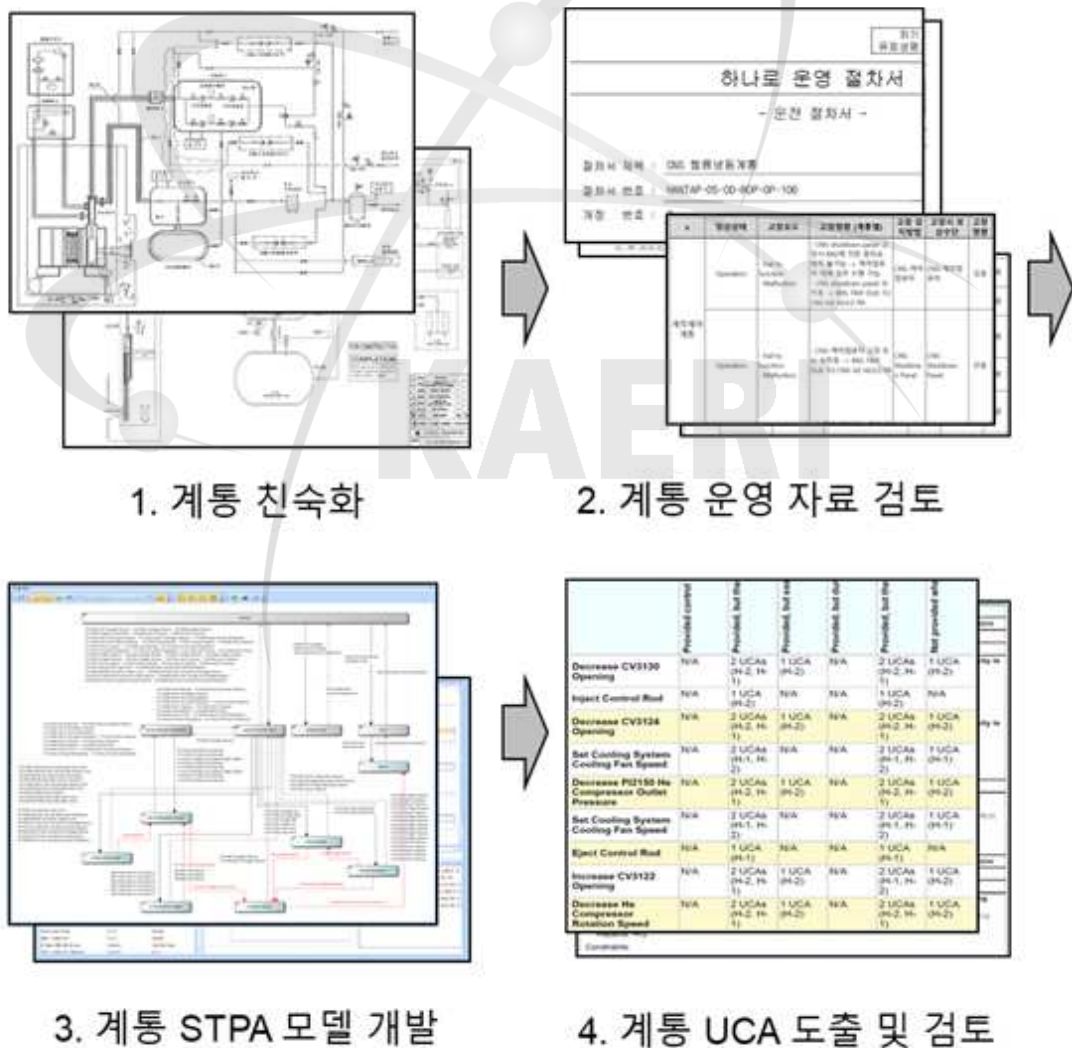


그림 12. 하나로 원자로 불시정지 STPA 분석 절차

제2절 계통 친숙화

친숙화란 분석 수행 이전 혹은 수행 중에 분석 대상인 CNS계통의 설계, 운전 및 정비에 관련된 자료를 수집 및 검토하여 정확한 운영 프로세스 모델링이 가능하도록 분석 대상을 이해하는 과정을 말한다. 구체적인 수행 과정은 관련 설계 문서를 수집 및 검토하며, 실제 운전, 시험 및 정비에 대한 정보를 수집함으로써 분석 대상 원자로의 기계적, 관리적 운전 특성을 이해하는 것이다. 또한 정상 및 특수조건 하에서 연구로 운전에 대한 이해를 위하여 여러 계통 운전절차서 자료를 수집하고 검토하여야 한다. 이러한 연구로 친숙화 작업은 STPA 분석 수행 중 계속 이어지게 되며, 이러한 과정을 통해 보다 정확한 연구용원자로 및 CNS계통 설계 및 운전 정보를 분석에 반영하게 된다. 본 하나로 연구로 친숙화 과정 중 검토한 문서 및 수행 행위 등은 다음과 같다.

- 설계문서(P&ID)
- 안전성분석보고서(SAR; Safety Analysis Report)
- 계통 운전절차서 (정상 및 비상운전절차서, 정주기점검절차서 등)
- 기타 문서 (관련 기술보고서)
- 운전원 면담 및 현장답사

하나로 CNS계통은 계통의 명칭과 같이 냉중성자의 생산을 그 주목적으로 하는데, 원자로의 열중성자를 20K 액체수소 감속재에 통과시키는 과정을 통해 CNS을 생산한다 [14]. 이와 같이 감속재로써 액체수소를 사용하고 있기 때문에 CNS계통에서 가장 심각한 사고는 외부로부터의 공기가 침투하거나 내부의 수소가 외부로 누설됨으로 발생할 수 있다. 그러므로 RRS는 원자로 정지변수로서 CNS 수소계통 내 압력을 감시하며, 비정상 상태가 감지될 시 원자로 정지논리에 의해 트립 신호가 발생된다. 관련 정지변수명은 수소계통 고압력과 저압력으로써 다음과 같은 원인에 의해 발생 할 수 있다.

- 수소계통 고압력(CNS 수소계통 내 압력이 200kPa 이상)
 - 정상운전 상태에서 헬륨냉동기 비정상(냉각헬륨의 공급 중단) → 열사이편 루프 내 액체수소 기화 → 수소계통 압력 상승
 - 헬륨냉동기 과냉각 → 수소계통 내 액체수소의 결빙 및 고착 → 열사이편 루프 차단 → 액체수소 기화 → 수소계통 압력 상승
 - 수소가스의 과다 충전 (작업자 실수) → 수소계통 압력 상승

○ 수소계통 저압력(CNS 수소계통 내 압력이 120kPa 이하)

- 헬륨냉동기 제어기능 비정상 → 액체수소 과냉각 → 수소계통 압력 하락
- 수소계통 누설 → 수소계통 압력 하락

CNS계통 수소 압력은 수소계통에 설치되어 있는 압력전송기를 통해 감시되며, 헬륨냉동계통과 보조 계통 중 하나인 냉각수 계통에 의해 조절된다. 수소계통은 헬륨냉동계통의 운전에 따라 피동적으로 운전되며 헬륨냉동계통에서 발생하는 압축열은 최종적으로 냉각수계통에 의해 제거된다. CNS계통 공정흐름도는 그림 13과 같으며 각 계통에 대한 설명은 다음과 같다.

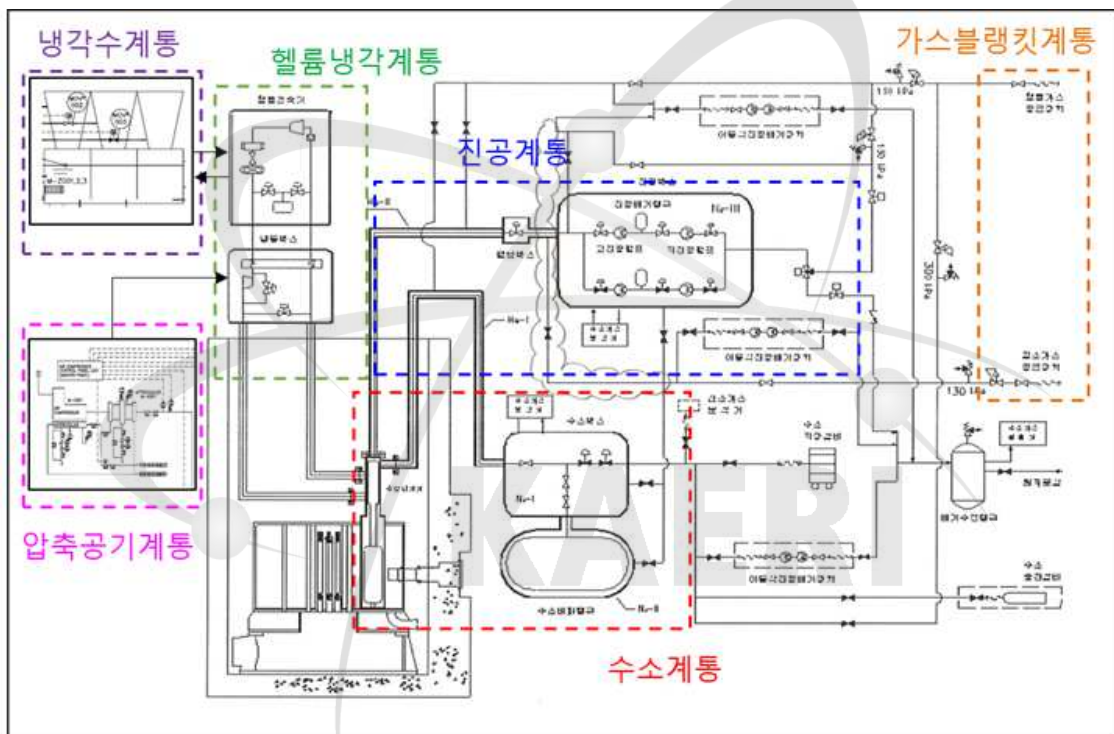


그림 13. 하나로 CNS 공정계통 흐름도

1. 수소계통

수소계통[14]은 열사이클 회로형성을 위한 수소의 공급과 회수를 위한 계통으로 완전 밀폐형 순환계통이며, 헬륨냉동계통의 운전에 따라 피동적으로 운전되며 계통 내부에 수소의 원활한 흐름에 장애가 되는 어떠한 장치도 설치되지 않는다. 수소계통은 수조 내에 설치되는 수조내기기(IPA; In-Pool Assembly)의 연결플랜지로부터 CNS공정실에 설치되는 수소박스내의 밸브 매니폴드를 거쳐 수소버퍼탱크까지의 기기 및 배관을 포함한다. 수소계통은 수소버퍼탱크, 수소버퍼탱크와 IPA 집합체 사이의 밸브매니폴드, 밸브매

니폴드가 내장된 수소박스, 수소충전설비, 수소저장설비 등으로 구성되며 CNS 공정실에 설치된다. 수소계통의 구성, 배관 및 제어계측은 수소계통 P&ID (HANCNS-772-MC-H001)에 나타나 있으며 그림 14와 같다[15]. 수소버퍼탱크로부터 IPA까지의 모든 기기 및 배관의 주변에는 가스블랭킷계통이 설치되며, 가스블랭킷계통은 수소와 공기, 수소와 원자로 수소수 사이의 2차 방벽을 구성한다. 수소계통의 가스블랭킷은 수소버퍼탱크, 수소박스, 수소박스와 IPA 집합체 사이 배관 등의 3개 부분이 독립적으로 적용되며, 서로 연결되지 않는다. 수소버퍼탱크 및 수소박스 블랭킷에는 질소가 채워지고, 수소박스와 IPA 집합체 사이 배관 블랭킷에는 저온 수소에 의한 응축을 방지하기 위하여 헬륨이 채워진다. 수소계통의 운전을 위한 압력신호전송기는 수소박스 내에 3중으로 설치되며, RRS에서는 2-out-of-3 논리에 따라 비정상 상태를 판단하여 원자로 정지신호를 발생한다.

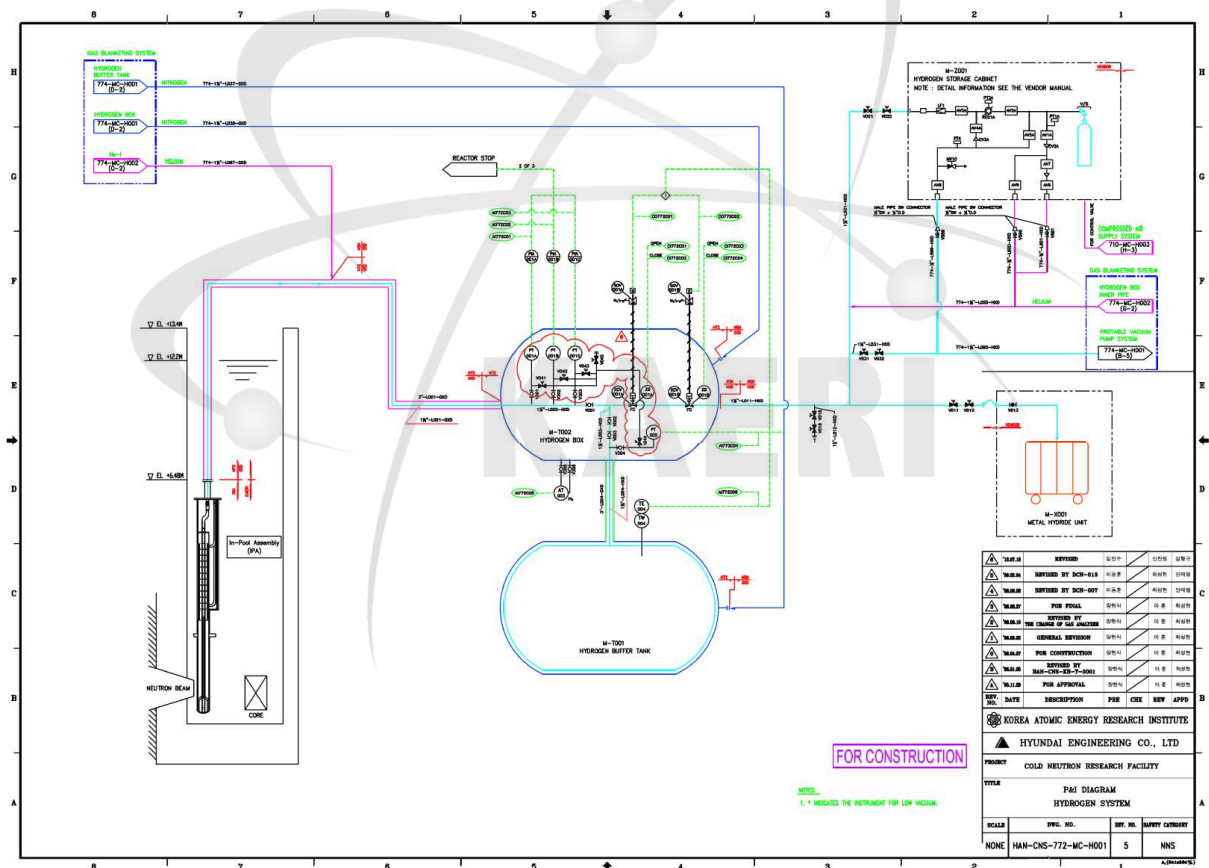


그림 14. 하나로 CNS-수소계통 계통도

2. 진공계통

진공계통[16, 17]은 IPA 집합체의 액체수소 열사이펀, 감속재용기 등의 극저온 부품들의 단열을 위하여 진공용기 내부 진공도를 공정진공도($1.33\text{E}-6 \text{ kPa(a)}$) 이하로 유지하기 위한 계통이다. 정상운전 시 진공계통으로부터 발생하는 배기가스는 배기수집탱크에 포집되고, 내부의 수소가스 농도를 확인하여 3.5% 미만인 경우 원자로실로 배출한다. 진공계통은 그림 15와 같이 진공 펌프, 진공배관 및 밸브, 진공배기 탱크, 배기수집 탱크, 진공박스 및 밸브박스로 구성된다. 펌프시스템은 운전용과 대기용 두 세트로 구성되어 있으며 각 세트는 저진공펌프 1대와 고진공펌프 1대로 구성된다. 정상운전 시 고진공펌프 단독운전 중에 배출되는 배기가스는 진공배기탱크에 저장되며, 진공배기탱크의 압력이 상승하게 되면 저진공펌프가 가동된다. CNS 시설계통의 정상운전 중 계통의 진공도가 정상운전압력 범위를 벗어나는 경우에는 운전원이 필요한 조치를 취할 수 있도록 단계별로 경보를 발생시키며, IPA와 연결되는 주배관의 압력이 특정 설정값을 초과할 경우는 원자로 정지 등의 조치가 취해질 수 있도록 제어실에 경보를 발생시킨다.

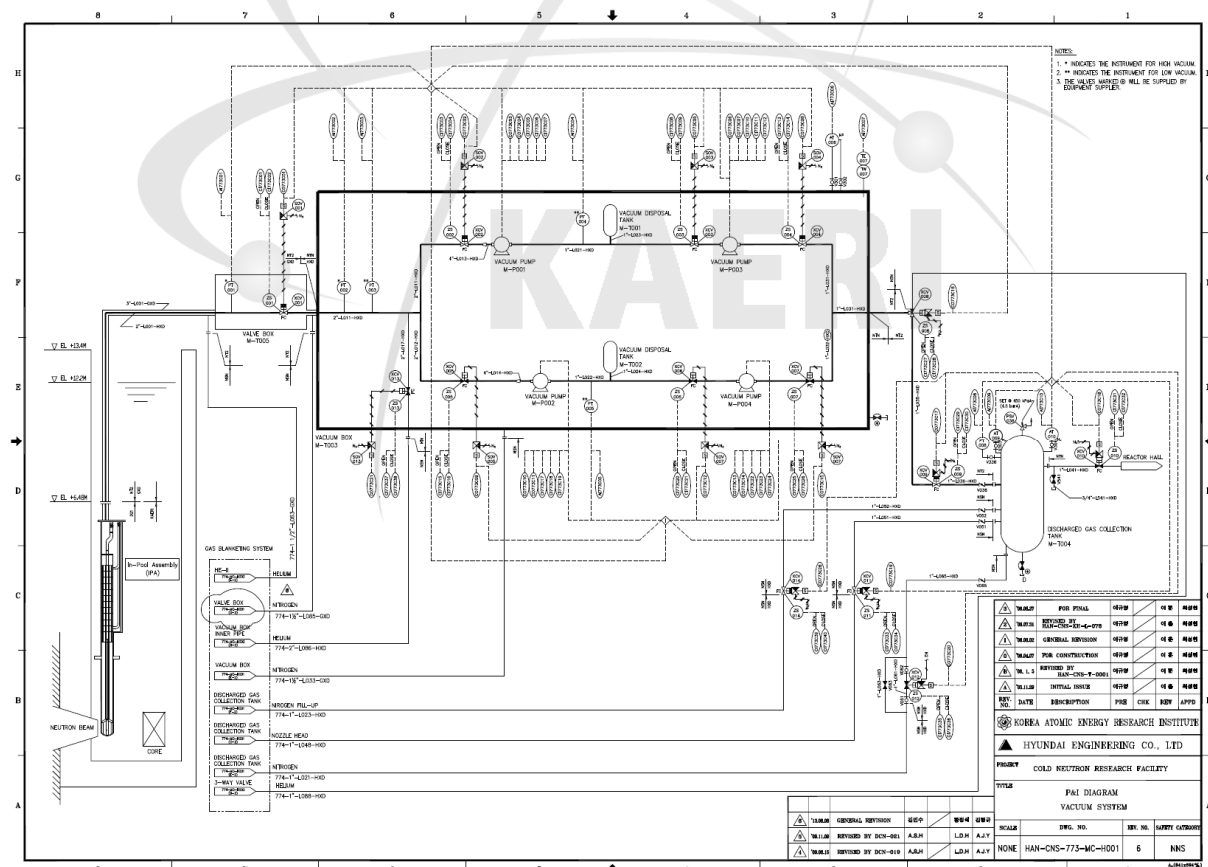


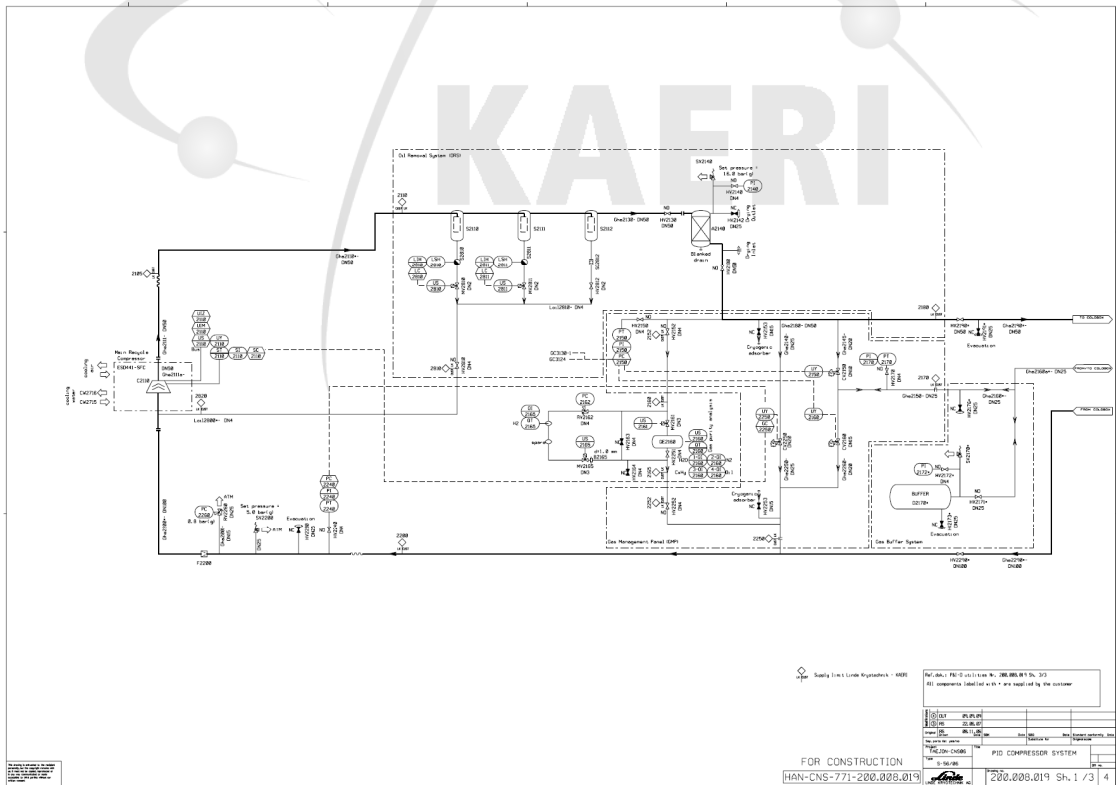
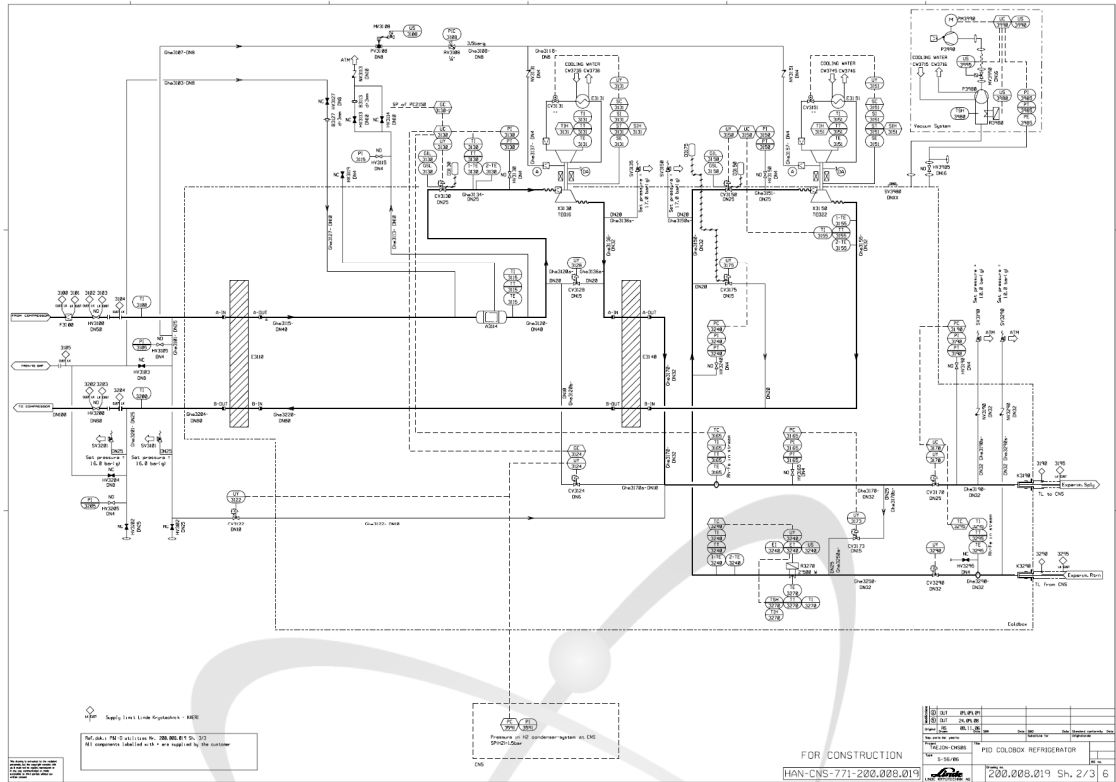
그림 15. 하나로 CNS-진공계통 계통도

3. 헬륨냉동계통

헬륨냉동계통[18]은 하나로의 냉증성자 수직공에 설치되는 IPA에 부하된 발열량으로 기화된 수소를 저온 헬륨가스와의 열교환으로 응축시키는 과정에서 열을 제거하는 계통이다. CNS 감속재인 수소가스를 충전하고 있는 수소계통 내 액체수소를 저온운전조건인 $152 \pm 3\text{kPa(a)}$, 21K로 유지하면서 액체수소/기체수소 2상(열사이펀)을 유지하기 위해 헬륨냉동계통은 1500W이상의 냉동용량을 생산하며 헬륨압축부분(헬륨압축기, 가스제어 계통 등)과 헬륨팽창부분(열교환기, 팽창터빈 등)으로 구성된다.

헬륨팽창부분인 냉동박스는 그림 16과 같이 두 개의 열교환기와 팽창터빈, 유량을 조절하기 위한 자동공압밸브들로 구성된다[19]. 헬륨압축부분에서 유입된 헬륨가스는 열교환기를 거치면서 팽창터빈을 거쳐서 나와 헬륨압축기 저압 측으로 유입될 gas와 열교환 공정을 거쳐 온도가 낮아진다. 이렇게 온도가 낮아진 고압의 gas는 일차 팽창터빈을 거치면서 온도가 낮아지게 되고 이렇게 온도가 낮아진 중고압의 gas는 다시 열교환기를 거치면서 온도가 더 낮아진다. 저온의 헬륨gas는 IPA내 열교환기로 유입되면서 수소가스와 열교환공정을 통해 수소가스를 냉각시키고 액화시켜 IPA내 감속재용기에 액체수소를 충전한다. 이 때, IPA로 유입되는 헬륨gas의 온도를 수소가스의 삼중점 초과로 유지하기 위해 일차 열교환기를 통과한 후 유입되는 gas(warm gas)를 유입시키도록 관련 자동공압밸브의 개도율이 조절된다. 수소가스와 열교환 공정 후 되돌아오는 헬륨gas는 이차 팽창터빈을 거치고 열교환기를 거치면서 온도가 상온에 가깝게 상승한다. 냉동 박스 저온모드 운전 초기에는 팽창터빈의 회전속도가 낮기 때문에 모든 팽창터빈 전단에는 우회밸브를 두어 운전 중 팽창터빈에서 흡수하지 못하는 유량은 우회밸브를 통해 흐르고 다시 팽창터빈을 거쳐서 나오는 저온의 헬륨gas와 혼합되어 다음 단계로 흘러간다.

헬륨압축부분은 그림 17과 같이 헬륨가스를 압축하는 헬륨압축기, 헬륨버퍼탱크, 오일 제거계통 등으로 구성된다[19]. 헬륨압축기는 헬륨 압축 시 발생하는 열에 의해 헬륨 gas의 온도 증가를 최소화하기 위해 오일과 같이 압축시키며 발생하는 압축열을 제거하기 위해 가스냉각기와 오일냉각기가 설치되어 있으며, 냉각수 계통에서 냉각수가 공급되어 열을 최종적으로 제거한다. 헬륨냉동계통에서 필요한 gas는 헬륨버퍼탱크 내에 충전되어 있으며, 헬륨압축기가 기동될 때 계통에 고압력을 생성하기 위해 헬륨버퍼탱크에서 가스를 공급하며 내부 온도가 낮아짐에 따라 감소된 압력을 설정값으로 유지하기 위해 헬륨버퍼탱크에서 필요한 gas가 헬륨냉각계통의 주요 루프로 공급된다. 헬륨냉동계통의 밸브/펌프류 기기들은 헬륨냉동계통 전용 제어컴퓨터에 의해 자동 제어된다.



4. 가스블랭킷계통

가스블랭킷계통[20]은 수소계통을 외기 및 경수로부터 격리시키며, 예기치 않은 상황에서 수소의 외부누출을 방지하고, 진공용기를 포함한 IPA내부로 공기 및 경수가 유입되지 않도록 일정 압력의 블랭킷가스로 보호층을 구성한다. 특히 IPA내부로 공기 및 경수가 유입되는 것을 막기 위하여 블랭킷가스를 대기압보다 높게 충전하여 CNS를 보호하고 수소계통에서 유입 가능한 수소의 농도를 희석하기 위하여 탱크 내로 블랭킷가스를 공급한다. 또한 진공계통의 배기수집탱크 내로 대기가 유입되는 것을 막기 위하여 블랭킷가스를 대기압보다 높게 충전하고 유입되는 수소의 농도를 희석하기 위하여 탱크 내로 블랭킷가스를 공급한다.

가스블랭킷계통의 블랭킷가스는 방사화 가능성이 있는 구역에는 불활성기체인 헬륨가스를 사용하며 그 외 구역에는 질소가스를 사용한다. 또한, 극저온 부품들이 설치되어 있는 IPA와 직접 연결되는 가스블랭킷에는 빙점이 높은 질소가스 대신에 헬륨가스를 적용하여 유사시 IPA로 블랭킷가스가 유입되더라도 동결되지 않도록 하고, 상온으로 유지되는 가스블랭킷에는 질소가스를 사용한다. 가스블랭킷이 사용되는 구역은 다음과 같다.

○ 헬륨 가스

- He-I: IPA와 수소박스를 연결하는 수소공급배관의 외부 배관
- He-II: IPA와 진공계통 내 밸브박스를 연결하는 진공배관의 외부 배관
- He-III: 진공계통 내 밸브박스

○ 질소 가스

- N2-I: 수소계통 내 수소박스
- N2-II: 수소계통 내 수소버퍼탱크
- N2-III: 진공계통 내 진공박스

진공용기를 포함한 가스블랭킷계통은 그림 18, 19과 같이 진공용기, 자동밸브로부터 질소가스 저장실린더와 가스 저장실린더까지의 배관 및 밸브류, 블랭킷가스를 배기하기 위한 이동식 진공배기장치부터 배기수집탱크와 연결된 자동차단밸브까지의 연결배관 및 밸브류를 포함한다[21, 22]. 각 구역의 블랭킷가스 공급은 별도의 자동감압밸브를 통하여 이루어지며 각 구역별로 차단밸브, 압력계측기 및 전송기가 설치된다.

5. 냉각수계통

냉각수 계통[23]은 CNS계통의 기동 및 정상 운전 시 헬륨냉동계통에서 발생하는 열을 제거할 수 있는 냉각수를 공급하는 계통이다. 냉각수 계통은 1차 순환계통과 2차 순환계통으로 구성된다. 1차 순환계통에서 순환되는 냉각수는 헬륨냉동계통의 압축기 및 냉동박스에서 발생하는 열을 흡수하여 2차 순환계통의 냉수에 열을 전달한다.

그림 20은 1차 순환계통을 나타내며 열교환기를 통과하여 33℃가 된 냉각수는 1차 냉각펌프를 통과하여 헬륨압축기와 냉동박스에 냉각수를 공급한다[24]. 1차 냉각펌프도 100% 용량의 2대로 구성되어 있고 운전 중 한대만을 기동하고 나머지 한 대는 예비용으로 설계되었다. 헬륨압축기와 냉동박스를 통과한 냉각수는 온도가 38℃로 상승하고 열교환기를 거쳐 다시 33℃로 냉각된다.

그림 21은 2차 순환계통을 나타내며 1차 계통과 열교환을 하여 온도가 상승한 2차 냉각수는 냉각탑을 통과하면서 온도가 하강한다[25]. 32℃로 온도가 하강된 2차 냉각수는 2차 냉각펌프를 통하여 열교환기로 이동하는데 냉각펌프는 100% 용량의 2대로 1대만 정상운전 시 사용하고 나머지 한 대는 예비용으로 사용된다. 열교환기를 통과하고 난 후의 냉각수는 온도가 37℃까지 상승하고 다시 냉각탑으로 이동한다. 냉각탑 하부에는 2차 계통의 수질을 관리하기 위하여 전체 순환수량의 2% 가 냉각수 여과설비로 이동하도록 설계되어 있다 [26].

냉각탑은 3개의 셀로 구성되어 있으며 각각의 셀은 고속/저속으로 운전 가능한 냉각팬이 설치되어 있다. 냉각팬의 운전은 자동 및 수동운전이 가능하며, 자동 운전 시 냉각탑의 출구온도가 32℃ 이하가 될 수 있도록 제어논리가 구성되어 있다. 냉각팬에는 운전 상태를 확인할 수 있도록 진동측정기가 부착되며 진동값은 실시간으로 제어실에 전달된다. 만약 측정된 진동값이 설정치를 초과할 경우에는 경보를 발생하고 냉각팬은 정지한다. 또한, 동결기 냉각탑 운전 시 하부수조의 결빙을 방지하기 위해서 동결방지용 전기히터가 설치되며 냉각수의 온도가 4℃ 이하로 떨어질 경우 자동 작동되도록 구성한다. 냉각수 공급계통에서 운전되는 각 펌프의 토출압력이 설정값 이하로 떨어질 경우 경보를 발하고 예비용 펌프가 기동된 후 해당펌프는 정지한다. 또한, 펌프 후단에 유량계를 설치하여 펌프의 토출량이 지시되도록 구성하고 냉각탑 하부수조의 수위가 설정값 이하로 떨어질 경우 경보를 발하고 냉각수계통은 정지한다.

6. 압축공기계통

압축공기계통[27]은 실험동의 실험기와 헬륨냉동계통에서 요구되는 충분한 양의 계기용 압축공기와 작업용 압축공기를 공급하는 계통이다. 압축공기 계통은 50% 용량의 공기압축기 3대, 공기저장탱크 1대, 100% 용량 2개의 건조탑을 가진 건조기 1대와 관련 배관 및 계기류 등으로 구성된다. 공기 압축기는 선행, 후행 및 예비용으로 구분되어 유지보수를 원활히 하고, 압축공기 요구유량에 맞추어 운전된다. 생산된 공기는 압축공기 저장탱크 후단에서 작업용 및 계기용으로 나누어지며 작업용은 건조기를 거치지 않고 직접 공급되고 계기용은 건조기를 거쳐 건조된 상태로 공급된다.

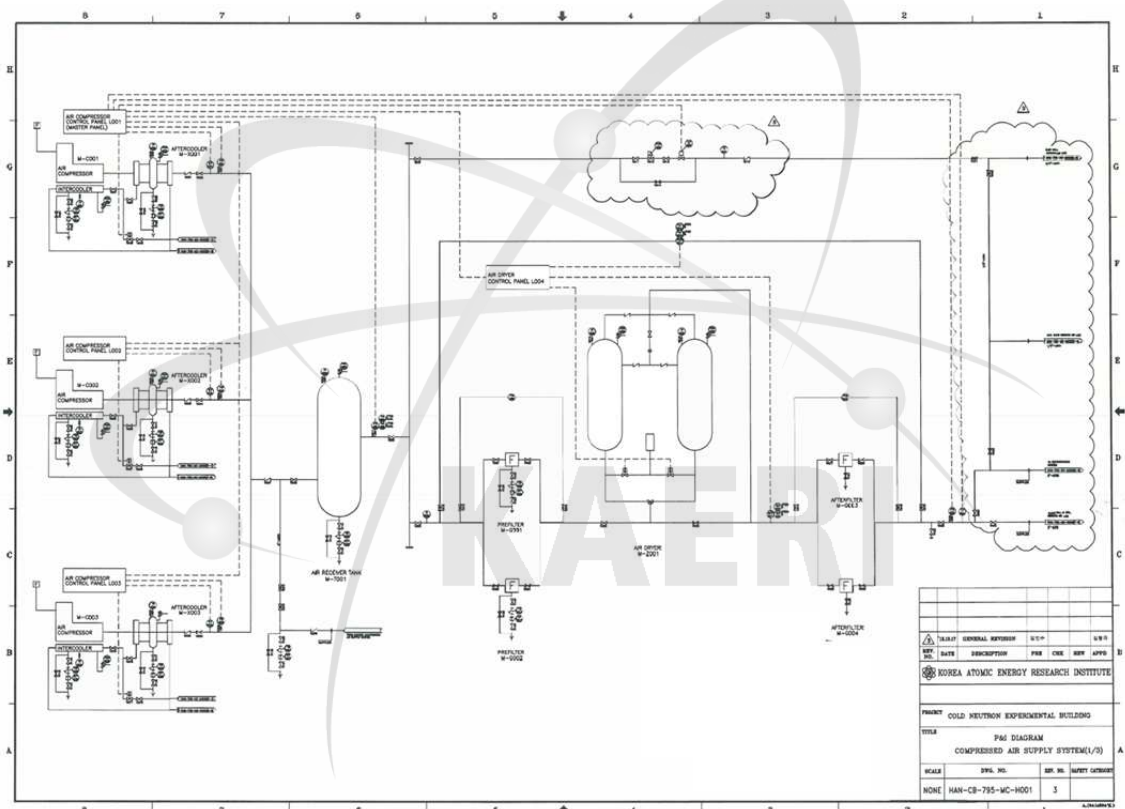


그림 22. 하나로 CNS-압축공기계통 계통도

7. 계측제어계통

계측제어 계통[14]은 CNS의 운전과 보호에 필요한 모든 신호의 취득, 운전원에게 정보 제공, 및 수동 또는 자동으로 조치를 취하는데 관련된 기기를 포함하며, 정지계통과 제어 및 감시계통으로 구성된다. CNS 시설의 정상운전은 하나로 원자로 제어실에서 수행하며, 원자로건물 내에 위치한 CNS 기기실 및 실험동 부속기기동 헬륨압축기실에 별도의 운전용 조작반을 설치하여 시설의 기동, 정지, 조작, 감시 및 이상 시의 조치 등을 수행한다. 원자로 제어실, CNS 계측실, 및 헬륨압축기실에 설치되는 운전용 조작반과 주 제어 컴퓨터시스템, 및 냉동기 제어시스템 사이에는 그림 23과 같이 이중화 데이터 네트워크를 구성하여 신호를 교환한다[28].

시스템 내의 모든 운전정보는 CNS계측실과 하나로 제어실의 운전원 조작반으로 전송되며 상시 감시된다. CNS의 정상운전은 하나로 제어실에 위치하는 통합 운전원 조작반에서 수행하기 때문에, 제어컴퓨터는 통합 운전원 조작반과 CNS계측실에 위치하는 운전원 조작반과 통신을 할 수 있도록 설계한다. CNS의 운전모드는 정지, 기동, 정상운전 모드로 이루어진다. 운전원이 조작을 정확하고 빠르게 취할 수 있도록 운전화면은 계층적 구조로 구성되며, 운전 이력의 저장 또는 각종 트렌드 표시 및 비교 등 상태감시나 경보기능이 가능하다. 헬륨냉동계통의 제어 및 감시는 제작사가 제공하는 별도의 독립적인 제어기에 의하여 이루어지며 CNS 제어컴퓨터와 통신이 가능하다.

제어컴퓨터는 CNS의 제어 및 감시기능 뿐만 아니라 원자로 및 CNS 주요기기에 대한 정지 기능을 수행한다. 표 9는 RRS에 의한 원자로 정지변수와 정지 설정값을 나타낸다. CNS계통에 의하여 원자로와 CNS 주요기기를 자동 정지시키는 신호는 수소계통 고압력 신호와 수소계통 저압력 신호이다. CNS에 의한 원자로 정지 기능에 다중성 및 다양성을 확보하기 위하여 제어컴퓨터와 별도의 정지패널을 설치하여, 제어컴퓨터가 고장 나더라도 원자로 정지가 가능하도록 설계되었다. 원자로 정지 기능을 수행하는 수소계통 내 수소압력 계측기는 신뢰성을 높이기 위하여 3중화로 설계되었으며 2-out-of-3 논리를 통하여 정지신호를 발생시킨다. CNS에 의한 원자로 정지는 하나로의 원자로 제어계통과 연계되며, 정지변수 측정치가 정지 설정치를 초과할 경우에 원자로 제어계통의 제어봉 구동용 마그네틱 클러치의 전원을 차단하고 제어봉을 낙하시켜 원자로를 정지시킨다.

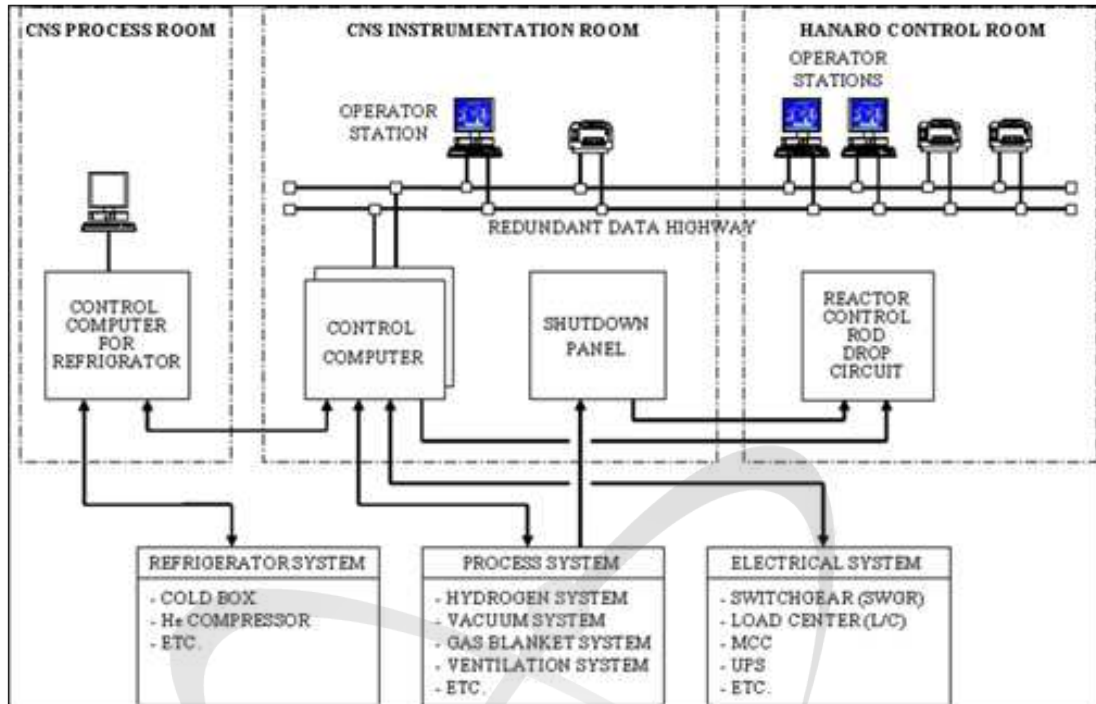


그림 23. 한라로 CNS-계측제어계통 구성도

표 9. 공정계통 비정상상태에 의한 원자로 정지변수

번호	정지변수	정지설정치	비고
1	원자로 출구측 온도	$T_{sp} = T_{sc} + 15.5$ (°C)	T_{sp} : 정지설정치 T_{sc} : 이차계통 HX 입구측 온도
2	반사체계통 유량	below 60% nominal flow for 60 sec	반사체계통의 냉각상실사고 발생 시 원자로 정지
3	반사체 출구측 온도	50°C	반사체계통의 출구온도가 50°C 이상일 경우 원자로 정지
4	수동 정지	-	-
5	냉각수 저유량	422 kg/sec	일차 냉각수 유량이 422 kg/sec 이하일 경우 원자로 정지
6	CNS 수소계통 고압력	200 kPa(a)	CNS 수소압력이 200 kPa(a) 이상일 때 원자로 정지
7	CNS 수소계통 저압력	120 kPa(a)	CNS 수소압력이 120 kPa(a) 이하일 때 원자로 정지

제3절 계통 운영 자료 분석

하나로는 원자력안전법 시행규칙 제 29조(규칙 제 5조, 20조 준용) “발전소 운전절차서 및 비상운전절차서의 시범적용에 관한 사항”에 의거하여 정상운전 및 비정상, 비상운전에 관한 절차서를 운전절차서로 구비하여 사용해왔다. 하나로의 운전절차서는 HANTAP-05-OD-ROP-TA-08(운영 절차서 작성 및 개정, 관리) 절차[29]에 따라 운전절차서로 통합하여 개정 및 관리되고 있으며 이 절차서에는 절차서의 작성, 검토, 승인에 관한 사항 및 절차서의 관리, 절차서 종류별 목차, 작성 양식 등을 규정하고 있다. 절차서의 작성, 검토 및 승인 절차는 하나로 운영 품질 보증 절차서 QAP-HA-6.2(하나로 운영 서류 관리)에 따라 수행하도록 명시되어 있다. CNS계통에 대한 운전절차서의 항목은 표 10과 같다.

표 10. 하나로 CNS계통 운전절차서 목록

절차서 번호	절차서 제목	참고문헌
HANTAP-05-OD-ROP-OP-01 (Rev.16)	원자로 기동 및 정지	[30]
HANTAP-05-OD-ROP-OP-101 (Rev. 4)	CNS 기동 및 정지	[31]
HANTAP-05-OD-ROP-OP-102 (Rev. 3)	CNS 수소계통	[32]
HANTAP-05-OD-ROP-OP-103 (Rev. 1)	CNS 진공계통	[33]
HANTAP-05-OD-ROP-OP-104 (Rev. 1)	CNS 가스블랭킷계통	[34]
HANTAP-05-OD-ROP-OP-105 (Rev. 1)	CNS 냉각수계통	[35]
HANTAP-05-OD-ROP-OP-106 (Rev. 3)	CNS 헬륨냉동계통	[36]
HANTAP-05-OD-ROP-OP-112 (Rev. 1)	CNS 공기압축기	[37]

각 운전절차서는 CNS계통을 기동하고 정지하는 종합운전절차서와 CNS계통을 구성하고 있는 각 하위계통별 운전절차서로 구분된다. 기동 및 정지 운전절차서는 CNS계통을 하나로 운전과 연계하여 정지 상태에서 고온 운전으로 도달하는 과정과 다시 정지 상태에 이르는 전 과정을 다루고 있다. 각 계통별 운전절차서는 계통 내 밸브류 및 펌프류의 배열, 각 계통에 속한 기기의 수동 및 자동 운전 방법, 경보 목록 및 각 경보별 조치 방법이 기술되어 있으며 운전절차서의 기본구성은 아래와 같다.

○ 목적 (절차서 1.0절)

- 기동 및 정지 절차서의 목적이 기술되어 있다.

○ 참조 (절차서 2.0절)

- 기동 및 정지 절차서 작성에 인용된 참고 문헌이 기술되어 있다.

○ 주의 사항 (절차서 3.0절)

- CNS계통 및 원자로와의 연계 운전 시 운전원이 주의하여야 할 사항이 기술되어 있다.

○ 초기 조건 (절차서 4.0절)

- CNS 수소계통을 기동하기 전에 확인하여야 할 사항(작업의뢰서나 부적합 사항에 대한 조치, 관련 계통 운전 가능 상태 확인)이 기술되어 있다.

○ 절차 (절차서 5.0절)

- 기동 및 정지 운전하는 절차가 기술되어 있으며, 운전 전 준비 절차, 기동 절차, 정상 운전 절차, (필요 시)원자로와의 연계운전 절차, 운전 중 감시 절차, 정지 절차 등으로 나뉘어져 있다.

○ 붙임 (절차서 6.0절)

- CNS계통의 정상 운전 시 밸브류, 펌프류의 상태 및 운전 절차 관련 자료들이 기술되어 있다.

본 연구에서는 원자로가 기동하고 안전하게 정지될 때까지 원자로 불시정지를 유발하는 CNS계통 내 UCA을 도출하고자 각 계통의 운전절차서, 특히 절차(5.0절)내 운전 절차들을 분석하였다. 표 11은 진공계통의 운전절차서(HANTAP-05-OD-ROP-OP-103)를 분석한 결과를 나타낸다. 운전절차서에 명시되어 있는 각 운전 절차(기기 제어)는 조치 특성에 따라 확인 및 제어조치로 나눌 수 있으며 조치 대상에 따라 제어컴퓨터(자동 운전), 운전원(수동 운전)으로 나눌 수 있다. 여기서 확인 조치는 운전 중 제어컴퓨터 혹은 운전원이 CNS계통 운전변수들을 감시하는 하는 절차를 의미하고, 제어 조치는 감시된 변수들을 바탕으로 혹은 정해진 제어로직에 의해 운전 중 제어컴퓨터나 운전원이 밸브류, 펌프류들을 제어하는 절차를 의미한다.

위와 같이 CNS 각 계통의 운전절차서를 바탕으로 표 12와 같이 운전원 및 제어컴퓨터에 의한 확인 조치 및 제어 조치들을 분석하였으며 도출된 운전절차들은 STAMP모델,

즉 Control Structure를 개발하는데 활용되었다. STPA 분석 방법론에 기준하여 볼 때, CNS계통 운전 시 운전원 및 제어컴퓨터가 각 계통의 운전 변수들을 감시하고 확인하는 행위는 Controller와 Controlled Process간의 Feedback으로 고려할 수 있다. 그리고 감시된 변수들을 바탕으로 운전원 및 제어컴퓨터의 Process Model에 의해 적절한 제어기능을 제어가 필요한 기기에 제공하는 행위는 Controller와 Controlled Process간의 Control Action으로 고려할 수 있다.

표 11. 하나로 CNS-진공계통 운전절차서 분석 결과

운전 절차	조치 구분	조치 대상	절차서 목차
밸브박스 압력신호(PT-001)	확인 조치	제어컴퓨터	OP-103 5.1.7절
진공박스 압력신호(PT-003)	확인 조치	제어컴퓨터	OP-103 5.1.3절
진공배기탱크(M-T001) 압력 신호 (PT-004)	확인 조치	제어컴퓨터	OP-103 5.1.5절-1 OP-103 5.1.6절-1
진공배기탱크(M-T002) 압력 신호 (PT-005)	확인 조치	제어컴퓨터	OP-103 5.1.5절-1 OP-103 5.1.6절-1
배기수집탱크(M-T004) 압력 신호 (PT-008)	확인 조치	제어컴퓨터	OP-103 5.1.5.1절
수소가스검출 신호(AT-009)	확인 조치	제어컴퓨터	OP-103 5.1.5.1절
수소가스검출 신호(AT-010)	확인 조치	제어컴퓨터	OP-103 5.1.5.1절
Stream A 스위치 설정	제어 조치	운전원	OP-103 5.2.2절
Stream B 스위치 설정	제어 조치	운전원	OP-103 5.2.2절
Vacuum Com 스위치 설정	제어 조치	운전원	OP-103 5.2.2절
XCV-001 밸브 열림	제어 조치	제어컴퓨터	OP-103 5.1.7절
		운전원	OP-103 5.2.2절-8
XCV-001 밸브 닫힘	제어 조치	제어컴퓨터	OP-103 5.1.7절
XCV-002 밸브 열림	제어 조치	제어컴퓨터	OP-103 5.1.6절-5
		운전원	OP-103 5.2.2절-8
XCV-002 밸브 닫힘	제어 조치	제어컴퓨터	OP-103 5.1.5절-2
XCV-003 밸브 열림	제어 조치	제어컴퓨터	OP-103 5.1.5절-6
		운전원	OP-103 5.2.2절-6
XCV-003 밸브 닫힘	제어 조치	제어컴퓨터	OP-103 5.1.6절-2
XCV-004 밸브 열림	제어 조치	제어컴퓨터	OP-103 5.1.5절-5
		운전원	OP-103 5.2.2절-5
XCV-004 밸브 닫힘	제어 조치	제어컴퓨터	OP-103 5.1.6절-4
XCV-005 밸브 열림	제어 조치	제어컴퓨터	OP-103 5.1.6절-5
XCV-005 밸브 닫힘	제어 조치	제어컴퓨터	OP-103 5.1.5절

XCV-006 밸브 열림	제어 조치	제어컴퓨터	OP-103 5.1.5절
		운전원	OP-103 5.2.2절-6
XCV-006 밸브 닫힘	제어 조치	제어컴퓨터	OP-103 5.1.6절-2
XCV-007 밸브 열림	제어 조치	제어컴퓨터	OP-103 5.1.5절-5
		운전원	OP-103 5.2.2절-5
XCV-007 밸브 닫힘	제어 조치	제어컴퓨터	OP-103 5.1.6절-4
XCV-008 밸브 열림	제어 조치	제어컴퓨터	OP-103 5.1.5절-4
		운전원	OP-103 5.2.2절-4
XCV-008 밸브 닫힘	제어 조치	제어컴퓨터	OP-103 5.1.6절-6
XCV-009 밸브 열림	제어 조치	제어컴퓨터	OP-103 5.1.5절-5
		제어컴퓨터	OP-103 5.1.5.2절
		운전원	OP-103 5.2.2절-3
XCV-009 밸브 닫힘	제어 조치	제어컴퓨터	OP-103 5.1.5.1절
			OP-103 5.1.6절-7
XCV-010 밸브 열림	제어 조치	제어컴퓨터	OP-103 5.1.5.1절-1
XCV-010 밸브 닫힘	제어 조치	제어컴퓨터	OP-103 5.1.5.2절
		운전원	OP-103 5.2.2절-1
XCV-012 밸브 열림	제어 조치	제어컴퓨터	OP-103 5.1.5.1절-2
고진공펌프(M-P001) 기동	제어 조치	제어컴퓨터	OP-103 5.1.3절
		운전원	OP-103 5.2.2절-7
고진공펌프(M-P001) 정지	제어 조치	제어컴퓨터	OP-103 5.1.3절
고진공펌프(M-P002) 기동	제어 조치	제어컴퓨터	OP-103 5.1.3절
		운전원	OP-103 5.2.2절-7
고진공펌프(M-P002) 정지	제어 조치	제어컴퓨터	OP-103 5.1.3절
저진공펌프(M-P003) 기동	제어 조치	제어컴퓨터	OP-103 5.1.3절
		운전원	OP-103 5.2.2절-2
저진공펌프(M-P003) 정지	제어 조치	제어컴퓨터	OP-103 5.1.3절
저진공펌프(M-P004) 기동	제어 조치	제어컴퓨터	OP-103 5.1.3절
		운전원	OP-103 5.2.2절-2
저진공펌프(M-P004) 정지	제어 조치	제어컴퓨터	OP-103 5.1.3절

표 12. 하나로 CNS계통 관련 운전원 및 제어컴퓨터 운전절차 목록

계통	확인조치	제어조치
수소계통	수소계통수소 압력(772-PT001A/B/C)	정지판넬 버튼 소등 (CNS Trip Reset)
	수소계통수소 압력(772-PT002)	정지판넬 버튼 소등 (Manual HANARO Trip Bypass)
	헬륨압축기 고압력 (771-PI2150)	.
	헬륨압축기 저압력 (771-PI2240)	.
	IPA 헬륨 회수온도(771-TI3295)	.
	IPA 헬륨 공급온도(771-TI3165)	.
	팽창터빈 입구밸브 (771-CV3130) 개도율	.
	정지판넬 점등 확인 (CNS Trip Reset)	.
	정지판넬 점등 확인 (Manual HANARO Trip Bypass)	.
	수소박스 질소불랭킷영역 수소 농도 (772-AT003)	.
	수소박스 질소불랭킷영역 압력 (774-PT008)	.
	수소배관 내부 헬륨불랭킷영역 압력 (774-PT030)	.
	수소배관 IPA 헬륨불랭킷영역 압력(774-PT018)	.
진공계통	진공배기탱크 압력 (773-PT004)	저진공펌프 기동 (773-M-P003)
	진공배기탱크 압력 (773-PT005)	고진공펌프 기동 (773-M-P001)
	배기수집탱크 압력 (773-PT008)	저진공펌프 정지 (773-M-P003)
	수소검출신호 (773-AT009)	고진공펌프 정지 (773-M-P001)
	수소검출신호 (773-AT010)	진공배기용 밸브 열음 (773-XCV001)
	밸브박스 전단 압력 (773-PT001)	진공배기용 밸브 열음 (773-XCV002)

	진공박스 전단 압력 (773-PT003)	진공배기용 밸브 열음 (773-XCV003)
	.	진공배기용 밸브 열음 (773-XCV004)
	.	진공배기용 밸브 열음 (773-XCV008)
	.	진공배기용 밸브 열음 (773-XCV009)
	.	진공배기용 밸브 열음 (773-XCV010)
	.	수소가스배기용 밸브 열음 (773-XCV012)
	.	진공배기용 밸브 닫음 (773-XCV001)
	.	진공배기용 밸브 닫음 (773-XCV002)
	.	진공배기용 밸브 닫음 (773-XCV003)
	.	진공배기용 밸브 닫음 (773-XCV004)
	.	진공배기용 밸브 닫음 (773-XCV008)
	.	진공배기용 밸브 닫음 (773-XCV009)
	.	수소가스배기용 밸브 닫음 (773-XCV010)
가스블랭킷계통	질소공급측 질소 공급용 압력 (774-PT001)	헬륨가스공급용 차단밸브 열음 (774-XCV001)
	질소버퍼탱크 질소 블랭킷 공급용 압력 (774-PT002)	헬륨가스공급용 차단밸브 닫음 (774-XCV001)
	진공박스 질소 블랭킷 공급용 압력 (774-PT007)	.
	수소박스 질소 블랭킷 공급용 압력 (774-PT008)	.
	수소버퍼탱크 질소 블랭킷 공급용 압력 (774-PT009)	.
	밸브박스 질소 블랭킷 공급용 압력 (774-PT020)	.
	차단밸브 질소 공압 공급용 압력 (774-PT031)	.

	헬륨공급측 헬륨 공급용 압력 (774-PT010)	.
	진공플랜지 헬륨 블랭킷 공급용 압력 (774-PT013)	.
	수소플랜지 헬륨 블랭킷 공급용 압력 (774-PT014)	.
	진공박스 내부배관 헬륨 블랭킷 공급용 압력 (774-PT021)	.
	진공계통 3-way 밸브 질소 공급용 압력 (774-PT022)	.
	수소박스 내부배관 헬륨 블랭킷 공급용 압력 (774-PT030)	.
냉각수계통	2차 냉각펌프 토출압력 (710-PS013)	2차 냉각펌프 기동 (710-M-P001)
	2차 냉각펌프 토출압력 (710-PS014)	2차 냉각펌프 기동 (710-M-P002)
	냉각탑 수조 수위 (710-LIT-001)	2차 냉각펌프 정지 (710-M-P001)
	냉각수 출구온도 (710-TE008)	2차 냉각펌프 정지 (710-M-P002)
	냉각팬-1 진동 (710-YE002)	냉각팬-1 회전속도 증가 (710-F001)
	냉각팬-2 진동 (710-YE003)	냉각팬-2 회전속도 증가 (710-F002)
	냉각팬-3 진동 (710-YE004)	냉각팬-3 회전속도 증가 (710-F003)
	2차 냉각펌프 출구압력 (710-PI011)	냉각팬-1 회전속도 감소 (710-F001)
	2차 냉각펌프 출구압력 (710-PI012)	냉각팬-2 회전속도 감소 (710-F002)
	1차 냉각펌프 토출압력 (710-PS025)	냉각팬-3 회전속도 감소 (710-F003)
	1차 냉각펌프 토출압력 (710-PS026)	냉각팬-1 정지 (710-F001)
	1차 냉각펌프 출구압력 (710-PI023)	냉각팬-2 정지 (710-F002)

	1차 냉각펌프 출구압력 (710-PI024)	냉각팬-3 정지 (710-F003)
	1차 냉각펌프 출구온도(710-TE030/031)	보충수 공급밸브-1 닫음 (710-MOV001)
	.	보충수 공급밸브-2 닫음 (710-MOV002)
	.	보충수 공급밸브-3 닫음 (710-MOV003)
	.	보충수 공급밸브-1 열음 (710-MOV001)
	.	보충수 공급밸브-2 열음 (710-MOV002)
	.	보충수 공급밸브-3 열음 (710-MOV003)
	.	1차 냉각펌프 기동 (710-M-P003)
	.	1차 냉각펌프 기동 (710-M-P004)
	.	1차 냉각펌프 정지 (710-M-P003)
	.	1차 냉각펌프 정지 (710-M-P004)
헬륨냉동계통	헬륨압축기 고압력 (771-PI2150)	1차 팽창터빈 우회밸브 개도를 증가 (771-CV3124)
	헬륨압축기 저압력 (771-PI2240)	1차 팽창터빈 우회밸브 개도를 감소 (771-CV3124)
	헬륨버퍼탱크 압력 (771-PI2170)	1차 팽창터빈 전단밸브 개도를 증가 (771-CV3130)
	헬륨저온배관 헬륨 압력 (771-PI3190)	1차 팽창터빈 전단밸브 개도를 감소 (771-CV3130)
	1차 팽창터빈 전단 헬륨 압력 (771-PI3240)	warm gas 주입밸브 개도를 증가 (771-CV3122)
	warm gas 주입밸브 개도를 (771-CV3124)	warm gas 주입밸브 개도를 감소 (771-CV3122)
	헬륨압축기 우회밸브 개도를 (771-CV2250)	헬륨압축기 우회밸브 개도를 증가 (771-CV2250)
	헬륨가스 순도 (771-QI2160)	헬륨압축기 우회밸브 개도를 감소 (771-CV2250)
	헬륨가스 순도 (771-QI2160)	헬륨압축기 우회밸브 개도를 증가 (771-CV2150)
	1차 팽창터빈 후단 헬륨 온도 (771-TI3165)	헬륨압축기 우회밸브 개도를 감소 (771-CV2150)

	IPA 헬륨회수 온도 (771-TI3295)	헬륨압축기 우회밸브 개도율 증가 (771-CV2160)
	IPA 헬륨회수 온도 (771-TI3295)	헬륨압축기 우회밸브 개도율 감소 (771-CV2160)
	2차 팽창터빈 후단 헬륨 온도 (771-TI3155)	헬륨압축기 회전속도 증가 (771-C2110)
	1차 팽창터빈 냉각수 온도 (771-TI3131)	헬륨압축기 회전속도 감소 (771-C2110)
	2차 팽창터빈 냉각수 온도 (771-TI3151)	IPA 격리밸브 개도율 증가 (771-CV3170)
	.	IPA 격리밸브 개도율 감소 (771-CV3170)
	.	IPA 우회밸브 개도율 증가 (771-CV3173)
	.	IPA 우회밸브 개도율 감소 (771-CV3173)
	.	2차 팽창터빈 전단밸브 개도율 증가 (771-CV3150)
	.	2차 팽창터빈 전단밸브 개도율 감소 (771-CV3150)
	.	2차 팽창터빈 우회밸브 개도율 증가 (771-CV3175)
압축공기계통	압축기-1 토출압력 (795-PS001)	2차 팽창터빈 우회밸브 개도율 감소 (771-CV3175)
	압축기-2 토출압력 (795-PS002)	압축기-2 기동 (795-M-C002)
	압축기-3 토출압력 (795-PS003)	압축기-3 기동 (795-M-C003)
	.	압축기-1 정지 (795-M-C001)
	.	압축기-2 정지 (795-M-C002)
	.	압축기-3 정지 (795-M-C003)

제4절 계통 STPA모델 개발

CNS 수소 압력 비정상에 의한 원자로 불시정지는 수소계통에 존재하면서 수소 압력에 직접적으로 영향을 미치는 기기의 고장에 의해 발생할 수 있다. 하지만 보다 포괄적인 분석을 위해, 기기 또는 관련 계통간의 상호작용, 인적 요인과의 상호작용, 그리고 환경과 같은 시스템 외적인 요인까지 통합적으로 고려한 분석이 필요할 것으로 판단된다. 본 연구에서는 MIT에서 새롭게 제안된 위험 분석 방법인 STAMP/STPA기법을 적용하여 사고가 시스템을 구성하는 요소(기기 및 인적요소 등) 간 제어문제에 의해 발생할 수 있는 위험요소들을 모델링하고 발생 가능한 불시정지 시나리오를 분석하고자 한다. 본 분석은 Klappir사에서 개발한 RMStudio v5.6 프로그램을 활용하여 수행하였다. RMStudio 프로그램의 실행 및 사용법은 부록 1을 참고하도록 한다.

STPA의 수행단계는 크게 4단계로 수행되며, 분석 대상과 관련한 사고(Loss) 및 위험(Hazard)을 정의하는 1단계, Control Structure를 도식화하는 2단계, 안전하지 못한 제어행위(UCA)를 도출하는 3단계, Causal Factor와 원인 시나리오(Causal Scenario)를 도출하는 4단계로 이루어진다. 본 연구에서는 하나로 CNS계통에 대한 불시정지 시나리오를 도출하는 목적으로 STPA 3단계 절차까지 수행하였다.

1. 사고 및 위험 정의

STPA 1단계에서는 분석의 목적과 관련하여 사고와 위험을 정의한다. 일반적인 STAMP/STPA체계에서는 사고(Accident)를 인명 피해, 재산 손실, 환경오염과 같은 시스템 수준의 사고로 정의하지만, 본 연구에서는 하나로 CNS계통 이상으로 인한 불시정지 시나리오를 도출하기 위해 표 13과 같이 CNS계통 및 원자로 연계 운전 중 발생할 수 있는 원자로 불시정지를 STPA분석의 사고(Accident)로 정의하였다. 또한, 사고를 유발할 수 있는 각 계통의 이상 현상들을 표 13과 같이 STPA분석의 위험(Hazard)으로 정의하였다. 사고와 위험간의 관계는 그림 24와 같다. 본 분석에서 정의된 위험(Hazard)의 물리적 속성은 하나로 계통별 이상현상에 대한 자세한 열수력학적 분석을 통해 도출될 수 있을 것으로 기대된다.

RRS기능 중 수소계통 내 수소 고압력 및 저압력 트립은 외부 공기 침투에 의한 수소-산소결합 폭발이나 수소의 외부 유출과 같은 설계기준사고를 방지하기 위해 설정된 CNS 관련 원자로 정지변수이다. 수소계통 내 수소 열사이편은 헬륨냉동계통, 진공계통 등 다양한 계통들의 복합적인 운전에 의해 조절된다. 따라서 RRS는 다양한 계통간 제어정보 및 상태정보를 기반으로 트립신호 개시여부를 판단한다. 예를 들어, CNS에서 진공계통의 주요 기능은 IPA내 진공용기의 진공상태를 유지하는 것인데, 진공계통 이상(H-2)은 원

자로수조와 IPA의 단열의 실패를 발생시킬 수 있고 이는 RRS에 의한 수소계통 고압력 트립 신호 발생까지 이어질 수 있다. 또 다른 예로 CNS에서 헬륨냉동계통의 주요 기능은 수소계통의 열사이편을 유지하는 것으로, 헬륨냉동계통 이상(H-3)은 헬륨냉동계통의 수소계통에 대한 과냉각 혹은 과열을 발생시킬 수 있고 이는 RRS에 의한 수소계통 고압력 혹은 저압력 트립 신호 발생까지 이어질 수 있다.

표 13. 하나로 CNS계통 관련사고 및 위험 목록 정의

사고(Accidents)	
A-1	CNS Hydrogen High Pressure Trip Signal Generation by RRS
A-2	CNS Hydrogen Low Pressure Trip Signal Generation by RRS
위험(Hazards)	
H-1	Abnormal "Maintain Hydrogen Thermo-Cyphon" by HRS
H-2	Abnormal "Maintain Vacuum in IPA VB" by VS
H-3	Abnormal "Provide Cooling Water to HET in HRS" by CWS
H-4	Abnormal "Provide Gas to Air Operated Valves in VS" by GBS
H-5	Abnormal "Power Uprate/Cutback Operation" by "ICS"
H-6	Abnormal "Provide Air to Air Operated Valves in HRS" by "CAS"

- RRS: Reactor Regulating System (원자로제어계통)
- HRS: Helium Refrigeration System (헬륨냉동계통)
- IPA: In-Pool Assembly (IPA)
- VB: Vacuum Box (진공박스)
- HET: Heat Exchanger Tube (열교환기)
- CWS: Cooling Water System (냉각수계통)
- GBS: Gas Blanket System (가스블랭킷계통)
- ICS: Instrumentation and Control System (계측제어계통)
- CAS: Compressed Air System (압축공기계통)

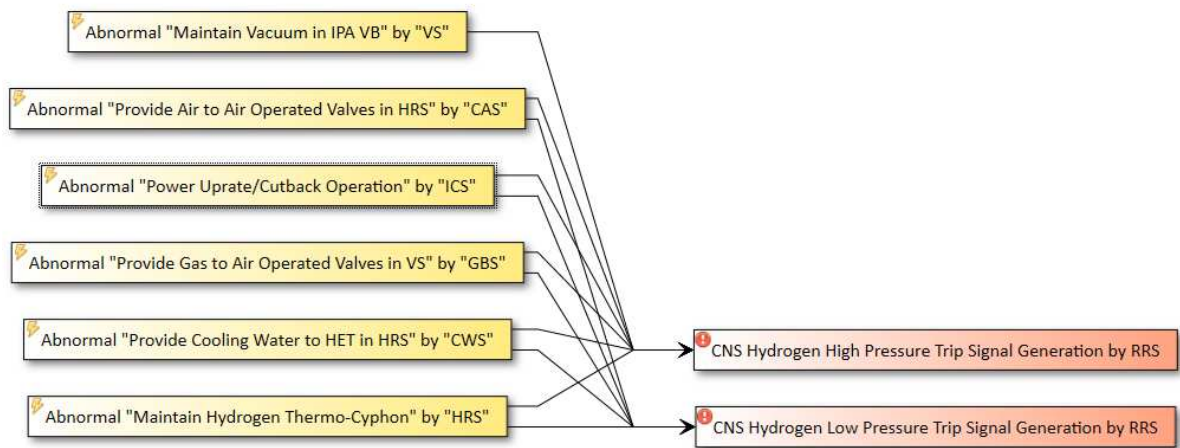


그림 24. 하나로 CNS계통 관련사고-위험간 관계 정의

2. Control Structure 개발

그림 25는 CNS계통 포함, CNS운전과 관련된 계통들을 STAMP에 기반한 Control Structure로 나타낸 것이다. 해당 Control Structure는 하나로 CNS계통 운전을 위해 존재하는 다양한 시스템들을 시스템이론 관점으로 나타내고 있으며, 계통간의 제어(Control action)는 검은 실선으로, 계통간의 물리적(열역학적) 관계성은 빨간 실선으로, 그리고 반응(Feedback)은 점선으로 표기하였다. 본 Control Structure는 총 6개의 제어주체(Controller), 7개의 제어객체(Controlled Process), 103개의 제어(Control Action), 122개의 반응(Feedback)으로 이루어지며 계통간의 제어 및 반응 목록은 표 14, 15와 같다.

표 14. Control Structure내 CNS계통간의 제어(Control Action) 목록

명칭	제어주체(Controller)	제어객체(Controlled Process)
710-F001 (Decrease Cooling Fan Speed)	Control Computer (Main)	Cooling Water System
710-F001 (Increase Cooling Fan Speed)	Control Computer (Main)	Cooling Water System
710-F001 (Stop Cooling Fan)	Control Computer (Main)	Cooling Water System
710-F002 (Decrease Cooling Fan Speed)	Control Computer (Main)	Cooling Water System
710-F002 (Increase Cooling Fan Speed)	Control Computer (Main)	Cooling Water System
710-F002 (Stop Cooling Fan)	Control Computer (Main)	Cooling Water System
710-F003 (Decrease Cooling Fan Speed)	Control Computer (Main)	Cooling Water System
710-F003 (Increase Cooling Fan Speed)	Control Computer (Main)	Cooling Water System

710-F003 (Stop Cooling Fan)	Control Computer (Main)	Cooling Water System
710-MOV-001 (Close Cooling Tower Inlet Valve)	Control Computer (Main)	Cooling Water System
710-MOV-002 (Close Cooling Tower Inlet Valve)	Control Computer (Main)	Cooling Water System
710-MOV-003 (Close Cooling Tower Inlet Valve)	Control Computer (Main)	Cooling Water System
710-MOV-004 (Open Cooling Tower Bypass Valve)	Control Computer (Main)	Cooling Water System
710-M-P001 (Start Secondary Cooling Water Standby Pump)	Control Computer (Main)	Cooling Water System
710-M-P001 (Stop Secondary Cooling Water Main Pump)	Control Computer (Main)	Cooling Water System
710-M-P002 (Start Secondary Cooling Water Standby Pump)	Control Computer (Main)	Cooling Water System
710-M-P002 (Stop Secondary Cooling Water Main Pump)	Control Computer (Main)	Cooling Water System
710-M-P003 (Start Primary Cooling Water Standby Pump)	Control Computer (Main)	Cooling Water System
710-M-P003 (Stop Primary Cooling Water Main Pump)	Control Computer (Main)	Cooling Water System
710-M-P004 (Start Primary Cooling Water Standby Pump)	Control Computer (Main)	Cooling Water System
710-M-P004 (Stop Primary Cooling Water Main Pump)	Control Computer (Main)	Cooling Water System
771-C2110 (Decrease He Compressor Rotation Speed)	Control Computer (Refrigerator)	Helium Refrigeration System
771-C2110 (Increase He Compressor Rotation Speed)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV2150 (Decrease Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV2150 (Increase Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV2160 (Decrease Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV2160 (Increase Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV2250 (Decrease Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV2250 (Increase Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3122 (Decrease Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3122 (Increase Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3124 (Decrease Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System

771-CV3124 (Increase Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3130 (Decrease Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3130 (Increase Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3150 (Decrease Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3150 (Increase Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3170 (Decrease Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3170 (Increase Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3173 (Decrease Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3173 (Increase Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3175 (Decrease Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-CV3175 (Increase Valve Opening)	Control Computer (Refrigerator)	Helium Refrigeration System
771-X3130 (Stop Helium Expansion Turbine-1)	Control Computer (Refrigerator)	Helium Refrigeration System
771-X3150 (Stop Helium Expansion Turbine-2)	Control Computer (Refrigerator)	Helium Refrigeration System
773-M-P001(Start Train A Main High Vacuum Pump)	Control Computer (Main)	Vacuum System
773-M-P001 (Start Train A High Vacuum Pump)	Operator	Control Computer (Main)
773-M-P001(Stop Train A Main High Vacuum Pump)	Control Computer (Main)	Vacuum System
773-M-P002(Start Train B Main High Vacuum Pump)	Control Computer (Main)	Vacuum System
773-M-P002 (Start Train A High Vacuum Pump)	Operator	Control Computer (Main)
773-M-P002 (Stop Train B Main High Vacuum Pump)	Control Computer (Main)	Vacuum System
773-M-P003 (Start Train A Low Vacuum Pump)	Control Computer (Main)	Vacuum System
773-M-P003 (Start Train A Low Vacuum Pump)	Operator	Control Computer (Main)
773-M-P003 (Stop Train A Low Vacuum Pump)	Control Computer (Main)	Vacuum System
773-M-P004 (Start Train B Low Vacuum Pump)	Control Computer (Main)	Vacuum System
773-M-P004 (Start Train B Low Vacuum Pump)	Operator	Control Computer (Main)

773-M-P004 (Stop Train B Low Vacuum Pump)	Control Computer (Main)	Vacuum System
773-XCV001 (Close Valve)	Control Computer (Main)	Vacuum System
773-XCV001 (Open Valve)	Control Computer (Main)	Vacuum System
773-XCV-001 (Open Valve)	Operator	Control Computer (Main)
773-XCV002 (Close Valve)	Control Computer (Main)	Vacuum System
773-XCV002 (Open Valve)	Control Computer (Main)	Vacuum System
773-XCV-002 (Open Valve)	Operator	Control Computer (Main)
773-XCV003 (Close Valve)	Control Computer (Main)	Vacuum System
773-XCV003 (Open Valve)	Control Computer (Main)	Vacuum System
773-XCV-003 (Open Valve)	Operator	Control Computer (Main)
773-XCV004 (Close Valve)	Control Computer (Main)	Vacuum System
773-XCV004 (Open Valve)	Control Computer (Main)	Vacuum System
773-XCV005 (Close Valve)	Control Computer (Main)	Vacuum System
773-XCV005 (Open Valve)	Control Computer (Main)	Vacuum System
773-XCV006 (Close Valve)	Control Computer (Main)	Vacuum System
773-XCV006 (Open Valve)	Control Computer (Main)	Vacuum System
773-XCV-006 (Open Valve)	Operator	Control Computer (Main)
773-XCV007 (Close Valve)	Control Computer (Main)	Vacuum System
773-XCV007 (Open Valve)	Control Computer (Main)	Vacuum System
773-XCV-007 (Open Valve)	Operator	Control Computer (Main)
773-XCV008 (Close Valve)	Control Computer (Main)	Vacuum System
773-XCV008 (Open Valve)	Control Computer (Main)	Vacuum System
773-XCV-008 (Open Valve)	Operator	Control Computer (Main)
773-XCV009 (Close Valve)	Control Computer (Main)	Vacuum System
773-XCV009 (Open Valve)	Control Computer (Main)	Vacuum System
773-XCV009 (Open Valve)	Operator	Control Computer (Main)

773-XCV010 (Close Valve)	Control Computer (Main)	Vacuum System
773-XCV010 (Close Valve)	Operator	Control Computer (Main)
773-XCV010 (Open Valve)	Control Computer (Main)	Vacuum System
773-XCV012 (Open Valve)	Control Computer (Main)	Vacuum System
795-M-C001 (Start Air Compressor-1)	Control Computer (Main)	Air Compression System
795-M-C001 (Stop Air Compressor-1)	Control Computer (Main)	Air Compression System
795-M-C002 (Start Air Compressor-2)	Control Computer (Main)	Air Compression System
795-M-C002 (Stop Air Compressor-2)	Control Computer (Main)	Air Compression System
795-M-C003 (Start Air Compressor-3)	Control Computer (Main)	Air Compression System
795-M-C003 (Stop Air Compressor-3)	Control Computer (Main)	Air Compression System
795-M-Z001 (Start Air Dryer-1)	Control Computer (Main)	Air Compression System
795-M-Z001 (Stop Air Dryer-1)	Control Computer (Main)	Air Compression System
795-M-Z002 (Start Air Dryer-2)	Control Computer (Main)	Air Compression System
795-M-Z002 (Stop Air Dryer-2)	Control Computer (Main)	Air Compression System
Disable Manual Trip Bypass	Operator	Shutdown Panel
Eject Control Rod	HCCS	Reactor
Eject Control Rod	Operator	HCCS
Enable Manual Trip Bypass	Operator	Shutdown Panel
Inject Control Rod	HCCS	Reactor
Set Reactor Power (Power Cutback)	Operator	HCCS
Set Reactor Power (Power Uprate)	Operator	HCCS
Set Stream A Manual	Operator	Control Computer (Main)
Set Stream B Manual	Operator	Control Computer (Main)
Set Vacuum Com Manual	Operator	Control Computer (Main)

표 15. Control Structure내 CNS계통간의 반응(Feedback) 목록

명칭	제어객체(Controlled Process)	제어주체(Controller)
637-ZI005 A/B/C/D (Control Rod Position)	Reactor	HCCS
637-ZI005 A/B/C/D (Control Rod Position)	Reactor	HCCS
710-LIT001 (Cooling Tower Water Level)	Cooling Water System	Control Computer (Main)
710-LIT001 (Cooling Tower Water Level)	Control Computer (Main)	Operator
710-PI011 (Secondary Cooling Pump Outlet Pressure)	Cooling Water System	Control Computer (Main)
710-PI011 (Secondary Cooling Pump Outlet Pressure)	Control Computer (Main)	Operator
710-PI012 (Secondary Cooling Pump Outlet Pressure)	Cooling Water System	Control Computer (Main)
710-PI012 (Secondary Cooling Pump Outlet Pressure)	Control Computer (Main)	Operator
710-PI023 (Primary Cooling Pump Outlet Pressure)	Control Computer (Main)	Operator
710-PI023 (Primary Cooling Pump Outlet Pressure)	Cooling Water System	Control Computer (Main)
710-PI024 (Primary Cooling Pump Outlet Pressure)	Control Computer (Main)	Operator
710-PI024 (Primary Cooling Pump Outlet Pressure)	Cooling Water System	Control Computer (Main)
710-PS013 (Secondary Cooling Pump Discharge Pressure)	Control Computer (Main)	Operator
710-PS014 (Secondary Cooling Pump Discharge Pressure)	Cooling Water System	Control Computer (Main)
710-PS013 (Secondary Cooling Pump Discharge Pressure)	Control Computer (Main)	Operator
710-PS014 (Secondary Cooling Pump Discharge Pressure)	Cooling Water System	Control Computer (Main)
710-PS025 (Primary Cooling Pump Discharge Pressure)	Control Computer (Main)	Operator
710-PS026 (Primary Cooling Pump Discharge Pressure)	Cooling Water System	Control Computer (Main)
710-PS025 (Primary Cooling Pump Discharge Pressure)	Control Computer (Main)	Operator
710-PS026 (Primary Cooling Pump Discharge Pressure)	Cooling Water System	Control Computer (Main)
710-TE008 (Secondary Cooling Water Outlet Temperature)	Control Computer (Main)	Operator
710-TE008 (Secondary Cooling Water Outlet Temperature)	Cooling Water System	Control Computer (Main)

710-TE030 (Primary Cooling Pump Outlet Temperature)	Control Computer (Main)	Operator
710-TE030 (Primary Cooling Pump Outlet Temperature)	Cooling Water System	Control Computer (Main)
710-YE002/003/004 (Cooling Fan Vibration Level)	Control Computer (Main)	Operator
710-YE002/003/004 (Cooling Fan Vibration Level)	Gas Blanket System	Control Computer (Main)
771-AT-003 (Nitrogen Pressure)	Helium Refrigeration System	Control Computer (Refrigerator)
771-CV2250 (Valve Opening)	Control Computer (Refrigerator)	Control Computer (Main)
771-CV2250 (Valve Opening)	Control Computer (Main)	Operator
771-CV2250 (Valve Opening)	Helium Refrigeration System	Control Computer (Refrigerator)
771-CV3130 (Valve Opening)	Control Computer (Refrigerator)	Control Computer (Main)
771-CV3130 (Valve Opening)	Control Computer (Main)	Operator
771-CV3130 (Valve Opening)	Helium Refrigeration System	Control Computer (Refrigerator)
771-PI2150 (Helium Compressor Pressure)	Control Computer (Refrigerator)	Control Computer (Main)
771-PI2150 (Helium Compressor Pressure)	Control Computer (Main)	Operator
771-PI2150 (Helium Compressor Pressure)	Helium Refrigeration System	Control Computer (Refrigerator)
771-PI2170 (Helium Pressure)	Control Computer (Refrigerator)	Control Computer (Main)
771-PI2170 (Helium Pressure)	Control Computer (Main)	Operator
771-PI2170 (Helium Pressure)	Helium Refrigeration System	Control Computer (Refrigerator)
771-PI2240 (Helium Compressor Pressure)	Control Computer (Refrigerator)	Control Computer (Main)
771-PI2240 (Helium Compressor Pressure)	Control Computer (Main)	Operator
771-PI2240 (Helium Compressor Pressure)	Helium Refrigeration System	Control Computer (Refrigerator)
771-PI3165 (Helium Temperature)	Control Computer (Refrigerator)	Control Computer (Main)
771-PI3165 (Helium Temperature)	Control Computer (Main)	Operator

771-PI3165 (Helium Temperature)	Helium Refrigeration System	Control Computer (Refrigerator)
771-PI3190 (Helium Pressure)	Control Computer (Refrigerator)	Control Computer (Main)
771-PI3190 (Helium Pressure)	Control Computer (Main)	Operator
771-PI3190 (Helium Pressure)	Helium Refrigeration System	Control Computer (Refrigerator)
771-PI3240 (Helium Pressure)	Control Computer (Refrigerator)	Control Computer (Main)
771-PI3240 (Helium Pressure)	Control Computer (Main)	Operator
771-PI3240 (Helium Pressure)	Helium Refrigeration System	Control Computer (Refrigerator)
771-PT3130 (Helium Pressure)	Control Computer (Refrigerator)	Control Computer (Main)
771-PT3130 (Helium Pressure)	Control Computer (Main)	Operator
771-PT3130 (Helium Pressure)	Helium Refrigeration System	Control Computer (Refrigerator)
771-PT3150 (Helium Pressure)	Control Computer (Refrigerator)	Control Computer (Main)
771-PT3150 (Helium Pressure)	Control Computer (Main)	Operator
771-PT3150 (Helium Pressure)	Helium Refrigeration System	Control Computer (Refrigerator)
771-PT3165 (Helium Pressure)	Control Computer (Refrigerator)	Control Computer (Main)
771-PT3165 (Helium Pressure)	Control Computer (Main)	Operator
771-PT3165 (Helium Pressure)	Helium Refrigeration System	Control Computer (Refrigerator)
771-PT3240 (Helium Temperature)	Control Computer (Refrigerator)	Control Computer (Main)
771-PT3240 (Helium Temperature)	Control Computer (Main)	Operator
771-PT3240 (Helium Temperature)	Helium Refrigeration System	Control Computer (Refrigerator)
771-QI2160 (Helium Purity)	Control Computer (Refrigerator)	Control Computer (Main)
771-QI2160 (Helium Purity)	Control Computer (Main)	Operator

771-QI2160 (Helium Purity)	Helium Refrigeration System	Control Computer (Refrigerator)
771-QI2165 (Helium Purity)	Control Computer (Refrigerator)	Control Computer (Main)
771-QI2165 (Helium Purity)	Control Computer (Main)	Operator
771-QI2165 (Helium Purity)	Helium Refrigeration System	Control Computer (Refrigerator)
771-ST3131 (ET-1 Rotation Speed)	Control Computer (Refrigerator)	Control Computer (Main)
771-ST3131 (ET-1 Rotation Speed)	Control Computer (Main)	Operator
771-ST3131 (ET-1 Rotation Speed)	Helium Refrigeration System	Control Computer (Refrigerator)
771-ST3151 (ET-2 Rotation Speed)	Control Computer (Refrigerator)	Control Computer (Main)
771-ST3151 (ET-2 Rotation Speed)	Control Computer (Main)	Operator
771-ST3151 (ET-2 Rotation Speed)	Helium Refrigeration System	Control Computer (Refrigerator)
771-TI3131 (ET-1 Coolant Temperature)	Control Computer (Refrigerator)	Control Computer (Main)
771-TI3131 (ET-1 Coolant Temperature)	Control Computer (Main)	Operator
771-TI3131 (ET-1 Coolant Temperature)	Helium Refrigeration System	Control Computer (Refrigerator)
771-TI3151 (ET-1 Coolant Temperature)	Control Computer (Refrigerator)	Control Computer (Main)
771-TI3151 (ET-1 Coolant Temperature)	Control Computer (Main)	Operator
771-TI3151 (ET-1 Coolant Temperature)	Helium Refrigeration System	Control Computer (Refrigerator)
771-TI3155 (ET-2 Outlet Temperature)	Control Computer (Refrigerator)	Control Computer (Main)
771-TI3155 (ET-2 Outlet Temperature)	Control Computer (Main)	Operator
771-TI3155 (ET-2 Outlet Temperature)	Helium Refrigeration System	Control Computer (Refrigerator)
771-TI3165 (Helium IPA Outlet Temperature)	Control Computer (Refrigerator)	Control Computer (Main)
771-TI3165 (Helium IPA Outlet Temperature)	Control Computer (Main)	Operator

771-TI3165 (Helium IPA Outlet Temperature)	Helium Refrigeration System	Control Computer (Refrigerator)
771-TI3295 (Helium IPA Inlet Temperature)	Control Computer (Refrigerator)	Control Computer (Main)
771-TI3295 (Helium IPA Inlet Temperature)	Control Computer (Main)	Operator
771-TI3295 (Helium IPA Inlet Temperature)	Helium Refrigeration System	Control Computer (Refrigerator)
771-TT3130 (Helium Temperature)	Control Computer (Refrigerator)	Control Computer (Main)
771-TT3130 (Helium Temperature)	Control Computer (Main)	Operator
771-TT3130 (Helium Temperature)	Helium Refrigeration System	Control Computer (Refrigerator)
771-TT3151 (ET-2 Coolant Temperature)	Control Computer (Refrigerator)	Control Computer (Main)
771-TT3151 (ET-2 Coolant Temperature)	Control Computer (Main)	Operator
771-TT3151 (ET-2 Coolant Temperature)	Helium Refrigeration System	Control Computer (Refrigerator)
771-TT3155 (Helium Temperature)	Control Computer (Refrigerator)	Control Computer (Main)
771-TT3155 (Helium Temperature)	Control Computer (Main)	Operator
771-TT3155 (Helium Temperature)	Helium Refrigeration System	Control Computer (Refrigerator)
771-TT3165 (Helium Temperature)	Control Computer (Refrigerator)	Control Computer (Main)
771-TT3165 (Helium Temperature)	Control Computer (Main)	Operator
771-TT3165 (Helium Temperature)	Helium Refrigeration System	Control Computer (Refrigerator)
771-TT3295 (Helium Temperature)	Control Computer (Refrigerator)	Control Computer (Main)
771-TT3295 (Helium Temperature)	Control Computer (Main)	Operator
771-TT3295 (Helium Temperature)	Helium Refrigeration System	Control Computer (Refrigerator)
772-AT003 (Hydrogen Concentration)	Control Computer (Main)	Operator
772-PT001A/B/C (Hydrogen Pressure)	Hydrogen System	Control Computer (Main)
772-PT001A/B/C (Hydrogen Pressure)	Hydrogen System	Shutdown Panel

772-PT001A/B/C (Hydrogen Pressure)	Control Computer (Main)	Operator
772-PT002 (Hydrogen Pressure)	Hydrogen System	Control Computer (Main)
772-PT002 (Hydrogen Pressure)	Hydrogen System	Shutdown Panel
772-PT002 (Hydrogen Pressure)	Control Computer (Main)	Operator
773-PT002 (Vacuum Pressure)	Vacuum System	Control Computer (Main)
773-AT009 (Hydrogen Gas Detector Signal)	Vacuum System	Control Computer (Main)
773-AT010 (Hydrogen Gas Detector Signal)	Vacuum System	Control Computer (Main)
773-PT001 (Vacuum Pressure)	Vacuum System	Control Computer (Main)
773-PT004 (Vacuum Disposal Tank Pressure)	Vacuum System	Control Computer (Main)
773-PT008 (Discharged Gas Collection Tank Pressure)	Vacuum System	Control Computer (Main)
774-PT001 (Nitrogen Pressure)	Gas Blanket System	Control Computer (Main)
774-PT001 (Nitrogen Pressure)	Control Computer (Main)	Operator
774-PT002 (Nitrogen Pressure)	Gas Blanket System	Control Computer (Main)
774-PT002 (Nitrogen Pressure)	Control Computer (Main)	Operator
774-PT007 (Nitrogen Pressure)	Gas Blanket System	Control Computer (Main)
774-PT007 (Nitrogen Pressure)	Control Computer (Main)	Operator
774-PT008 (Nitrogen Pressure)	Gas Blanket System	Control Computer (Main)
774-PT008 (Nitrogen Pressure)	Control Computer (Main)	Operator
774-PT009 (Nitrogen Pressure)	Gas Blanket System	Control Computer (Main)
774-PT009 (Nitrogen Pressure)	Control Computer (Main)	Operator
774-PT010 (Helium Pressure)	Gas Blanket System	Control Computer (Main)
774-PT010 (Helium Pressure)	Control Computer (Main)	Operator
774-PT013 (Helium Pressure)	Gas Blanket System	Control Computer (Main)
774-PT013 (Helium Pressure)	Control Computer (Main)	Operator

774-PT014 (Helium Pressure)	Gas Blanket System	Control Computer (Main)
774-PT014 (Helium Pressure)	Control Computer (Main)	Operator
774-PT018 (Helium Pressure)	Gas Blanket System	Control Computer (Main)
774-PT018 (Helium Pressure)	Control Computer (Main)	Operator
774-PT020 (Nitrogen Pressure)	Gas Blanket System	Control Computer (Main)
774-PT020 (Nitrogen Pressure)	Control Computer (Main)	Operator
774-PT021 (Helium Pressure)	Gas Blanket System	Control Computer (Main)
774-PT021 (Helium Pressure)	Control Computer (Main)	Operator
774-PT022 (Helium Pressure)	Gas Blanket System	Control Computer (Main)
774-PT022 (Helium Pressure)	Control Computer (Main)	Operator
774-PT030 (Helium Pressure)	Gas Blanket System	Control Computer (Main)
774-PT030 (Helium Pressure)	Control Computer (Main)	Operator
774-PT031 (Nitrogen Pressure)	Gas Blanket System	Control Computer (Main)
774-PT031 (Nitrogen Pressure)	Control Computer (Main)	Operator
795-MT001 (Air Moisture)	Air Compression System	Control Computer (Main)
795-PTI001 (Air Pressure)	Air Compression System	Control Computer (Main)
CNS Trip Reset Alarm	Shutdown Panel	Operator
Manual Trip Bypass Alarm	Shutdown Panel	Operator

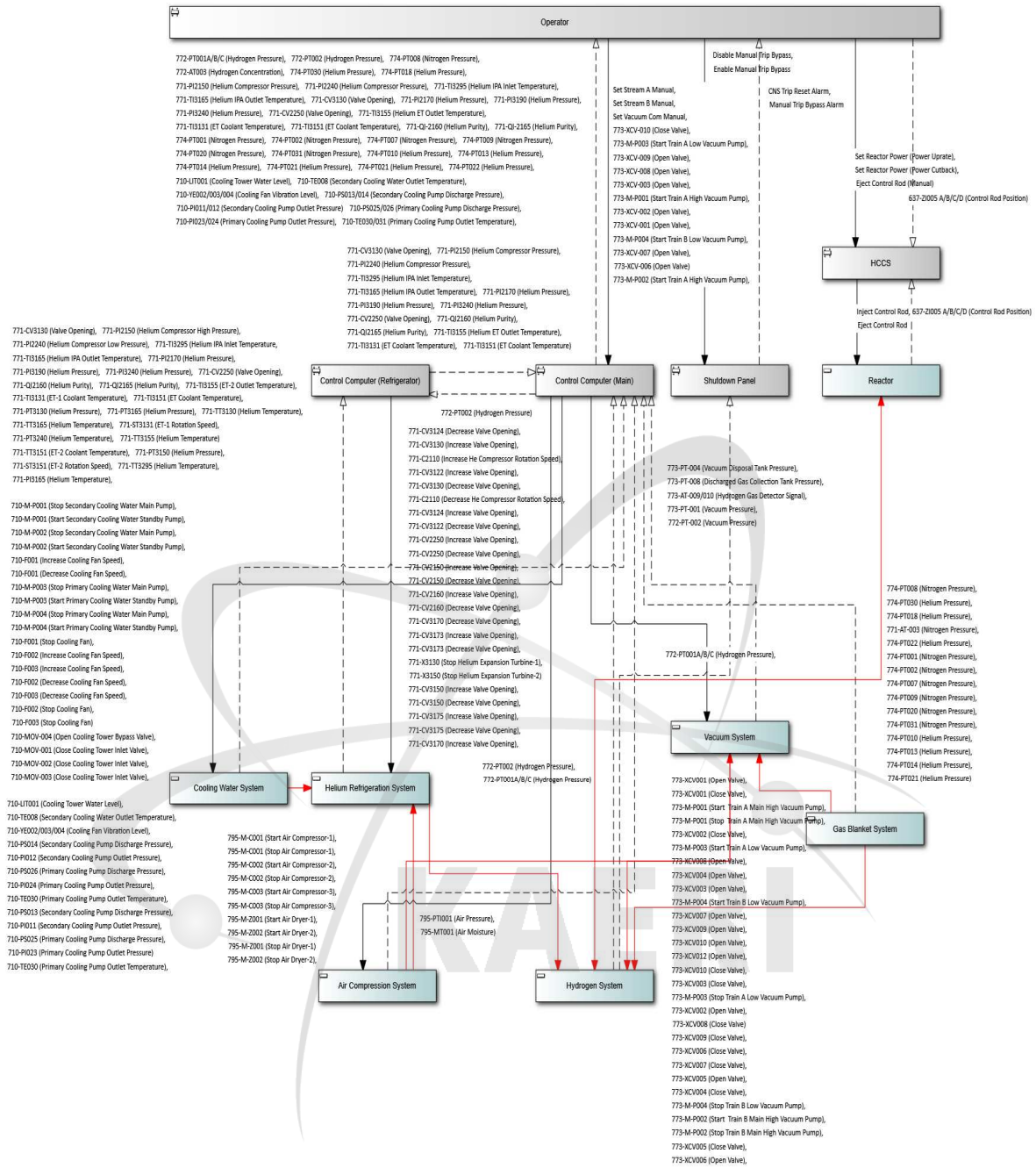


그림 25. 하나로 CNS계통 Control Structure

제5절 계통 UCA 도출 및 검토

1. 계통 UCA 도출

RRS에 의한 수소 고압력 및 저압력 트립 신호는 수소계통 내 수소 압력 계측값 (772-PT001A/B/C) 의해 자동으로 동작한다. 본 연구에서는 해당 수소 압력이 비정상적인 상황을 발생시킬 수 있는 각 계통의 UCA를 찾아내기 위해, Control Action이 위험을 유발할 수 있는 경우를 아래와 같은 6가지 UCA 카테고리를 정의/적용하여 분석하였다.

- Provided, but not needed and unsafe
 - Controller가 Control Action을 불필요한 상황에 제공하여 위험(Hazard) 발생 가능.
- Provided, but the intensity is incorrect (too much or too little)
 - Controller가 Control Action을 제공하였으나 과/부족의 세기로 제공하여 위험(Hazard) 발생 가능.
- Provided, but executed in incorrect order
 - Controller가 Control Action을 제공하였으나 잘못된 순서로 제공하여 위험(Hazard) 발생 가능.
- Provided, but the duration is too long or too short
 - Controller가 (지속적으로 요구되는) Control Action을 제공하였으나 너무 이른 시점에 제공을 종료하거나 너무 오랫동안 제공하여 위험(Hazard) 발생 가능.
- Provided, but the starting time is too soon or too late
 - Controller가 Control Action을 제공하였으나 너무 빨리 또는 너무 늦게 제공하여 위험(Hazard) 발생 가능.
- Not provided, when needed to maintain safety
 - Controller가 Control Action을 제공하지 않아서 위험(Hazard) 발생 가능.

본 연구에서 UCA의 Context는 CNS계통별 운전절차서를 기반으로 작성되었다. Context는 기본적으로 Hazard에서 식별된 물리적 속성과 이에서 유도된 상세 속성들이 사용되어 정의되므로 추후 각 운전절차 수행 중 계통의 물리적 상태를 열수력적 분석을 통해 분석하고 UCA를 작성할 경우 UCA의 객관적 커버리지를 평가할 수 있을 것으로 기대된다. 본 연구에서는 사례 분석으로서 CNS계통 중 수소계통, 진공계통, 원자로제어 계통의 수동(운전원) 및 자동 운전(제어컴퓨터)과 관련된 Control Action들에 대해 UCA들을 도출하였으며, 그 결과 표 16과 같이 51개의 Control Action 목록에 대해 총 127개의 UCA들이 도출되었다. 본 분석에서는 향후 분석을 위해 UCA가 사고/위험을 발생시키는 시나리오를 포함하도록 작성되었다.

표 16. CNS계통 UCA 분석 결과

Control Action	Source Target	UCA Categories					
		A	B	C	D	E	F
		Provided	Intensity is too much or too little	Executed in incorrect order	Duration is too long or too short	Starting time is too soon or too late	Not provided
773-XCV-008 (Open Valve)	Operator Control Computer (Main)						진공계통수동운전(OP-1035.2.2.)시, 운전원이OWS를통해XCV-008을열지않아배기수집탱크로배기되지않아IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-1)
773-XCV002 (Open Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-004)고압력시,고진공펌프전단밸브XCV-002가열려IPA내적절한진공상태가유지				진공계통정상운전(OP-1035.1.5.3), 진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-002가늦게열려진공배기탱크내가스가누	진공계통정상운전(OP-1035.1.5.3), 진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-002가열리지않아진공배기탱크내가스가

		되지않아, 수소계통 내수소압력이증가 하여, 수소고압력트 립신호발생가능. (UCA-2)				출되어IPA내적절 한진공상태가유지 되지않아, 수소계통 내수소압력이증가 하여, 수소고압력트 립신호발생가능. (UCA-3)	누출되어IPA내적 절한진공상태가유 지되지않아, 수소계 통내수소압력이증 가하여, 수소고압력 트립신호발생가능. (UCA-4)
Set Vacuum Com Manual	Operator Control Computer (Main)	진공계통수동운전(OP-1035.2.2.)시, 수동트레인A동작 경우, StreamB스위 치를Manual로설정 하여이후진공계통 수동운전이불가하 여IPA내적절한진 공상태가유지되지 않아, 수소계통내수 소압력이증가하여, 수소고압력트립신 호발생가능. (UCA-5)				진공계통수동운전(OP-1035.2.2.)시, 수동 트레인 B동작 경우, 초기조건(OP-103 4.0)을 확인하지 않고 진공계통 수동 운전을 수행하여 이후 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-6)	진공계통수동운전(OP-1035.2.2.)시, 수동트레인B동작 경우, StreamB스위 치를Manual로설정 하지않아이후진공 계통수동운전이불 가하여IPA내적절 한진공상태가유지 되지않아, 수소계통 내수소압력이증가 하여, 수소고압력트 립신호발생가능. (UCA-7)
Set Reactor Power (Power Cutback)	Operator HCCS		원자로 출력 감발(OP-01 5.2)시, 원자로			원자로 출력 감발(OP-01 5.2)시, 원자로	

			출력값을 너무 낮게 설정하여, 갑작스런 출력 감발에 CNS 수소 저압력에 의한 트립 또는 CNS 수소 압력이 5분이상 저압력으로 유지되어 원자로 수동 트립. (UCA-8)			도달출력값을 확인하지 않고 빨리 목표출력치를 설정하여, 갑작스런 출력 감발에 CNS 수소 압력이 5분이상 저압력으로 유지되어 원자로 수동 트립. (UCA-9)	
773-XCV-010 (Close Valve)	Operator Control Computer (Main)						진공계통수동운전(OP-1035.2.2.)시, 운전원이OWS를통해XCV-010를닫지않아야후IPA내 적절한진공상태가 유지되지않아,수소 계통내수소압력이 증가하여,수소고압 력트립신호발생가 능. (UCA-10)
773-XCV003 (Open Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-004)저압 력시,고진공펌프전				진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-004)고압 력시,고진공펌프전	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-004)고압 력시,고진공펌프전

		<p>단밸브XCV-003 이열려IPA내적절 한진공상태가유지 되지않아,수소계통 내수소압력이증가 하여,수소고압력트 립신호발생가능. (UCA-11)</p>				<p>단밸브XCV-003 이너무늦게열려진 공배기탱크내가스 가배출되지않아IP A내적절한진공상 태가유지되지않아, 수소계통내수소압 력이증가하여,수소 고압력트립신호발 생가능 (UCA-12).</p>	<p>단밸브XCV-003 이열리지않아진공 배기탱크내가스가 배출되지않아IPA 내적절한진공상태 가유지되지않아,수 소계통내수소압력 이증가하여,수소고 압력트립신호발생 가능. (UCA-13)</p>
Set Stream B Manual	Operator Control Computer (Main)	<p>진공계통수동운전(OP-1035.2.2.)시, 수동트레인A동작 경우,StreamB스위 치를Manual로설정 하여이후진공계통 수동운전이불가하 여IPA내적절한진 공상태가유지되지 않아,수소계통내수 소압력이증가하여, 수소고압력트립신 호발생가능. (UCA-14)</p>				<p>진공계통수동운전(OP-1035.2.2.)시, 수동 트레인 B동작 경우, 초기조건(OP-103 4.0)을 확인하지 않고 진공계통 수동 운전을 수행하여 이후 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능.</p>	<p>진공계통수동운전(OP-1035.2.2.)시, 수동트레인B동작 경우,StreamB스위 치를Manual로설정 하지않아이후진공 계통수동운전이불 가하여IPA내적절 한진공상태가유지 되지않아,수소계통 내수소압력이증가 하여,수소고압력트 립신호발생가능. (UCA-16)</p>

						(UCA-15)	
773-XCV010 (Close Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.3), 진공배기탱크압력(773-PT-004)고압력시, 고진공펌프전단밸브XCV-010이닫혀진공배기탱크내가스가배출되지못해IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여, 수소고압력트립신호발생가능. (UCA-17)				진공계통정상운전(OP-1035.1.5.3), 진공배기탱크압력(773-PT-004)저압력시, 고진공펌프전단밸브XCV-010이늦게닫혀진공배기탱크내가스가누출되어IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여, 수소고압력트립신호발생가능. (UCA-18)	진공계통정상운전(OP-1035.1.5.3), 진공배기탱크압력(773-PT-004)저압력시, 고진공펌프전단밸브XCV-010이닫히지않아진공배기탱크내가스가누출되어IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여, 수소고압력트립신호발생가능. (UCA-19)
773-M-P003 (Start Train A Low Vacuum Pump)	Operator Control Computer (Main)						진공계통수동운전(OP-1035.2.2.)시, 운전원이OWS를통해저진공펌프M-P003을기동하지않아IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여, 수소고압력트립신호발생가능. (UCA-20)

773-XCV003 (Close Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5),진공배기탱크압력(773-PT-004)고압력시,고진공펌프전단밸브XCV-003이단히배기수집탱크로배출되지않아IPA내 적절한진공상태가유지되지 않아,수소계통내수소압력이증가하여, 수소고압력 트립 신호발생 가능. (UCA-21)				진공계통정상운전(OP-1035.1.5.3),진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-003이늦게단히진공배기탱크내가스가배출되지않아IPA내 적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-22)	진공계통정상운전(OP-1035.1.5.3),진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-003이단히지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-23)
773-XCV009 (Open Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.3),진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-009이열려IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트					

		립신호발생가능. (UCA-24)					
773-XCV008 (Open Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.3), 진공배기탱크압력(773-PT-004)저 압력시,고진공펌프 전단밸브XCV-008이열려IPA내적절 한진공상태가유지 되지않아,수소계통 내수소압력이증가 하여,수소고압력트 립신호발생가능. (UCA-25)				진공계통정상운전(OP-1035.1.5.),진 공배기탱크압력(773-PT-004)고압 력시,고진공펌프전 단밸브XCV-008 가너무늦게열려배 기수집탱크로배출 되지않아IPA내적 절한진공상태가유 지되지않아,수소계 통내수소압력이증 가하여,수소고압력 트립신호발생가능. (UCA-26)	진공계통정상운전(OP-1035.1.5),진 공배기탱크압력(773-PT-004)고압 력시,고진공펌프전 단밸브XCV-008 가열리지않아배기 수집탱크로배출되 지않아IPA내적절 한진공상태가유지 되지않아,수소계통 내수소압력이증가 하여,수소고압력트 립신호발생가능. (UCA-27)
Set Reactor Power (Power Uprate)	Operator HCCS		원자로 출력 증강(OP-01 5.1)시, 원자로 출력값을 너무 높게 설정하여, 갑작스런 출력 증가에 CNS 수소 고압력에 의한 트립 또는 CNS 수소 압력이 5분이상			원자로 출력 증강(OP-01 5.1)시, 원자로 도달출력값을 확인하지 않고 빨리 목표출력치를 설정하여, 갑작스런 출력 증가에 CNS 수소 압력이 5분이상 고압력으로	

			고압력으로 유지되어 원자로 수동 트립. (UCA-28)			유지되어 원자로 수동 트립 (UCA-29)	
773-M-P001(Start Train A Main High Vacuum Pump)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5),773-PT-004저압력시,고진공펌프M-P001이기동되어펌프가파손되어이후IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-30)			진공계통정상운전(OP-1035.1.5),773-PT-004고압력시,고진공펌프M-P001이기동중일찍중단되어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-31)	진공계통정상운전(OP-1035.1.5),773-PT-004고압력시,고진공펌프M-P001이늦게작동하여IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-32)	진공계통정상운전(OP-1035.1.5),773-PT-004고압력시,고진공펌프M-P001이작동하지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-33)
773-M-P002(Start Train B Main High Vacuum Pump)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5),773-PT-005저압력시,고진공펌프M-P002이기동되어펌프가파손되어이후IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발			진공계통정상운전(OP-1035.1.5),773-PT-005고압력시,고진공펌프M-P002이기동중일찍중단되어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능.	진공계통정상운전(OP-1035.1.5),773-PT-005고압력시,고진공펌프M-P002이늦게작동하여IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능.	진공계통정상운전(OP-1035.1.5),773-PT-005고압력시,고진공펌프M-P002이작동하지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능.

		생가능. (UCA-34)			(UCA-35)	(UCA-36)	(UCA-37)
773-XCV007 (Close Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-005)고압력시,고진공펌프전단밸브XCV-007가단해배기수집탱크로배출되지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-38)				진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-005)저압력시,고진공펌프전단밸브XCV-007가너무늦게단해IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-39)	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-005)저압력시,고진공펌프전단밸브XCV-007가단하지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-40)
773-XCV010 (Open Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.3),진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-010이열려IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트				진공계통정상운전(OP-1035.1.5.),배기수집탱크압력(773-PT-008)고압력,XCV-010이너무늦게열려배기수집탱크내가스가배출되지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이	진공계통정상운전(OP-1035.1.5.),배기수집탱크압력(773-PT-008)고압력,XCV-010이열리지않아배기수집탱크내가스가배출되지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증

		립신호발생가능. (UCA-41)				증가하여,수소고압 력트립신호발생가 능. (UCA-42)	가하여,수소고압력 트립신호발생가능. (UCA-43)
773-XCV002 (Close Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.),진 공배기탱크압력(7 73-PT-004)저압 력시,고진공펌프전 단밸브XCV-002 가닫혀IPA내적절 한진공상태가유지 되지않아,수소계통 내수소압력이증가 하여,수소고압력트 립신호발생가능. (UCA-44)				진공계통정상운전(OP-1035.1.5.),진 공배기탱크압력(7 73-PT-004)고압 력시,고진공펌프전 단밸브XCV-002 가너무늦게닫혀IP A내적절한진공상 태가유지되지않아, 수소계통내수소압 력이증가하여,수소 고압력트립신호발 생가능 (UCA-45).	진공계통정상운전(OP-1035.1.5.),진 공배기탱크압력(7 73-PT-004)고압 력시,고진공펌프전 단밸브XCV-002 가닫히지않아IPA 내적절한진공상태 가유지되지않아,수 소계통내수소압력 이증가하여,수소고 압력트립신호발생 가능. (UCA-46)
Eject Control Rod (Manual)	Operator HCCS		원자로 출력 증강(OP-01 5.1)시, 운전원이 Control Rod를 많이 인출하여, 수소계통에 전달되는 열이 많아져, 수소계통내 수소압력이 증가하여, 수소	원자로 출력 증강(OP-01 5.1)시, 운전원이 제어봉#1~4중 잘못된 Control Rod를 선택하여 인출하여 이후 원자로 출력 이상으로 수소계통에 전달되는 열이		원자로 출력 증강(OP-01 5.1)시, 운전원이 Control Rod를 너무 빠르게 인출하여, 수소계통에 전달되는 열이 많아져 수소 고압력 발생 가능. (UCA-49)	

			고압력 트립 신호 발생 가능. (UCA-47)	많아져, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-48)			
773-XCV-003 (Open Valve)	Operator Control Computer (Main)						진공계통수동운전(OP-1035.2.2.)시, 운전원이OWS를통해XCV-003을열지않아진공배기탱크로배기되지않아, PA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여,수소고압력트립신호발생가능 (UCA-50).
Eject Control Rod	HCCS Reactor		원자로 출력 증강(OP-01 5.1)시, HCCS가 Control Rod를 많이 인출하여 , 수소계통에 전달되는 열이 많아져 수소			원자로 출력 증강(OP-01 5.1)시, HCCS가 Control Rod를 너무 빠르게 인출하여, 수소계통에 전달되는 열이	원자로 출력 증강(OP-01 5.1)시, HCCS가 Control Rod를 인출하지 않아, 수소계통에 전달되는 열이 적어져 수소

			고압력 발생 가능. (UCA-51).			많아져 수소 고압력 발생 가능. (UCA-52)	저압력 발생 가능. (UCA-53)
773-XCV012 (Open Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.3), 진공배기탱크압력(773-PT-004)저 압력시,고진공펌프 전단밸브XCV-01 2이열려IPA내적절 한진공상태가유지 되지않아,수소계통 내수소압력이증가 하여,수소고압력트 립신호발생가능. (UCA-54)				진공계통정상운전(OP-1035.1.5.),배 기수집탱크압력(7 73-PT-008)고압 력,수소검출신호(A T-009/010)발생 시,XCV-012이너 무늯게열려배기수 집탱크내가스가배 출되지않아IPA내 적절한진공상태가 유지되지않아,수소 계통내수소압력이 증가하여,수소고압 력트립신호발생가 능. (UCA-55)	진공계통정상운전(OP-1035.1.5.),배 기수집탱크압력(7 73-PT-008)고압 력,수소검출신호(A T-009/010)발생 시,XCV-012이열 리지않아배기수집 탱크내가스가배출 되지않아IPA내적 절한진공상태가유 지되지않아,수소계 통내수소압력이증 가하여,수소고압력 트립신호발생가능. (UCA-56)
Disable Manual Trip Bypass	Operator ShutdownPanel			원자로 목표출력 도달(OP-102 5.2.7)시, CNS Trip Reset 버튼을 누르지 않은채, Manual HANARO Trip Bypass 버튼을 먼저 눌러 CNS 고/저압력		원자로 목표출력 도달(OP-102 5.2.7)시, 운전변수들이 안정화 상태에 있음을 확인하지 않고, Trip bypass를 해제하여 CNS 고/저압력	

				트립 발생. (UCA-57)		트립 발생. (UCA-58)	
773-XCV-01 (Open Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.7),PT-001저압력시,밸브박스전단밸브(XCV-001)이열려IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-59)				진공계통정상운전(OP-1035.1.7.),PT-001고압력시,밸브박스전단밸브(XCV-001)이늦게열려IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-60)	진공계통정상운전(OP-1035.1.7.),PT-001고압력시,밸브박스전단밸브(XCV-001)이열리지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-61)
773-M-P004 (Start Train B Low Vacuum Pump)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5),진공배기탱크압력(773-PT-004)고압력시,저진공펌프M-P004가기동되어펌프가파손되어이후 IPA내 적절한진공상태가유지되지 않아,수소계통내수소압력이증가하여, 수소고압력 트립 신호			진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-005)고압력시,저진공펌프M-P004가기동중일찍중단되어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-63)	진공계통정상운전(OP-1035.1.5),진공배기탱크압력(773-PT-005)고압력시,저진공펌프M-P004가늦게기동하여IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-64)	진공계통정상운전(OP-1035.1.5),진공배기탱크압력(773-PT-005)고압력시,저진공펌프M-P004가기동하지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-65)

		발생 가능. (UCA-62)					
773-XCV008 (Close Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.3), 진공배기탱크압력(773-PT-004)고압력시,고진공펌프전단밸브XCV-008이단혀진공배기탱크내가스가배출되지못해IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-66)				진공계통정상운전(OP-1035.1.5.3), 진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-008이늦게단혀진공배기탱크내가스가누출되어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능.(UCA-67)	진공계통정상운전(OP-1035.1.5.3), 진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-008이단히지않아진공배기탱크내가스가누출되어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-68)
773-XCV006 (Close Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5),진공배기탱크압력(773-PT-005)고압력시,고진공펌프전단밸브XCV-006이단혀배기수집탱크로배출되지않아IPA내 적절한진공상태가유지되지 않아,				진공계통정상운전(OP-1035.1.5.3), 진공배기탱크압력(773-PT-005)저압력시,고진공펌프전단밸브XCV-006이늦게단혀진공배기탱크내가스가배출되지않아IPA내 적절한진공상태가유지되지않아,수소	진공계통정상운전(OP-1035.1.5.3), 진공배기탱크압력(773-PT-005)저압력시,고진공펌프전단밸브XCV-006이단히지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고

		수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-69)				계통내수소압력이 증가하여,수소고압 력트립신호발생가 능. (UCA-70)	압력트립신호발생 가능. (UCA-71)
773-XCV-006 (Open Valve)	Operator Control Computer (Main)						진공계통수동운전(OP-1035.2.2.)시, 운전원이OWS를통해XCV-006을열지않아배기수집탱크로배기되지않아IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여,수소고압력트립신호발생가능 (UCA-72).
773-XCV005 (Close Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-005)저압력시,고진공펌프전단밸브XCV-005가단히IPA내적절한진공상태가유지되지않아,수소계통				진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-005)고압력시,고진공펌프전단밸브XCV-005가너무늦게단히IPA내적절한진공상태가유지되지않아,	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-005)고압력시,고진공펌프전단밸브XCV-005가단히지않아IPA내적절한진공상태가유지되지않아,수

		내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-73)				수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-74)	소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-75)
773-XCV001 (Close Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.7.),PT-001고압력시,밸브박스전단밸브(XCV-001)이달히IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-76)				진공계통정상운전(OP-1035.1.7.),PT-001저압력시,밸브박스전단밸브(XCV-001)이늦게달히IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-77)	진공계통정상운전(OP-1035.1.7.),PT-001저압력시,밸브박스전단밸브(XCV-001)이달히지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-78)
773-XCV009 (Close Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.3),진공배기탱크압력(773-PT-004)고압력시,고진공펌프전단밸브XCV-009이달히진공배기탱크내가스가배출되지못해IPA내적절한진공상태가유지되지않아,수소계통				진공계통정상운전(OP-1035.1.5.3),진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-009이늦게달히진공배기탱크내가스가누출되어IPA내적절한진공상태가유지되지않아,수소계통	진공계통정상운전(OP-1035.1.5.3),진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-009이달히지않아진공배기탱크내가스가누출되어IPA내적절한진공상태가유지되지않아,수소계

		내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-79)				내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-80)	통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-81)
773-XCV004 (Open Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-004가열려IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-82)				진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-004)고압력시,고진공펌프전단밸브XCV-004가너무늦게열려배기수집탱크로배출되지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-83)	진공계통정상운전(OP-1035.1.5),진공배기탱크압력(773-PT-004)고압력시,고진공펌프전단밸브XCV-004가열리지않아배기수집탱크로배출되지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-84)
773-M-P002 (Start Train A High Vacuum Pump)	Operator Control Computer (Main)						진공계통수동운전(OP-1035.2.2.)시,운전원이OWS를통해고진공펌프M-P002를기동하지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,

							수소고압력트립신호발생가능. (UCA-85)
Inject Control Rod	HCCS Reactor		원자로 출력 감발(OP-01 5.2)시, HCCS가 Control Rod를 많이 삽입하여, 수소계통에 전달되는 열이 적어져 수소 저압력 발생 가능. (UCA-86)			원자로 출력 감발(OP-01 5.2)시, HCCS가 Control Rod를 너무 빠르게 삽입하여, 수소계통에 전달되는 열이 적어져 수소 저압력 발생 가능. (UCA-87)	원자로 출력 감발(OP-01 5.2)시, HCCS가 Control Rod를 삽입하지 않아, 수소계통에 전달되는 열이 많아져 수소 고압력 발생 가능. (UCA-88)
773-M-P004 (Stop Train B Low Vacuum Pump)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-004)고압력시,저진공펌프M-P004가멈추어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-89)				진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-005)저압력시,저진공펌프M-P004가일찍멈추어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-90)	진공계통정상운전(OP-1035.1.5.),773-PT-005저압력시,저진공펌프M-P004이정지하지않아펌프가파손되어이후IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-91)
773-M-P002	Control	진공계통정상운전(진공계통정상운전(진공계통정상운전(

(Stop Train B Main High Vacuum Pump)	Computer (Main) VacuumSystem	OP-1035.1.5.),773-PT-004고압력시,고진공펌프M-P001이기동되지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-92)				OP-1035.1.5.),773-PT-005저압력시,고진공펌프M-P002이일찍정지되어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-93)	OP-1035.1.5.),773-PT-005저압력시,고진공펌프M-P002이정지하지않아펌프가파손되어이후IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-94)
773-XCV006 (Open Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-005)저압력시,고진공펌프전단밸브XCV-006이열려IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-95)				진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-005)고압력시,고진공펌프전단밸브XCV-006이너무늦게열려진공배기탱크내가스가배출되지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능 (UCA-96).	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-005)고압력시,고진공펌프전단밸브XCV-006이열리지않아진공배기탱크내가스가배출되지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능 (UCA-97)

773-M-P001 (Start Train A High Vacuum Pump)	Operator Control Computer (Main)						진공계통수동운전(OP-1035.2.2.)시, 운전원이OWS를통해고진공펌프M-P001을기동하지않아IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여, 수소고압력트립신호발생가능. (UCA-98)
773-XCV-002 (Open Valve)	Operator Control Computer (Main)						진공계통수동운전(OP-1035.2.2.)시, 운전원이OWS를통해XCV-002을열지않아진공배기탱크로배기되지않아IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여, 수소고압력트립신호발생가능. (UCA-99)
773-XCV004 (Close Valve)	Control Computer (Main)	진공계통정상운전(OP-1035.1.5.), 진공배기탱크압력(7				진공계통정상운전(OP-1035.1.5.), 진공배기탱크압력(7	진공계통정상운전(OP-1035.1.5.), 진공배기탱크압력(7

	VacuumSystem	73-PT-004)고압 력시,고진공펌프전 단밸브XCV-004 가닫혀배기수집탱 크로배출되지않아 IPA내적절한진공상 태가유지되지않아, 수소계통내수소압 력이증가하여,수소 고압력트립신호발 생가능. (UCA-100)				73-PT-004)저압 력시,고진공펌프전 단밸브XCV-004 가너무늦게닫혀IP A내적절한진공상 태가유지되지않아, 수소계통내수소압 력이증가하여,수소 고압력트립신호발 생가능. (UCA-101)	73-PT-004)저압 력시,고진공펌프전 단밸브XCV-004 가닫히지않아IPA 내적절한진공상태 가유지되지않아,수 소계통내수소압력 이증가하여,수소고 압력트립신호발생 가능. (UCA-102)
Set Stream A Manual	Operator Control Computer (Main)	진공계통수동운전(OP-1035.2.2)시, 수동 트레인 B동작 경우, Stream A 스위치를 Manual로 설정하여 이후 진공계통 수동 운전이 불가하여 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소				진공계통수동운전(OP-1035.2.2)시, 수동 트레인 A동작 경우, 초기조건(OP-103 4.0)을 확인하지 않고 진공계통 수동 운전을 수행하여 이후 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호	진공계통수동운전(OP-1035.2.2)시, 수동 트레인 A동작 경우, Stream A 스위치를 Manual로 설정하지 않아 이후 진공계통 수동 운전이 불가하여 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소

		고압력 트립 신호 발생 가능. (UCA-103)				발생 가능. (UCA-104)	고압력 트립 신호 발생 가능. (UCA-105)
773-XCV-007 (Open Valve)	Operator Control Computer (Main)						진공계통수동운전(OP-1035.2.2.)시, 운전원이OWS를통해XCV-007을열지않아배기수집탱크로배기되지않아IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-106)
773-M-P003 (Start Train A Low Vacuum Pump)	Control Computer (Main) VacuumSystem						진공계통수동운전(OP-1035.2.2.)시, 운전원이OWS를통해저진공펌프M-P003을기동하지않아IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여, 수소고압력트립신호발생가능. (UCA-107)

773-XCV-009 (Open Valve)	Operator Control Computer (Main)					진공계통수동운전(OP-1035.2.2.)시, 운전원이OWS를통해XCV-009를열지않아배기수집탱크로배출되지않아IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여, 수소고압력트립신호발생가능. (UCA-108)
773-XCV007 (Open Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.), 진공배기탱크압력(773-PT-005)저압력시, 고진공펌프전단밸브XCV-007가열려IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여, 수소고압력트립신호발생가능. (UCA-109)			진공계통정상운전(OP-1035.1.5.), 진공배기탱크압력(773-PT-005)고압력시, 고진공펌프전단밸브XCV-007가너무늦게열려배기수집탱크로배출되지않아IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여, 수소고압력트립신호발생가능. (UCA-110)	진공계통정상운전(OP-1035.1.5.), 진공배기탱크압력(773-PT-005)고압력시, 고진공펌프전단밸브XCV-007가열리지않아배기수집탱크로배출되지않아IPA내적절한진공상태가유지되지않아, 수소계통내수소압력이증가하여, 수소고압력트립신호발생가능. (UCA-111)

Enable Manual Trip Bypass	Operator ShutdownPanel						원자로 출력 감발전(OP-01 5.2.1.1), Manual HANARO Trip Bypass 버튼을 누르지 않고 원자로 출력 감발중 CNS 고/저압력 트립 발생. (UCA-112)
773-XCV005 (Open Valve)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-004)고압력시,고진공펌프전단밸브XCV-005가열려IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-113)				진공계통정상운전(OP-1035.1.5.3),진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-005이늦게열려진공배기탱크내가스가누출되어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-114)	진공계통정상운전(OP-1035.1.5.3),진공배기탱크압력(773-PT-004)저압력시,고진공펌프전단밸브XCV-005이열리지않아진공배기탱크내가스가누출되어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-115)

773-XCV-001 (Open Valve)	Operator Control Computer (Main)				진공계통정상운전(OP-103 5.1.7.),PT-001고압력시,밸브박스전단밸브(XCV-001)이늦게열려IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-116)	진공계통정상운전(OP-103 5.1.7.),PT-001고압력시,밸브박스전단밸브(XCV-001)이열리지않아HPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-117)
773-M-P004 (Start Train B Low Vacuum Pump)	Operator Control Computer (Main)	진공계통정상운전(OP-1035.1.5),진공배기탱크압력(773-PT-004)고압력시,저진공펌프M-P004가기동되어펌프가파손되어이후 IPA내 적절한진공상태가유지되지 않아,수소계통내수소압력이증가하여, 수소고압력 트립 신호발생 가능. (UCA-118)		진공계통정상운전(OP-1035.1.5),진공배기탱크압력(773-PT-005)고압력시,저진공펌프M-P004가기동중일찍중단되어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-119)	진공계통정상운전(OP-1035.1.5),진공배기탱크압력(773-PT-005)고압력시,저진공펌프M-P004가늦게기동하여IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-120)	진공계통정상운전(OP-1035.1.5),진공배기탱크압력(773-PT-005)고압력시,저진공펌프M-P004가기동하지않아HPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-121)

773-M-P003 (Stop Train A Low Vacuum Pump)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-004)고압력시,저진공펌프M-P003가멈추어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-122)				진공계통정상운전(OP-1035.1.5.),진공배기탱크압력(773-PT-004)저압력시,저진공펌프M-P003가일찍멈추어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-123)	진공계통정상운전(OP-1035.1.5.),773-PT-004저압력시,저진공펌프M-P003이정지하지않아펌프가파손되어이후IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-124)
773-M-P001(Stop Train A Main High Vacuum Pump)	Control Computer (Main) VacuumSystem	진공계통정상운전(OP-1035.1.5.),773-PT-004고압력시,고진공펌프M-P001이기동되지않아IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-125)				진공계통정상운전(OP-1035.1.5.),773-PT-004저압력시,고진공펌프M-P001이일찍정지되어IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-126)	진공계통정상운전(OP-1035.1.5.),773-PT-004저압력시,고진공펌프M-P001이정지하지않아펌프가파손되어이후IPA내적절한진공상태가유지되지않아,수소계통내수소압력이증가하여,수소고압력트립신호발생가능. (UCA-127)

2. 전문가 자문을 통한 UCA 중요도 분석

본 분석에서 도출된 UCA들의 타당성을 확인하고자, 각 UCA들의 발생가능성에 대해 다음과 같은 평가지표를 설정하였다.

○ 평가지표

- O: 발생가능성에 대한 추가 검토 필요함.
- X: 발생가능성 없거나 대응조치 존재함.

현재 하나로 연구용원자로에 종사하고 있는 전문가에게 CNS 수소계통, 진공계통, 원자로제어계통에 관하여 도출된 35개의 UCA들에 대하여 위의 평가지표에 따른 평가를 요청하였으며, 2020년 5월 12일에 자문결과를 수집하였다. 표 17과 18은 수집된 평가결과들 중 추가 검토가 필요한 UCA 및 해당 UCA에 대한 대응조치가 수립된 항목들을 보여준다. 표에서 O으로 파악된 UCA들은 제어컴퓨터에 의해서 진공계통 관련 특정 밸브가 열리지 않는 경우(2건)로 평가되었다. 또한 평가지표 상 X로 파악된 UCA들 중 대응조치가 이미 수립된 항목들은 1) 운전원이 원자로 목표출력 도달 후 트립 우회 수행에 실패한 경우(버튼 조작번호 부착 등 방지대책 수립), 2) 운전원이 출력 증강/감발 시 CNS 수소계통의 수소압력 불안정(절차화되어 있어 인적오류 발생 희박), 3) 제어컴퓨터에 의한 진공계통 관련 펌프류가 작동에 이상이 발생한 경우(자동기동오류 시, 운전원 수동 조작으로 백업 가능)로 파악되었다.

이러한 결과는 하나로 운전경험이 풍부한 전문가 의견에 따라 도출되었으나, 본 분석을 통해 얻어진 UCA와 관련되어 있음을 강조할 필요가 있다. 따라서 STPA 방법을 적용하여 얻어진 UCA는 하나로 불시정지 방지를 위한 효과적 방안 도출의 기초자료로 될 것으로 기대된다. 또한 기존 분석 계통(수소계통, 진공계통, 원자로제어계통) 이외 헬륨냉동계통, 냉각수계통 등 수소계통의 수소압력 안정에 필요한 계통들에 대한 추가분석을 수행할 시 보다 포괄적인 불시정지 시나리오 및 방지대책을 수립할 수 있을 것으로 판단된다.

표 17. 전문가 검토 결과 평가지표 O로 평가된 UCA 목록

하나로 CNS계통 STPA 모델 분석 결과					평가 지표	전문가 메모
관련 계통	Controller	Controlled Process	Control Action	UCA		
진공계통	Control Computer (Main)	Vacuum System	773-XCV-001 (Open Valve)	진공 계통 정상운전(OP-103 5.1.7), PT-001 고압력 시, 밸브박스 전단 밸브(XCV-001)이 늦게 열려 IPA내 적절한 진공상태가 유지되지 않아, 수소계통 내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-60)	O	계측기나 밸브가 단일구성이므 로 문제가 발생될 가능성이 있으 며 운전경험 바탕으로 해당점수 를 설정함.
				진공 계통 정상운전(OP-103 5.1.7), PT-001 고압력 시, 밸브박스 전단 밸브(XCV-001)이 열리지 않아 IPA내 적절한 진공상태가 유지되지 않아, 수소계통 내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-61)	O	계측기나 밸브가 단일구성이므 로 문제가 발생될 가능성이 있으 며 운전경험 바탕으로 해당점수 를 설정함.

KAERI

표 18. 전문가 검토 결과 평가지표 X로 평가된 UCA 목록

하나로 CNS계통 STPA 모델 분석 결과					평가 지표	전문가 메모
관련 계통	Controller	Controlled Process	Control Action	UCA		
운전원/ 수소계통	Operator	Shutdown Panel	Enable Manual Trip Bypass	원자로 출력 감발 전(OP-01 5.2.1.1), Manual HANARO Trip Bypass 버튼을 누르지 않고 원자로 출력 감발중 CNS 고/저압력 트립 발생. (UCA-112)	X	절차화가 되어 있으므로 가능성 희박
운전원/원자로제어계통	Operator	HCCS	Set Reactor Power (Power Cutback)	원자로 출력 감발(OP-01 5.2)시, 원자로 출력값을 너무 낮게 설정하여, 갑작스런 출력 감발에 CNS 수소 압력이 5분 이상 고압력으로 유지되어 원자로 수동 트립. (UCA-8)	X	재발방지 대책으로 절차서 개정 및 운전원 교육을 완료.
				원자로 출력 감발(OP-01 5.2)시, 원자로 도달출력값을 확인하지 않고 빨리 목표 출력치를 설정하여, 갑작스런 출력 감발에 CNS 수소 압력이 5분 이상 고압력으로 유지되어 원자로 수동 트립. (UCA-9)	X	

진공계통	Control Computer (Main)	Vacuum System	773-M-P004 (Start Train B Low Vacuum Pump)	진공 계통 정상운전(OP-103 5.1.5), 진공배기탱크 압력(773-PT-004) 고압력 시, 저진공펌프 M-P004가 기동되어 펌프가 파손되어 이후 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-118)	X	운전중 원인모를 저진공 펌프의 고 장 가능성은 있지만 고장이 발생하 면 예비펌프가 자동으로 기동됨. 로직에의한 자동기동오류시 운전 원이 수동으로 조작하여 기동할수 있음.
				진공 계통 정상운전(OP-103 5.1.5), 진공배기탱크 압력(773-PT-005) 고압력 시, 저진공펌프 M-P004가 기동 중 일찍 중단되어 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-119)	X	
				진공 계통 정상운전(OP-103 5.1.5), 진공배기탱크 압력(773-PT-005) 고압력 시, 저진공펌프 M-P004가 늦게 기동하여 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-120)	X	
				진공 계통 정상운전(OP-103 5.1.5), 진공배기탱크 압력(773-PT-005) 고압력 시, 저진공펌프 M-P004가 기동하지 않아 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-121)	X	

운전원/ 진공계통	Operator	Control Computer (Main)	773-XCV-008 (Open Valve)	진공 계통 수동 운전(OP-103 5.2.2) 시, 운전원이 OWS를 통해 XCV-008을 열지 않아 배기수집탱크로 배기되지 않아 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-1)	X	이 밸브는 하나로와 연계운전시 수 동운전을 하지 않고 자동동작되므 로 오동작 가능성이 낮음.
운전원/ 진공계통	Operator	Control Computer (Main)	Set Vacuum Com Manual	진공 계통 수동 운전(OP-103 5.2.2) 시, 수동 트레인 동작 경우, 초기조건(OP-103 4.0)을 확인하지 않고 진공계통 수동 운전을 수행하여 이후 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능 (UCA-6)	X	CNS 전계통은 하나로 기동전 운전을 시작하여 수소압력이 안정화된 상태에서 하나로와 연계운전을 시작하고, 항상 자동운전 상태를 유지하므로, 운전 중 수동조작에 따른 인적오류가 발생할 수 없음.
				진공 계통 수동 운전(OP-103 5.2.2) 시, 수동 트레인 동작 경우, Vacuum Com 스위치를 Manual로 설정하지 않아 이후 진공계통 수동 운전이 불가하여 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-7)	X	
운전원/ 진공계통	Operator	Control Computer (Main)	773-XCV-010 (Close Valve)	진공 계통 수동 운전(OP-103 5.2.2) 시, 운전원이 OWS를 통해 XCV-010를 닫지 않아 이후 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-10)	X	이 밸브는 하나로와 연계운전시 수동운전을 하지 않고 자동동작되므로 오동작 가능성이 낮음.

운전원/ 진공계통	Operator	Control Computer (Main)	Set Stream B Manual	진공 계통 수동 운전(OP-103 5.2.2) 시, 수동 트레인 A동작 경우, Stream B 스위치를 Manual로 설정하여 이후 진공계통 수동 운전이 불가하여 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-14)	X	하나로 연계운전시 수동운전을 하지 않음. 진공상태가 불량하여도 조치시간이 비교적 여유가 있음. 이 밸브는 하나로와 연계운전시 수동운전을 하지 않고 자동동작되므로 오동작 가능성이 낮음.
				진공 계통 수동 운전(OP-103 5.2.2) 시, 수동 트레인 B동작 경우, 초기조건(OP-103 4.0)을 확인하지 않고 진공계통 수동 운전을 수행하여 이후 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-15)	X	
				진공 계통 수동 운전(OP-103 5.2.2) 시, 수동 트레인 B동작 경우, Stream B 스위치를 Manual로 설정하지 않아 이후 진공계통 수동 운전이 불가하여 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-16)	X	

운전원/ 진공계통	Operator	Control Computer (Main)	773-M-P003 (Start Train A Low Vacuum Pump)	진공 계통 수동 운전(OP-103 5.2.2) 시, 운전원이 OWS를 통해 저진공펌프 M-P003을 기동하지 않아 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능 (UCA-107)	X	고진공펌프 후단 MT001, 002의 알람경보 발생으로 운전원 인식이 가능하며, 진공계통은 자동 동작되기 때문에 수동운전을 하나로 연계운전 시 하지 않음.
운전원/원자로제 어계통	Operator	HCCS	Set Reactor Power (Power Uprate)	원자로 출력 증강(OP-01 5.1)시, 원자로 출력값을 너무 높게 설정하여, 갑작스런 출력 증가에 CNS 수소 고압력에 의한 트립 또는 CNS 수소 압력이 5분이상 고압력으로 유지되어 원자로 수동 트립. (UCA-28)	X	CNS 헬륨냉동계통의 운전변수(자동밸브의 Parameter)는 30MW에 설정되어 있어 하나로 출력 증,감 시 수소압력은 안정화를 벗어나는 경우가 종종 있음. 수소압력에 의한 하나로 정지 신호를 by-pass하고 하나로 출력을 조절함.
				원자로 출력 증강(OP-01 5.1)시, 원자로 도달출력값을 확인하지 않고 빨리 목표출력치를 설정하여, 갑작스런 출력 증가에 CNS 수소 압력이 5분이상 고압력으로 유지되어 원자로 수동 트립 (UCA-29)	X	

운전원/원자로 제어계통	Operator	HCCS	Eject Control Rod (Manual)	원자로 출력 증강(OP-01 5.1)시, 운전원이 Control Rod를 많이 인출하여, 수소계통에 전달되는 열이 많아져, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-47)	X	CNS 헬륨냉동계통의 운전변수(자동밸브의 Parameter)는 30MW에 설정되어 있어 하나로 출력 증,감 시 수소압력은 안정화를 벗어나는 경우가 종종 있음. 수소압력에 의한 하나로 정지 신호를 by-pass하고 하나로 출력을 조절함.
				원자로 출력 증강(OP-01 5.1)시, 운전원이 제어봉#1~4중 잘못된 Control Rod를 선택하여 인출하여 이후 원자로 출력 이상으로 수소계통에 전달되는 열이 많아져, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-48)	X	CNS 헬륨냉동계통의 운전변수(자동밸브의 Parameter)는 30MW에 설정되어 있어 하나로 출력 증,감 시 수소압력은 안정화를 벗어나는 경우가 종종 있음. 수소압력에 의한 하나로 정지 신호를 by-pass하고 하나로 출력을 조절함.
				원자로 출력 증강(OP-01 5.1)시, 운전원이 Control Rod를 너무 빠르게 인출하여, 수소계통에 전달되는 열이 많아져 수소 고압력 발생 가능. (UCA-49)	X	

운전원/ 진공계통	Operator	Control Computer (Main)	773-XCV-003 (Open Valve)	진공 계통 수동 운전(OP-103 5.2.2) 시, 운전원이 OWS를 통해 XCV-003을 열지 않아 진공배기탱크로 배기되지 않아 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-50)	X	이 밸브는 하나로와 연계운전시 수동운전을 하지 않고 자동동작되므로 오동작 가능성이 낮음.
운전원/ 수소계통	Operator	Shutdown Panel	Disable Manual Trip Bypass	원자로 목표출력 도달(OP-102 5.2.7)시, CNS Trip Reset 버튼을 누르지 않은 채, Manual HANARO Trip Bypass 버튼을 먼저 눌러 CNS 고/저압력 트립 발생. (UCA-57)	X	재발방지 대책으로 Shutdown Panel 안내문구 설치 및 운전원 교육을 완료.
				원자로 목표출력 도달(OP-102 5.2.7)시, 운전변수들이 안정화 상태에 있음을 확인하지 않고, Trip bypass를 해제하여 CNS 고/저압력 트립 발생 (UCA-58)	X	운전변수의 불안정화는 결국 수소압력의 불안정상태이므로 운전원은 운전기록지에 수소압력을 작성하게 되어 있음. 수소압력이 안정화범위 이내에서 버튼을 해제하는건 불가능함.
운전원/ 진공계통	Operator	Control Computer (Main)	773-XCV-006 (Open Valve)	진공 계통 수동 운전(OP-103 5.2.2) 시, 운전원이 OWS를 통해 XCV-006을 열지 않아 배기수집탱크로 배기되지 않아 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-72)	X	이 밸브는 하나로와 연계운전시 수동운전을 하지 않고 자동동작되므로 오동작 가능성이 낮음.

운전원/ 진공계통	Operator	Control Computer (Main)	773-M-P002 (Start Train A High Vacuum Pump)	진공 계통 수동 운전(OP-103 5.2.2) 시, 운전원이 OWS를 통해 고진공펌프 M-P002를 기동하지 않아 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-85)	X	이 밸브는 하나로와 연계운전시 수동운전을 하지 않고 자동동작되므로 오동작 가능성이 낮음.
운전원/ 진공계통	Operator	Control Computer (Main)	773-M-P001 (Start Train A High Vacuum Pump)	진공 계통 수동 운전(OP-103 5.2.2) 시, 운전원이 OWS를 통해 고진공펌프 M-P001을 기동하지 않아 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-98)	X	이 밸브는 하나로와 연계운전시 수동운전을 하지 않고 자동동작되므로 오동작 가능성이 낮음.
운전원/ 진공계통	Operator	Control Computer (Main)	773-XCV-002 (Open Valve)	진공 계통 수동 운전(OP-103 5.2.2) 시, 운전원이 OWS를 통해 XCV-002을 열지 않아 진공배기탱크로 배기되지 않아 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-99)	X	이 밸브는 하나로와 연계운전시 수동운전을 하지 않고 자동동작되므로 오동작 가능성이 낮음.

운전원/ 진공계통	Operator	Control Computer (Main)	Set Stream A Manual	진공 계통 수동 운전(OP-103 5.2.2) 시, 수동 트레인 B동작 경우, Stream A 스위치를 Manual로 설정하여 이후 진공계통 수동 운전이 불가하여 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-103)	X	이 밸브는 하나로와 연계운전시 수동운전을 하지 않고 자동동작되므로 오동작 가능성이 낮음.
				진공 계통 수동 운전(OP-103 5.2.2) 시, 수동 트레인 A동작 경우, 초기조건(OP-103 4.0)을 확인하지 않고 진공계통 수동 운전을 수행하여 이후 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-104)	X	
				진공 계통 수동 운전(OP-103 5.2.2) 시, 수동 트레인 A동작 경우, Stream A 스위치를 Manual로 설정하지 않아 이후 진공계통 수동 운전이 불가하여 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-105)	X	

운전원/ 진공계통	Operator	Control Computer (Main)	773-XCV-007 (Open Valve)	진공 계통 수동 운전(OP-103 5.2.2) 시, 운전원이 OWS를 통해 XCV-007을 열지 않아 배기수집탱크로 배기되지 않아 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-106)	X	이 밸브는 하나로와 연계운전시 수동운전을 하지 않고 자동동작되므로 오동작 가능성이 낮음.
운전원/ 진공계통	Operator	Control Computer (Main)	773-XCV-009 (Open Valve)	진공 계통 수동 운전(OP-103 5.2.2) 시, 운전원이 OWS를 통해 XCV-009를 열지 않아 배기수집탱크로 배출되지 않아 IPA내 적절한 진공상태가 유지되지 않아, 수소계통내 수소압력이 증가하여, 수소 고압력 트립 신호 발생 가능. (UCA-108)	X	이 밸브는 하나로와 연계운전시 수동운전을 하지 않고 자동동작되므로 오동작 가능성이 낮음.



제4장

하나로 운영 프로세스 평가

제1절 하나로 정지이력과의 비교분석

제2절 CNS계통 FMEA결과와의 비교분석

KAERI



제4장 하나로 운영 프로세스 평가

제1절 하나로 정지이력 비교분석

본 연구에서는 도출된 UCA의 타당성을 추가적으로 확인하고자 CNS계통이 설치된 2009년 이후 CNS계통 관련 원자로 정지 이력과 본 STPA분석의 결과인 UCA와의 비교 분석하였다. STPA는 동적 제어 또는 신호전달의 관점에서 시스템의 리스크를 분석한다. 반면 단순 기기 고장으로 인해 발생한 불시정지는 별도의 신호전달 체계로 표현되지 않는다. 본 비교분석에서는 이와 같은 성격의 단순 기기 고장 및 운전원의 합리적 판단에 의한 수동정지로 인한 정지이력을 제외한 원자로 자동 정지 건수는 총 6건이며 아래와 같다.

- ① 2009년 11월 27일, 압축공기계통 정지 - CNS 수소 고압력 트립 발생
- ② 2010년 1월 17일, 냉각탑 수조 수위스위치 오동작 - CNS 수소 고압력 트립 발생
- ③ 2010년 4월 18일, 헬륨냉동계통 압력전송기 PT-2240 신호선 접촉 불량 - CNS 수소 고압력 트립 발생
- ④ 2012년 2월 29일, CNS 우회 스위치 운전원 오조작 - 원자로 제어계통에 의한 원자로 트립 발생.
- ⑤ 2013년 1월 2일, 헬륨냉동박스 냉각수 유량스위치 FS3731 오작동 - CNS 수소 고압력에 의한 원자로 정지 발생.
- ⑥ 2018년 12월 10일, 헬륨냉동계통 터빈우회밸브 고장 - CNS 수소 압력 불안정으로 CNS 및 원자로 수동정지.

본 비교분석에서는 CNS 수소계통, 진공계통, 원자로제어계통, 압축공기계통과 관련된 불시정지 사례들이 최종적으로 비교분석 되었으며, 표 19는 그 결과를 보여준다. 표를 통해 볼 때 한 건의 UCA(표 17 UCA-57)가 기존에 발생된 정지이력과 상응하는 것을 확인할 수 있다. 만약 해당 UCA가 관련 불시정지 발생 이전에 도출되었다면, 불필요한 원자로 정지를 예방하는 데 활용 될 수도 있었을 것이다.

표 19. 하나로 CNS계통 STPA모델 결과와 정지이력의 비교분석

하나로 CNS계통 STPA 모델 분석 결과						관련 정지이력	
관련 계통	Controller	Controlled Process	관련 계통	Control Action	UCA	일자	정지원인
운전원	Operator	Shutdown Panel	운전원	Disable Manual Trip Bypass	원자로 목표출력 도달(OP-102 5.2.7) 시, CNS Trip Reset 버튼을 누르지 않은 채, Manual HANARO Trip Bypass 버튼을 먼저 눌러 CNS 고/저압력 트립 발생. [H-5]	2012년 02월 29일	원자로출력 30MW에서 CNS 정지판넬에서 'CNS TRIP RESET' 해제 없이, 바로 'MANUAL HANARO TRIP BYPASS' 버튼 조작 → RRS에 의한 원자로정지 발생

KAERI

제2절 CNS계통 FMEA결과와의 연계

STPA는 거대한 규모와 높은 복잡성을 가지는 시스템 구성요소간의 상호작용, 조직이나 사람 등 인적요소간의 상호작용, 그리고 인적요소-시스템간의 상호작용에서 발생하는 제어신호를 모델에 포함한다. 그리고 그 제어신호의 이상특성을 정의하고 해당 이상신호가 전체 시스템에 전파되는 과정을 체계적으로 분석한다.

반면 FMEA는 시스템의 주요 구성 기기들의 고장모드를 분석하고 해당 고장으로 인한 계통상의 영향을 식별하는 체계적인 분석 방법이다. 본 분석에서는 UCA 도출까지를 분석범위로 설정하였는데, 더 나아가 STPA방법론 하에서 안전한 시스템의 구축과 보완사항 도출을 위해 각 UCA 발생의 원인(Causal Factor Analysis)을 파악할 필요가 있다. 이 과정에서 FMEA의 특정 고장모드의 영향이 특정 이상신호 발생으로 이어지는 경우, FMEA의 결과가 STPA방법론과 연계되어 시스템의 기계적 구성요소간의 이상신호 발생원인 파악에 활용될 수 있다.

CNS 진공계통에 대해 수행된 FMEA의 예시는 표 20과 같다[38]. 이와 같은 FMEA 결과는 중요 UCA로 평가된 항목들의 발생원인 파악에 활용되어 특정 원인으로부터 원자로 불시정지가 최종적으로 발생하게 되는 loss scenario들을 도출할 수 있으며, 이를 방지할 수 있는 체계적인 대책 수립의 기초자료로 활용될 수 있을 것이다.



KAERI

표 20. CNS 진공계통 FMEA분석 결과 예제

계통명	기기명	기능	정상상태	고장모드	고장영향 (계통별)	고장 감지방법	고장 시 보상수단	고장 영향	정지 변수
진공계통	Valve Box 밸브 AOV (HAN-CNS-773-XCV 001)	<ul style="list-style-type: none"> - IPA내 진공도를 유지하기 위한 격리 AOV - AOV를 제어하는 SOV-001A는 Hydrogen Box 외부에 위치 - PT-001과 연동되어, 밸브 개방/닫힘을 반복하면서 IPA내 진공도 유지, 경험상 개방된 상태 유지가 현저히 많음 	Operation	Fail Closed	<ul style="list-style-type: none"> - 고장시 FC (Fail Closed) type임, 따라서 loss of air 및 loss of electricity시에도 닫힘 유지, 그러므로 IPA 진공도는 변동 없음. 	기기 주변 계측기	없음	없음	-
	저진공펌프 (HAN-CNS-773-M-P 003/P004)	<ul style="list-style-type: none"> -저진공펌프 운전은 CNS 운전 중 가압되는 Vacuum Disposal Tank의 진공도를 높이기 위함 -이는 Vacuum Disposal Tank의 진공도를 높임으로서, 고진공 펌프 운전을 원활하게 하기 위함 	Standby	Fail to Function	<ul style="list-style-type: none"> - 저진공펌프 M-P3/P004의 공통원인고장으로 인해 CNS 운전에 미치는 영향 없음 	기기 주변 계측기	없음	없음	-

제5장

결론





제5장 결론

본 분석에서는 최근 10년간 불시정지 횟수가 많았던 하나로 연구용원자로 CNS 계통 운영 프로세스를 STAMP/STPA체계에 따라 모델링하고, 이를 토대로 원자로 불시정지를 유발할 수 있는 UCA를 도출하였다. STAMP/STPA기법은 계통의 안전에 직접적으로 영향을 미치는 기기의 고장뿐 아니라, 정상적 기기 혹은 관련 계통간의 상호작용 및 인적 오류, 환경과 같은 시스템 외적인 요인까지 통합적으로 고려한 위험 요소를 분석할 수 있는 체계를 제공해준다.

본 분석에서의 STPA분석절차는 1) 계통 친숙화, 2) 계통 운전 관련 자료 분석, 3) 계통 STPA 모델(CS) 개발, 4) 계통 UCA 도출 및 검토의 단계로 수행되었다. 개발된 STPA모델에서 주체(Controller)-객체(Controlled process)간의 제어(Control action)는 운전절차서에 명시되어있는 계통 구성 기기들(밸브, 펌프)의 운전 원리를 바탕으로 작성되었다. 작성된 각 제어(Control action)리스트를 바탕으로 6가지 UCA 카테고리에 대해 RRS로 인한 CNS 수소 계통 수소 고/저압력 불시정지가 발생할 수 있는 UCA들을 도출하였다.

도출된 UCA의 타당성을 평가하기 위해 각 UCA들에 대해 하나로 운전원 및 전문가 자문을 통해 평가지표에 따른 검토를 하였으며 도출된 UCA를 기존의 정지이력을 비교분석하였다. 그 결과, 실제 발생했던 불시정지와 유사 것으로 확인되었고, 하나로 운전 전문가 검토결과 발생 가능성은 작지만 2건의 UCA에 대한 추가 검토가 필요한 것으로 확인되었다. 따라서 본 분석을 통해 도출된 UCA는 실제 경험하지는 않았으나 하나로 불시정지를 일으킬 수 있는 개연성이 있다는 측면에서, 추후 체계적으로 관리되어야 할 대상이라고 판단된다.

STPA기반의 리스크 분석절차 및 결과물은 FMEA와 상호보완적으로 연계될 수 있다. STPA는 기계적 요소와 더불어 인적오류에 이르는 제어신호의 이상특성을 다양하게 정의하고 그 이상신호가 전체시스템에 전파되는 과정을 체계적으로 분석하게 된다. 이후 보다 안전한 시스템의 구축을 위해 이상신호 발생의 원인을 파악할 필요가 있는데, 기계적 요소의 이상신호 발생 원인 파악에 FMEA 분석 과정 및 결과가 활용될 수 있다. 또한, 기존의 Control Structure에 추가적인 요소들(현장운전원, 운전원간 지시체계 등)을 모델링 할 시, 더 구체적이고 포괄적인 운영 프로세스 분석이 가능할 것으로 기대된다.



제6장

참고문헌






제6장 참고문헌

- [1] 강인혁 외, 하나로 불시 정지 및 비정상 현상에 대한 원인 분석 및 조치, KAERI/TR-4223/2010, 한국원자력연구원, 2010.
- [2] 이윤환 외, 하나로 연구용원자로 Level 1 PSA 초기사건 분석, KAERI/TR-7661/2019, 한국원자력연구원, 2019.
- [3] N. G. Leveson, J. P. Thomas, STPA Handbook, MIT, 2018.
- [4] EPRI, HAZCADs: Hazards and Consequences Analysis for Digital Systems, 3002012755, EPRI, 2018.
- [5] J. P. Thomas, F. L. de Lemos, N. G. Leveson, Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants, NRC-HQ-11-6-04-0060, MIT, 2012.
- [6] SAE International, Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, ARP 4761, SAE International, 1996.
- [7] ISO, Road vehicles - Functional Safety, ISO 26262, ISO, 2018.
- [8] Heimdahl et al., Software Assurance Approaches, Considerations, and Limitations, DOT/FAA/TC-15-57, U.S. DoT, 2016.
- [9] Becker et al., Functional Safety Assessment of Generic Conventional, Hydraulic Braking System with Antilock Brakes, Traction Control, and Electronic Stability Control, DOT-HS-812-574, U.S. NHTSA, 2018.
- [10] Okada et al., STPA Trial Case for Automated Driving System Life Cycles, STAMP Workshop 2019, Mar. 25-27, 2019.
- [11] Masci et al., Extending STPA to Improve the Analysis of User Interface Software in Medical Devices, STAMP Workshop 2018, Mar. 26-29, 2018.
- [12] Song Y., Applying System-Theoretic Accident Model and Processes (STAMP) to Hazard Analysis, Master Thesis, McMaster University, 2012.
- [13] 유준범 외, 정형기법 기반 안전등급 소프트웨어 평가방법 개발, KAERI/CM-2015/2014, 건국대학교, 2014.
- [14] 정환성 외, 하나로 냉중성자원 시설 계통의 기본 설계 요건, KAERI/TR-2993/2005, 한국원자력연구원, 2005.
- [15] Hyundai Engineering Co., LTD, P&I Diagram Hydrogen System, HAN-CNS-772-MC-H001 Rev. 5, 한국원자력연구원, 2012.
- [16] 우상익 외, 하나로 냉중성자원 진공계통의 상세설계, KAERI/TR-3389/2007, 한국원자력연구원, 2007.
- [17] Hyundai Engineering Co., LTD, P&I Diagram Vacuum System, HAN-CNS-773-MC-H001 Rev. 6, 한국원자력연구원, 2006.
- [18] 최정운 외, 하나로 냉중성자원 헬륨냉동계통 설치 및 시운전, KAERI/TR-3935/2009, 한국원자력연구원, 2009.
- [19] Linde Kryotechnik AG, PID Refrigerator, HAN-CNS-771-200.008.019 Rev. 7, 한국원자력연구원, 2015.

- [20] 최정운 외, 하나로 냉중성자원 수소계통 및 가스블랭킷계통의 상세설계, KAERI/TR-3410/2007, 한국원자력연구원, 2007.
- [21] Hyundai Engineering Co., LTD, P&I Diagram Gas Blanketing System (Nitrogen), HAN-CNS-774-MC-H001 Rev. 9, 한국원자력연구원, 2013.
- [22] Hyundai Engineering Co., LTD, P&I Diagram Gas Blanketing System (Helium), HAN-CNS-774-MC-H002 Rev. 9, 한국원자력연구원, 2013.
- [23] 김봉수 외, 하나로 냉중성자원 냉각수계통의 상세설계, KAERI/TR-3393/2007, 한국원자력연구원, 2007.
- [24] Hyundai Engineering Co., LTD, P&I Diagram Cooling Water System, HAN-CNS-710-MC-H001 Rev. 6, 한국원자력연구원, 2008.
- [25] Hyundai Engineering Co., LTD, P&I Diagram Cooling Water System, HAN-CNS-710-MC-H003 Rev. 7, 한국원자력연구원, 2009.
- [26] Hyundai Engineering Co., LTD, P&I Diagram Cooling Water System, HAN-CNS-710-MC-H002 Rev. 8, 한국원자력연구원, 2009.
- [27] 한국원자력연구원, P&I Diagram Compressed Air Supply System, HAN-CNS-710-MC-H001 Rev. 3, 한국원자력연구원, 2013.
- [28] 이지복 외, 하나로 안전성 분석 보고서, KAERI/TR-710/1996, 한국원자력연구원, 1996.
- [29] 우종섭 외, 하나로 기술 행정 절차서, 절차서 작성, 개정 및 관리, HANTAP-05-OD-ROP-TA-08, 한국원자력연구원, 2008.
- [30] 인원호 외, 원자로 기동 및 정지, HANTAP-05-OD-ROP-OP-01 Rev. 16, 한국원자력연구원, 2019.
- [31] 황정식 외, CNS 기동 및 정지 운전, HANTAP-05-OD-ROP-OP-101 Rev. 4, 한국원자력연구원, 2019.
- [32] 황정식 외, CNS 수소계통, HANTAP-05-OD-ROP-OP-102 Rev. 3, 한국원자력연구원, 2019.
- [33] 김민수 외, CNS 진공계통, HANTAP-05-OD-ROP-OP-103 Rev. 1, 한국원자력연구원, 2013.
- [34] 황정식 외, CNS 가스블랭킷계통, HANTAP-05-OD-ROP-OP-104 Rev. 1, 한국원자력연구원, 2013.
- [35] 황정식 외, CNS 냉각수계통, HANTAP-05-OD-ROP-OP-105 Rev. 1, 한국원자력연구원, 2013.
- [36] 김민수 외, CNS 헬륨냉동계통, HANTAP-05-OD-ROP-OP-106 Rev. 3, 한국원자력연구원, 2013.
- [37] 김민수 외, CNS 공기압축기, HANTAP-05-OD-ROP-OP-112 Rev. 1, 한국원자력연구원, 2013.
- [38] 이윤환 외, 냉중성자원 시설계통 대상 고장모드영향분석(FMEA) 및 정지이력 분석, KAERI/TR-8079/2020, 한국원자력연구원, 2020.



부 록

[부록 1] RMStudio 프로그램 소개 및 사용법



KAERI



부 록



[부록 1] RMStudio 프로그램 소개 및 사용법

RMStudio는 검증된 리스크 관리 프로세스 및 정책의 구현을 위해 개발된 동적 리스크 관리 소프트웨어로 Microsoft Solution Framework의 절차에 따라 개발되었으며, ISO 9001:2015 및 ISO/IEC 27001:2013에 따라 British Standards Institution에서 인증되었다. RMStudio는 사용자에게 STPA를 적절하게 수행하는데 필요한 다음과 같은 기능들을 제공한다.

- 계층적 제어 구조(Hierarchical Control Structure), Loss-Hazard 관계 및 Loss Scenario 모델링의 설계에 사용되는 다이어그램 작성
- STPA 도구의 자동화, 특히 Control Structure를 사용한 Unsafe Control Action 및 Loss Scenario 분석
- HCS, UCA, Loss Scenario 등 각 단계별 분석의 완전성을 자동으로 측정하며 분석 프로세스의 진행상황 및 일관성 확인
- STPA 도구의 자동화, 특히 Control Structure를 사용한 Unsafe Control Action 및 Loss Scenario 분석
- 모델 및 도표를 포함한 보고서의 자동적 생성(전체 또는 구간별)

RMStudio를 활용하여 STPA분석을 수행하는 과정은 다음과 같다.

1. STPA 프로젝트 실행

1. RM Studio Navigation 트리에서 STPA를 열어 오른쪽 작업 공간에서 STPA 프로젝트 탭을 실행한다.
2.  버튼을 클릭하여 새로운 STPA 프로젝트를 생성한다.
3. 프로젝트의 이름을 정한다.
4. 적절한 Business Entity를 설정하고  버튼을 클릭하여 데이터베이스에 프로젝트를 저장한다.

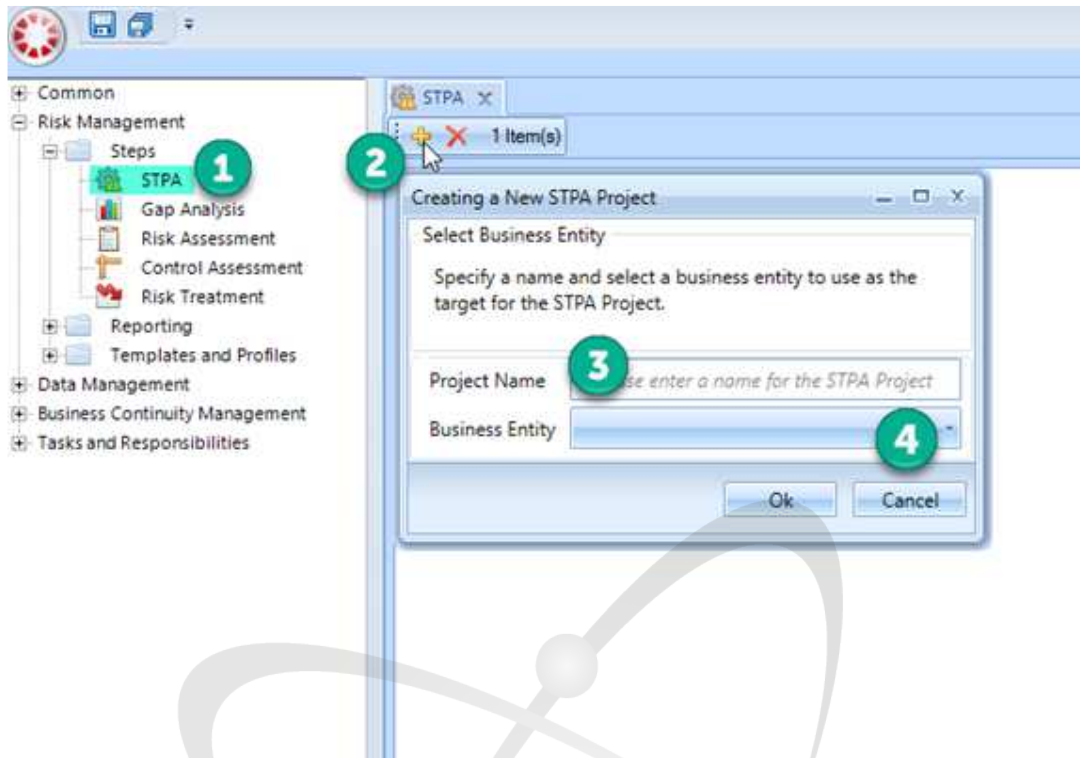


그림 부록 1-1. RMStudio STPA 프로젝트 생성

위의 과정 후에 새 STPA 프로젝트가 파일로 생성됨. 생성한 각 STPA 프로젝트는 위에서 아래로, 가장 오래된 것으로부터 가장 최신으로 정렬된 파일 목록에 나타난다. 사용자 선호도에 따라 파일을 재배열할 수 있으며 파일을 선택하면 파일 주위에 노란색 테두리 및 체크 표시가 나타나며 Open 버튼을 클릭하여 선택한 STPA 프로젝트에서 작업을 시작할 수 있다.

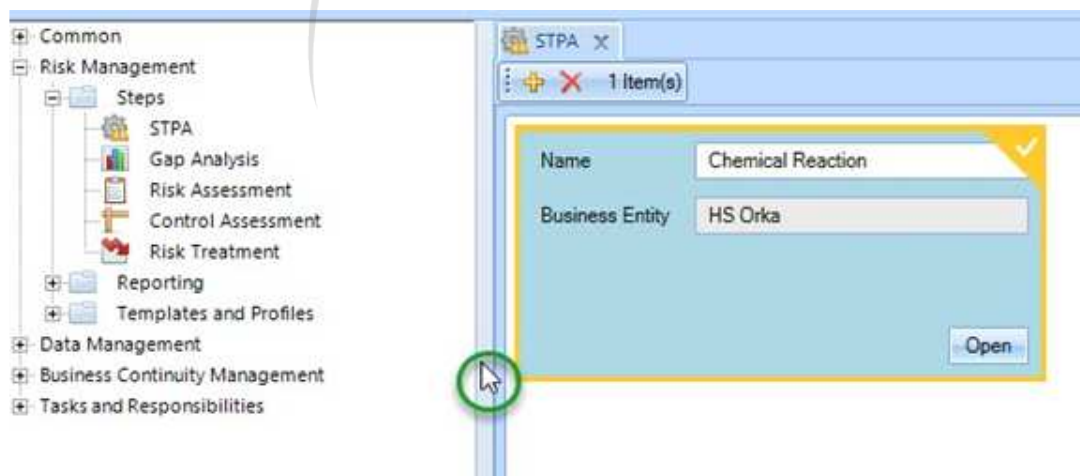


그림 부록 1-2. RMStudio STPA 프로젝트 실행

위의 과정 후에 새 STPA 프로젝트가 타일로 생성됨. 생성한 각 STPA 프로젝트는 위에서 아래로, 가장 오래된 것으로부터 가장 최신으로 정렬된 타일 목록에 나타난다. 사용자 선호도에 따라 타일을 재배열할 수 있으며 타일을 선택하면 타일 주위에 노란색 테두리 및 체크 표시가 나타나며 Open 버튼을 클릭하여 선택한 STPA 프로젝트에서 작업을 시작할 수 있다. 프로젝트의 이름은 트리의 맨 위에 있으며 모델 및 분석의 이름은 프로젝트와 동일하다. 트리에서 모델을 두 번 클릭하면 다음이 표시되는 새 컨텍스트 탭이 열린다.

- 모델 이름 편집
- 프로젝트의 시스템 목표 입력
- 모형에 대한 설명

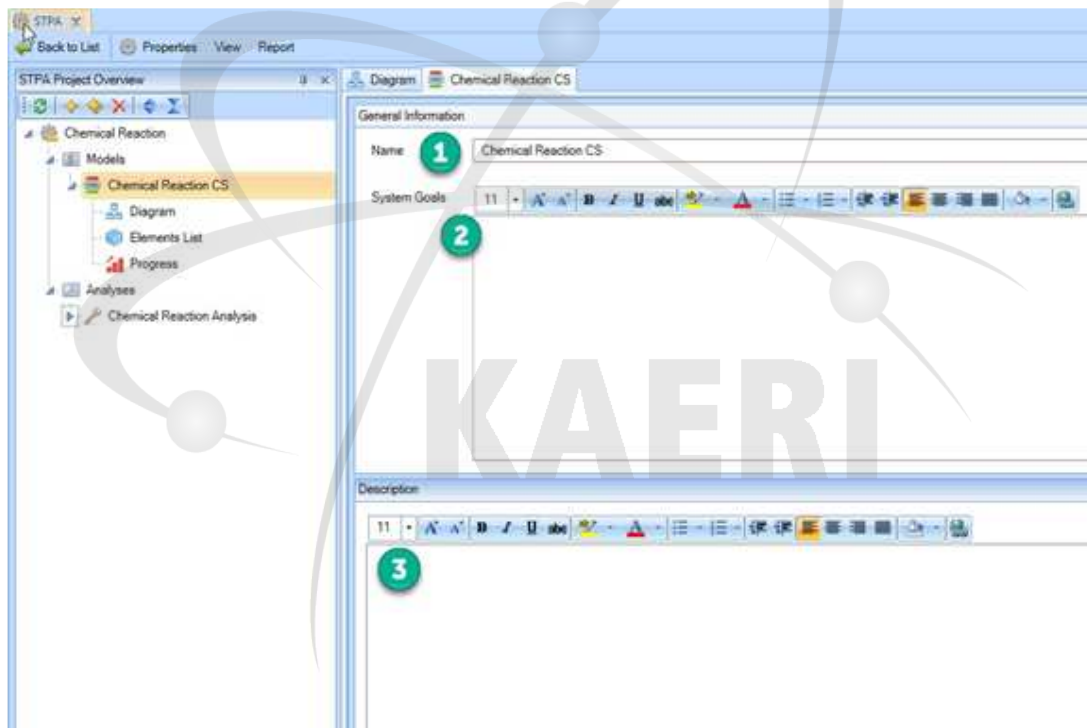


그림 부록 1-3. RMStudio STPA 프로젝트 이름 및 설명 설정

2. Control Structure 모델 생성

CS 모델은 STPA Project Overview의 'Models' 노드에 표시된다. Control Structure 모델은 하나 또는 여러 개의 Control Structure 다이어그램의 컨테이너 역할을 한다. 새 STPA 프로젝트를 만든 후, Control Structure 모델은 프로젝트와 동일한 이름으로 자동으로 생성된다. 다음으로, 도표를 만들고 원하는 이름을 지정해야 할 수 있다. Control Structure 모델은 STPA Project Overview의 'Models' 노드에 표시된다. Control Structure 모델은 하나 또는 여러 개의 Control Structure 다이어그램의 컨테이너 역할을 한다. 새 STPA 프로젝트를 만든 후, Control Structure 모델은 프로젝트와 동일한 이름으로 자동으로 생성된다. 다음으로, 도표를 만들고 원하는 이름을 지정해야 할 수 있다.

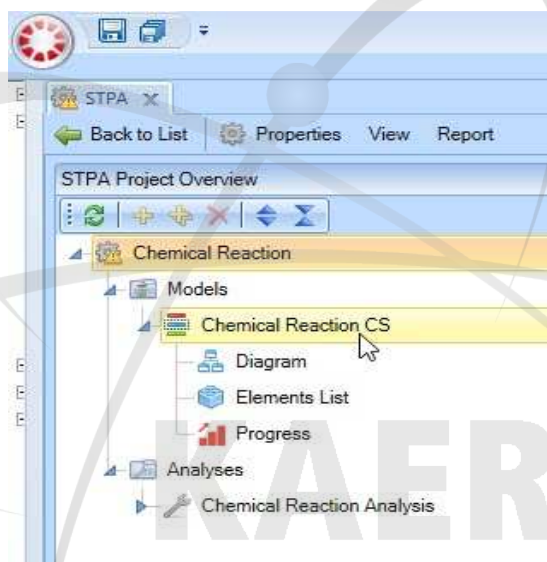


그림 부록 1-4. RMStudio Models 탭

CS 다이어그램은 제어기, 제어 프로세스, 제어 조치 및 피드백을 시각화한다. 다이어그램에 새 요소를 추가하거나 다이어그램에 이미 존재하는 요소를 수정할 수 있다. Control Structure 다이어그램은 Control Structure 모델에 상주하며, STPA 모듈은 하나의 Control Structure 모델에 대해 다중 다이어그램을 지원한다. 다이어그램에 생성된 주석 요소를 제외한 모든 요소는 각 Control Structure 모델의 일부로 저장된다. Control Structure 다이어그램 작성 방법은 다음과 같다.

1. 새 Control Structure 다이어그램을 생성할 Control Structure 모델을 STPA 프로젝트 개요 패널에서 선택한다.
2. 새 Control Structure 다이어그램을 생성한 후, 모델을 마우스 오른쪽 단추로 클릭하

- 여 New Diagram 버튼을 클릭하여 새 다이어그램을 만들 수 있다.
3. 모델 아래에서 새 다이어그램을 두 번 클릭하여 새로운 캔버스를 열 수 있다.
 4. 캔버스에 있는 모델 요소와 모델 커넥터를 선택하여 제어 구조를 생성한다.
 5. 모델을 생성한 후 진행률을 저장하여 이름이 탭과 트리에 저장한다.

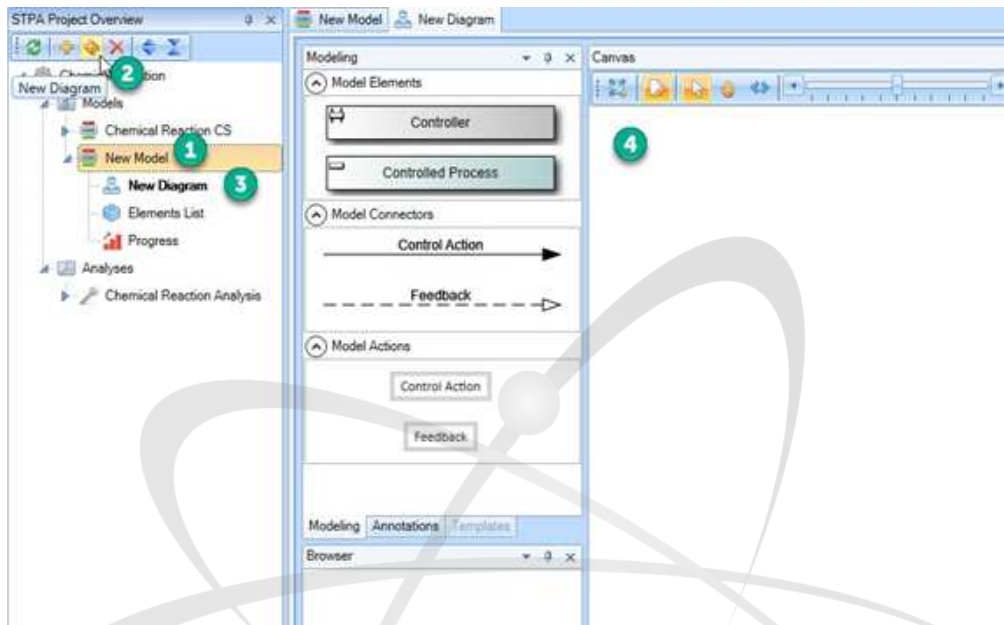


그림 부록 1-5. RMStudio Control Structure 모델링

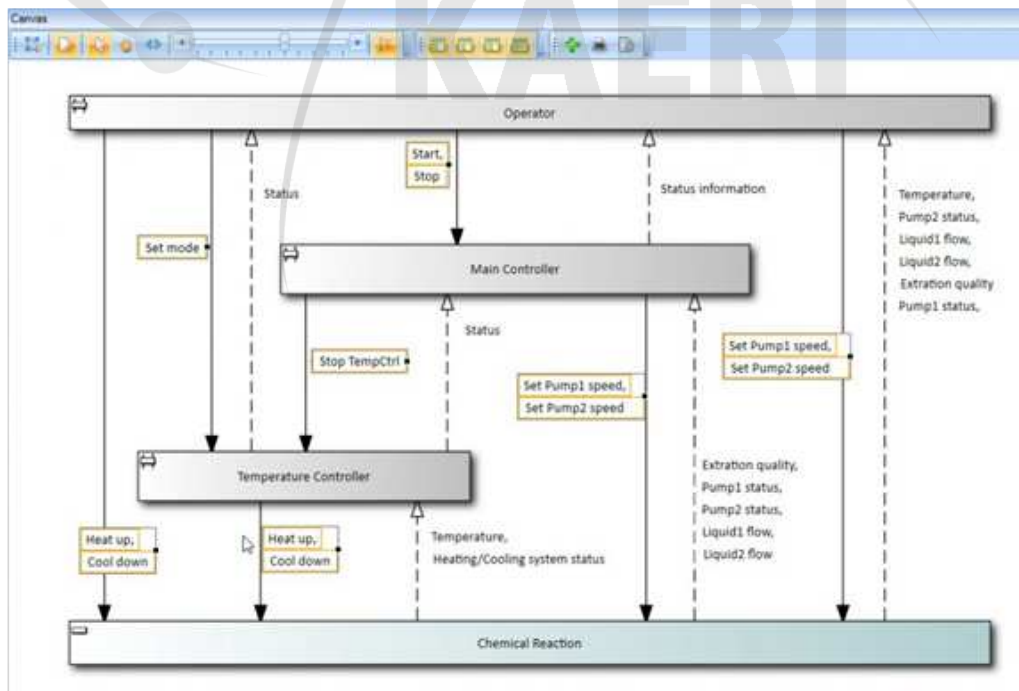


그림 부록 1-6. RMStudio Control Structure 개발 예시

3. STPA 분석 수행

Analysis 섹션은 STPA에 필요한 여러 가지 다른 유형의 분석을 위한 것이다. STPA 프로젝트 개요 트리는 모델 후 분석을 제공한다. 프로젝트가 STPA 모듈에서 생성되면 분석에 대해 동일한 이름이 자동으로 생성된다. 분석의 목적을 정의하는 것은 종종 STPA 방법의 첫 번째 단계지만, 손실과 위험이 브레인스토밍 단계에 있는 동안 분석가가 제어 구조 모형을 시작할 수 있다.

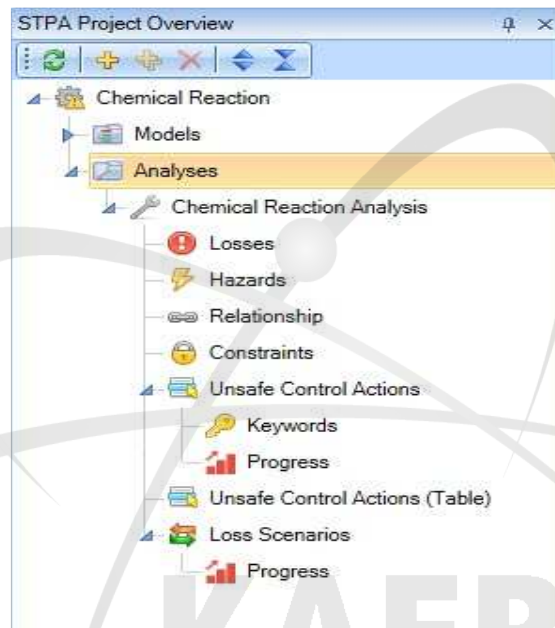


그림 부록 1-7. RMStudio Analysis 탭

분석 단계에서는 다음과 같은 질문이 다루어진다.


- 어떤 종류의 손실을 예방하는 것을 목표로 할 것인가
- STPA는 인명 손실을 방지하는 것과 같은 전통적인 안전 목표에만 적용될 것인가
- 보안, 프라이버시, 성능 및 기타 시스템 속성에 더 광범위하게 적용될 것인가
- 분석해야 할 시스템은 무엇이며 시스템 경계는 무엇인가

분석의 목적 정의에는 다음이 포함된다.

1. Loss 식별
2. Hazard 식별
3. UCA카테고리 정의

4. UCA 식별

(1) Loss 식별

1. STPA 프로젝트 트리에서 Loss(손실)를 두 번 클릭한다.
2.  버튼을 클릭하여 새 Loss를 만든다.
3. 생성된 Loss의 이름을 입력한다.
4. 새 Loss에 대한 고유 ID를 입력한다. (예: L1, L-2).
5. 다른 Loss와 구별하기 위해 Loss에 대한 설명을 입력한다.
6. Hazard를 생성한 후 분석가는 Loss와 Hazard를 연결할 수 있다.
7. 해당 열에서는 식별된 손실에 관련된 위험의 총 개수가 표시된다.

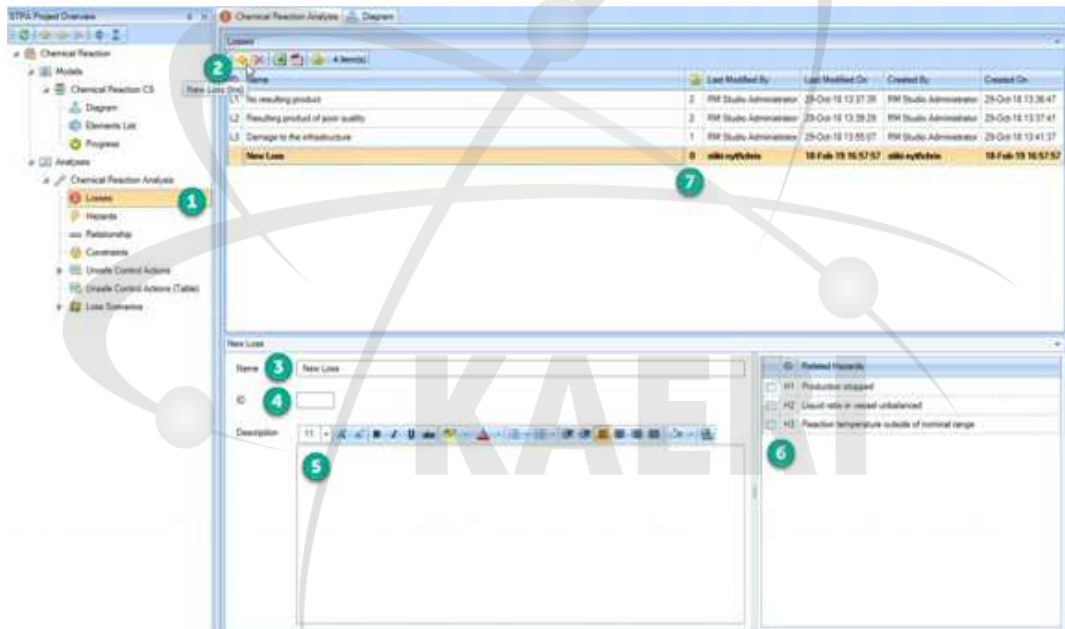


그림 부록 1-8. RMStudio Loss 설정

(2) Hazard 식별

시스템 수준 Hazard는 RM Studio STPA 모듈에서 정의될 수 있다. Hazard 노드 또는 STPA 프로젝트 개요의 Relationship 노드 아래에 이러한 노드를 생성할 수 있다. 생성된 Hazard는 Loss와 연관될 수 있다. 또한 시스템 수준 Hazard는 하위 Hazard에 의해 조정될 수 있으므로 Hazard는 다른 Hazard이나 Loss에 연결될 수 있다. Hazard 정의 방법은 다음과 같다.

1. STPA 프로젝트 트리에서 Hazard 노드를 두 번 클릭한다.
2. 새로운 Hazard를 만들려면 도구 모음에서 새 항목 추가 아이콘 아이콘을 클릭한다.
3. 이름 텍스트 상자를 클릭하여 Hazard의 이름을 변경한다.
4. Hazard의 ID(예: H1, H-2 등)를 정의한다.
5. Hazard를 명확히 하기 위해 설명과 기타 정보를 추가한다.

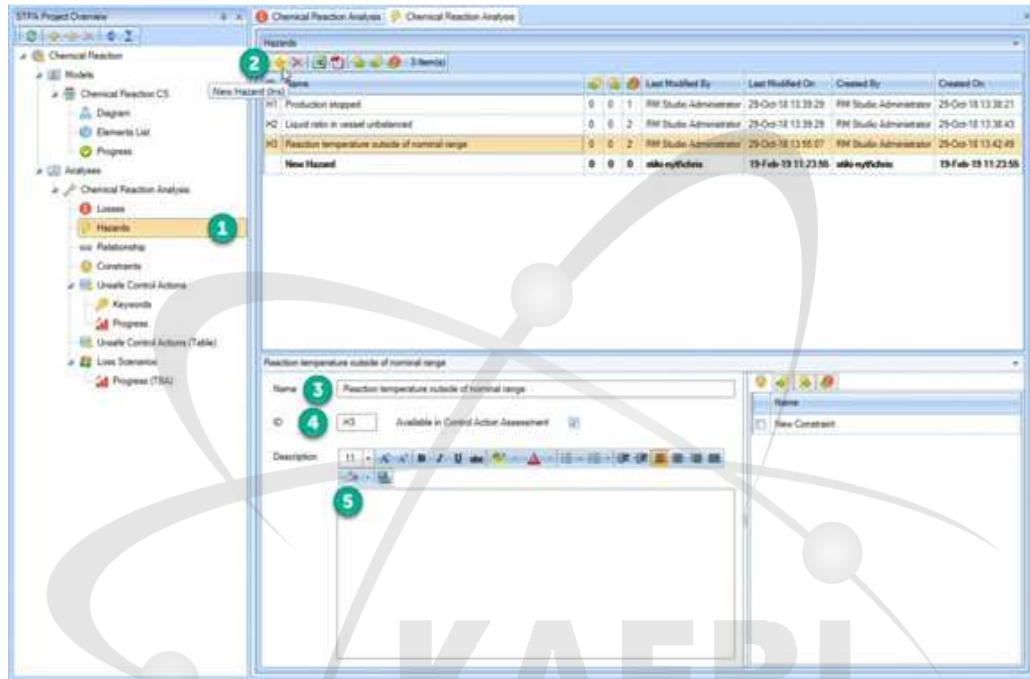


그림 부록 1-9. RMStudio Hazard 설정

(3) Loss-Hazard 관계 설정

1. STPA 프로젝트 트리에서 Relationship 노드를 두 번 클릭한다.
2. Relationship 캔버스용 도구 상자에서 Hazard와 Loss를 추가적으로 정의할 수 있다.
3. Relationship 캔버스용 도구 상자에서 Link 화살표로 Loss-Hazard과 Hazard-Hazard 관계를 정의할 수 있다.

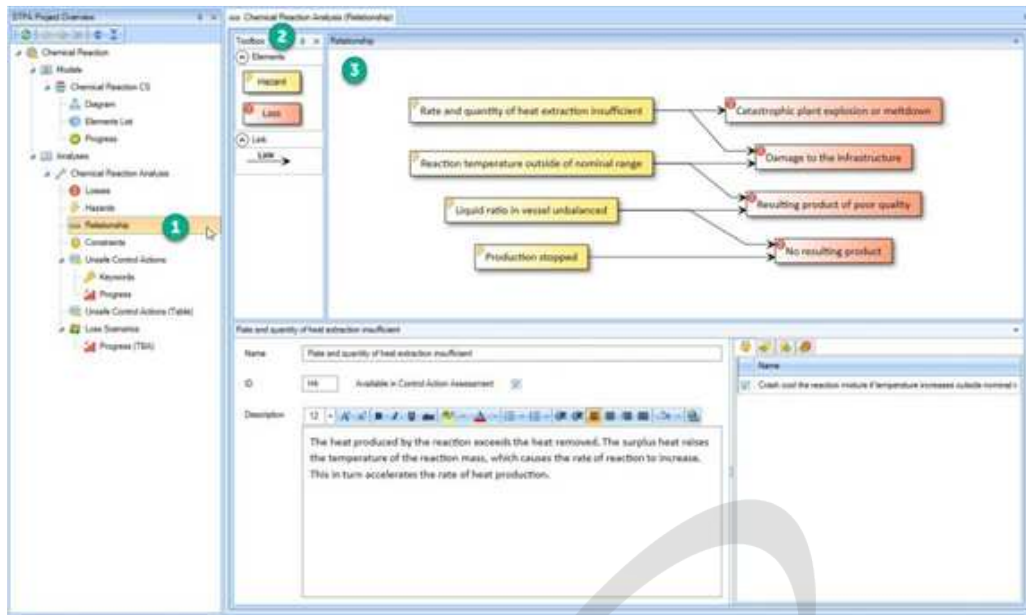


그림 부록 1-10. RMStudio Loss-Hazard 관계 설정

(3) UCA 카테고리 정의

UCA를 식별하는 것은 STPA 분석의 핵심 요소로서 철저한 분석을 위해 많은 시간을 투자해야 하는 경우가 많다. UCA를 식별하려면 Control Structure 다이어그램에서 각 Control Action를 검토해야 한다. RMStudio STPA 모듈은 Control Structure 모델의 모든 제어 동작을 채운다. Control Action 분석에 사용되는 UCA 카테고리(Keywords)는 분석을 수행하기 전에 결정한다.

1. STPA 프로젝트 트리에서 Keywords를 실행한다.
2. 새 키워드를 추가하려면 새 항목 추가 아이콘을 클릭하여 기본 키워드를 추가한다.
3. 드롭다운 메뉴에서 Keyword를 선택한다.
4. UCA 분석에서 모두 사용하려면 Add All Default Keywords 버튼을 클릭하고 OK 버튼 아이콘을 클릭하여 작업을 완료한다.
5. 기본 키워드를 선택한 후 각 키워드 뒤에 설명 텍스트를 추가할 수 있다. 이 텍스트는 키워드 세부 정보 창에서 편집할 수 있다. 이후 UCA를 자동으로 작성하기 위한 기본 형식(template) 및 고유한 UCA 카테고리(키워드)를 만들 수 있다.

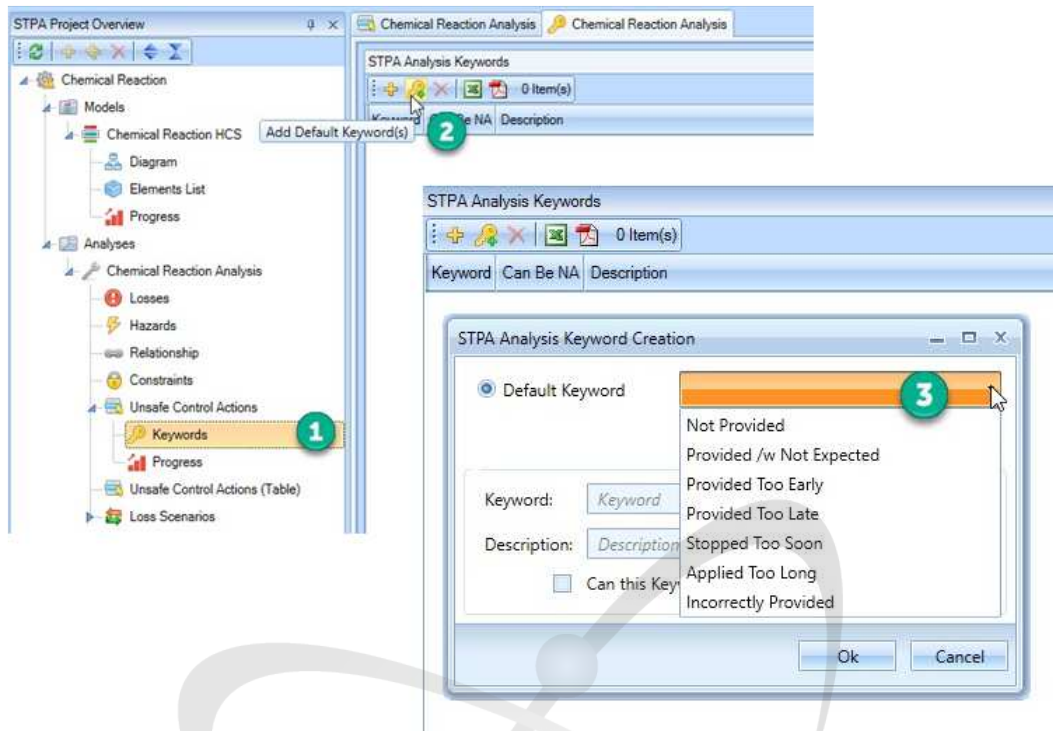


그림 부록 1-11. RMStudio Keywords 설정

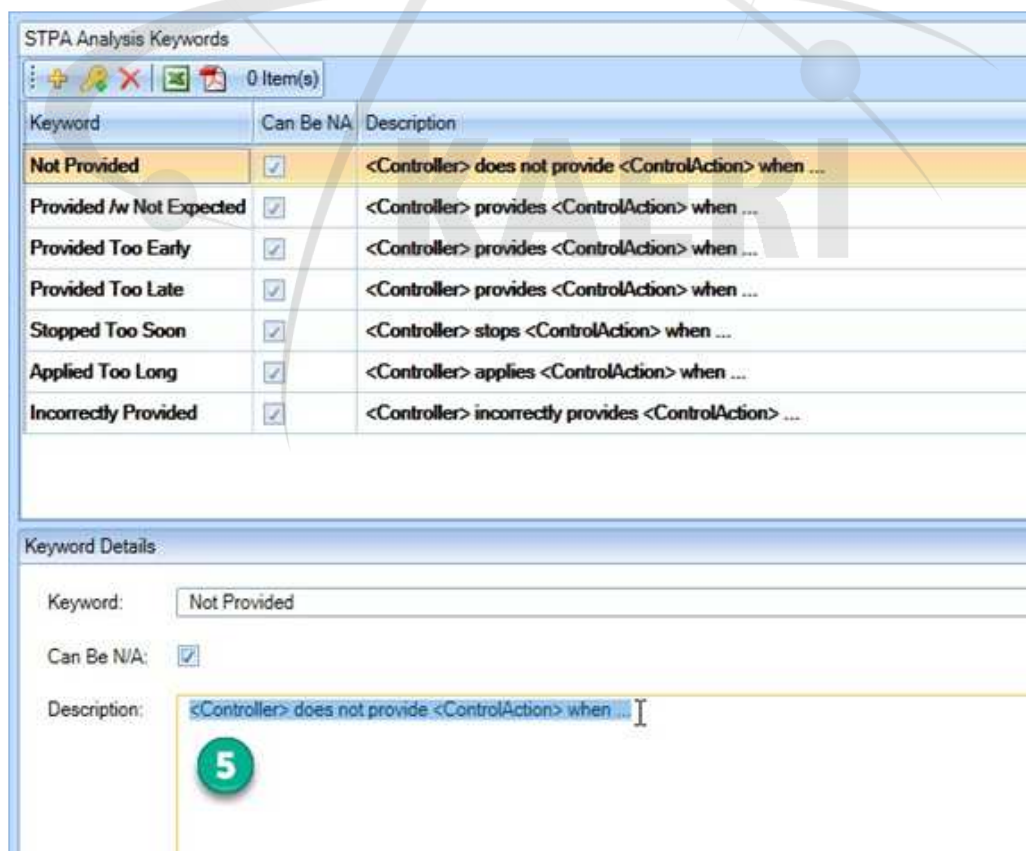


그림 부록 1-12. RMStudio Keywords 템플릿 설정

(4) UCA 식별

RMStudio는 STPA의 품질과 완전성을 보장하기 위해 다음과 같은 자동화 기능이 내장되어 있다. UCA 식별 단계에서는 제어 구조 모델의 제어 조치 목록을 채우며 다이어그램에 대한 진행률 검사를 수행할 수 있다. 이 때 모든 제어 작업 커넥터가 식별되었는지 확인하여 모든 Control Action가 UCA 분석 목록에 포함되었는지 확인할 수 있다.

1. Control Actions는 Control Structure 모델에서 생성된 순서대로 표시된다.
2. 마우스 포인터가 Control Action 위를 맴돌면 Source와 Target이 표시되며 분석가는 Control Structure 모델에서 Control Action가 위치한 위치를 확인할 수 있다.
3. 이 UCA에 대해 선택된 Keyword가 채워지고 분석을 수행한다.
4. New item add 아이콘을 클릭하여 새 UCA를 추가할 수 있으며 Delete(삭제) 아이콘을 클릭하여 작성된 UCA를 삭제할 수 있다.
5. UCA 생성 시, Keyword가 평가되었음을 나타내는 확인 표시가 Evaluated(평가됨) 상자에 나타난다. UCA를 생성하지 않으면 Assessed(평가됨) 확인란을 선택하여 해당 Control Action가 안전함을 표시할 수 있다. 여기서 안전함이란 키워드로 설명된 비상 상황이 발생하더라도 어떠한 위험도 야기하지 않는다는 것을 의미한다.
6. N/A를 사용하여 Keyword를 적용할 수 없음을 표시할 수 있다. N/A는 Keyword로 기술된 상황에 대해 Control Action이 적용될 수 없음을 의미한다.

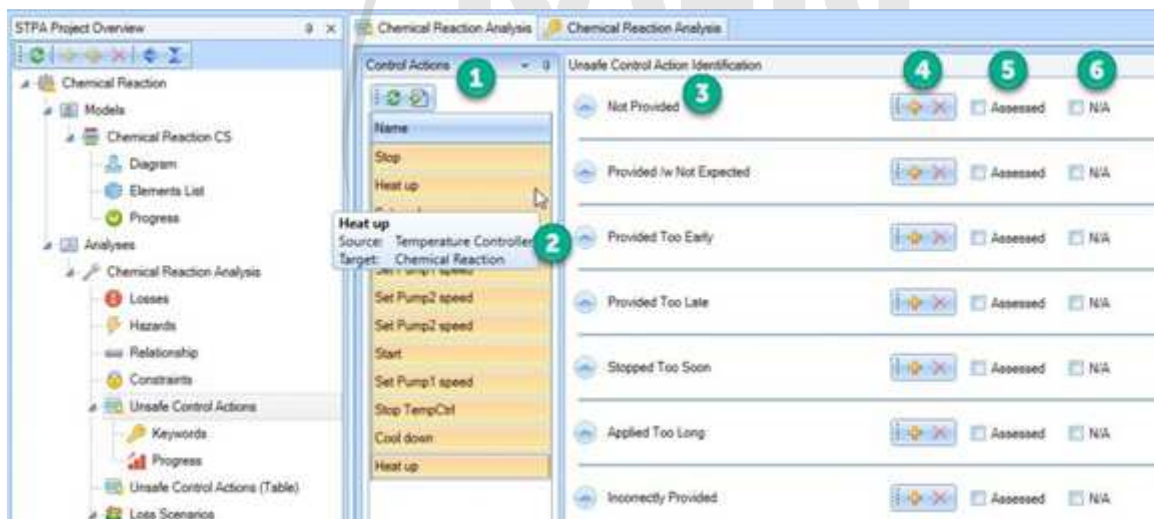


그림 부록 1-13. RMStudio UCA 식별

4. 결과 리포트 생성

STPA 분석을 수행한 뒤, Reporting을 통해 분석 결과를 생성할 수 있다. 생성된 결과 리포트는 각 분석 단계별 분석자가 설정한 Loss, Hazard, Loss-Hazard 관계를 보여주며, UCA로 평가된 Control Action을 정리하여 보여준다.

Analyses

2 Chemical Reaction Analysis

Description	
Related Models	Chemical Reaction CS

2.1 Losses and Hazards

Losses

ID	Name	Description
L1	No resulting product	
L2	Resulting product of poor quality	
L3	Damage to the infrastructure	
L4	Catastrophic plant explosion or meltdown	Thermal runaway can occur because, as the temperature increases, the rate at which heat is removed increases linearly but the rate at which heat is produced increases exponentially. Once control of the reaction is lost, temperature can rise rapidly leaving little time for correction. The reaction vessel may be at risk from over-pressurisation due to violent boiling or rapid gas generation.

Hazards

ID	Name	Description	Relationship
H1	Production stopped		L1
H2	Liquid ratio in vessel unbalanced		L1, L2
H3	Reaction temperature outside of nominal range	The chemical reaction temperature	H3, L2, L3
H4	Rate and quantity of heat extraction insufficient	The heat produced by the reaction exceeds the heat removed. The surplus heat raises the temperature of the reaction mass, which causes the rate of reaction to increase. This in turn accelerates the rate of heat production.	H4, L3, L4

그림 부록 1-14. RMStudio Reporting - Loss/Hazard 분석 결과 예시

2.4 Unsafe Control Actions

	Not Provided	Provided /w Not Expected	Provided Too Early	Provided Too Late	Stopped Too Soon	Applied Too Long	Incorrectly Provided
Stop	0 UCA	0 UCA	0 UCA	0 UCA	0 UCA	N/A	0 UCA
Set Pump2 speed	1 UCA ()	0 UCA	0 UCA	0 UCA	---	---	---
Heat up	1 UCA (H1, H3)	0 UCA	0 UCA	0 UCA	1 UCA ()	0 UCA	N/A
Set Pump1 speed	0 UCA	0 UCA	1 UCA ()	0 UCA	0 UCA	1 UCA (H2)	N/A
Set Pump1 speed	---	---	---	---	---	1 UCA ()	---
Heat up	---	---	---	0 UCA	1 UCA ()	---	---
Start	---	---	---	---	0 UCA	---	---
Cool down	0 UCA	0 UCA	0 UCA	1 UCA (H3, H4)	0 UCA	1 UCA ()	0 UCA
Set Pump2 speed	---	0 UCA	0 UCA	1 UCA ()	0 UCA	0 UCA	---
Set mode	2 UCAs (H3, H2)	0 UCA	N/A	0 UCA	0 UCA	N/A	0 UCA
Stop TempCtrl	---	---	---	---	---	---	---
Cool down	---	---	---	---	---	1 UCA ()	---

List View

Cool down	
Not Provided	---
Provided /w Not Expected	---
Provided Too Early	---
Provided Too Late	---
Stopped Too Soon	---

Applied Too Long	Assessed
UCA-12: «Operator» applies «Cool down» when ... Assumption: Interpretation: Leads to Hazards ()	
Incorrectly Provided	---
Cool down	
Not Provided	Assessed
No UCA identified	
Provided /w Not Expected	Assessed
No UCA identified	
Provided Too Early	Assessed
No UCA identified	
Provided Too Late	Assessed
UCA-4: «Temperature Controller» provides «Cool down» control action later than expected causing insufficient heat extraction Assumption: Interpretation: Leads to Hazards (H3, H4)	
Stopped Too Soon	Assessed
No UCA identified	
Applied Too Long	Assessed
UCA-11: «Temperature Controller» applies «Cool down» when ... Assumption: Interpretation: Leads to Hazards ()	
Incorrectly Provided	Assessed
No UCA identified	
Heat up	
Not Provided	Assessed
UCA-1: «Temperature Controller» does not provide «Heat up» control action when the current temperature value is below the nominal threshold and automatic temperature control is enabled. Assumption: Interpretation: Leads to Hazards (H1, H3)	
Provided /w Not Expected	Assessed
Provided Too Early	Assessed
No UCA identified	

2.5 Loss Scenarios

Unsafe Loss Scenarios

Control Action	Description	Source	UCAs
Heat up	US-3: New Loss Scenario	Feedback	
Set mode	US-1: New Loss Scenario caused by the Unsage Control Action that will lead to the system-level hazards	Controller, Feedback	
	US-2: New Loss Scenario	None	UCA-2
	US-4: New Loss Scenario is entered here. This looks weird. The UCA is on both sides of the Description feild.	Controller	UCA-2

Hazard Loss Scenarios

Control Action	Description	Source	Hazards
Heat up	HS-2: New Loss Scenario	Action	H1
Set mode	HS-1: New Loss Scenario	Action	H2

KAERI



서지정보양식

KAERI보고서번호	KAERI/TR-8100/2020	보고서종류	기술보고서
제 목 / 부 제	STAMP/STPA기반 하나로 연구용원자로 운영 프로세스 모델링 및 평가		
주저자 및 부서명	이상훈 (리스크·신뢰도평가연구실)		
공저자 및 부서명	신성민, 박진균 (리스크·신뢰도평가연구실)		
출 판 지	대전	발 행 일	2020.06.02
공 개 여 부	공개(○), 비공개()	참 고 사 항	총 페이지 p. 156 표(20)개, 그림(42)개, 참고문헌(38)개
비 밀 여 부	대외비(), _ 급 비밀		
초록 (15-20줄 내외)			
<p>본 연구에서는 STAMP/STPA체계에 따라 최근 불시정지 횟수가 많았던 하나로 연구용원자로 CNS 계통 운영 프로세스를 모델링하고, 이를 토대로 원자로 불시정지를 유발할 수 있는 Unsafe Control Action(UCA)를 도출하였다. STAMP/STPA기법은 계통의 안전에 직접적으로 영향을 미치는 기기의 고장뿐 아니라, 정상적 기기 혹은 관련 계통간의 상호작용 및 인적오류, 환경과 같은 시스템 외적인 요인까지 통합적으로 고려한 위험 요소를 분석할 수 있는 체계를 제공해준다.</p> <p>본 연구에서 STPA분석절차는 1) 계통 친숙화, 2) 계통 운전 관련 자료 분석, 3) 계통 STPA 모델(Control Structure) 개발, 4) 계통 UCA 도출 및 검토의 단계로 수행되었다. 개발된 계통 STPA 모델에서 제어(Control action)는 운전절차서에 명시되어있는 계통 구성 기기들(밸브, 펌프 등)의 운전 원리를 바탕으로 작성되었다. 계통별 제어 목록을 바탕으로 6가지 UCA 카테고리에 따라 전문가 판단 및 제 3자 검토를 통해 RRS에 의한 CNS 수소계통 수소 고/저압력 불시정지가 발생할 수 있는 UCA들을 도출하였다.</p> <p>도출된 UCA의 타당성을 평가하기 위해 하나로 운전원 및 전문가 자문을 통해 각 UCA들의 평가지표에 따른 검토를 수행하였으며 해당 UCA들이 기존의 정지이력을 사전에 시사할 수 있었는지 분석하였다. 본 분석을 통해 도출된 UCA들은 시스템의 비정상적인 행위를 포함하여 운전절차서, 인적 오류에 이르는 운전원 관련 위험요인들을 식별하며, 안전성 분석뿐만 아니라 원자로 재가동간의 위해상태 분석을 위한 기초자료로 활용할 수 있을 것으로 판단된다.</p> <p>본 분석에서는 UCA 도출까지를 분석범위로 설정하였는데 더 나아가 FMEA를 활용하여 각 UCA 발생 원인(Causal Factor)을 추가적으로 분석할 시, 보다 체계적으로 불시정지 보완요건을 도출할 수 있을 것이다. 또한, 기존 Control Structure에 계통 운영관련 추가요소들(현장운전원, 운전원간 지시체계 등)을 모델링 할 시 더 구체적이고 포괄적인 운영 프로세스 분석이 가능할 것으로 기대된다.</p>			
주제명키워드 (10단어내외)	하나로 연구용원자로, 운영안전성 평가, STAMP, STPA		

BIBLIOGRAPHIC INFORMATION SHEET

KAERI Report No.	KAERI/TR-8100/2020		Report Type	Technical Report	
Title / Subtitle	Operational Process Modelling and Analysis for HANARO Research Reactor based on STAMP/STPA				
Main Author and Department	Sang Hun Lee (Risk Assessment and Management Research Team)				
Co-Author and Department	Sung Min Shin, Jinkyun Park (Risk Assessment and Management Research Team)				
Publication Place	Daejeon	Date of Publication	2020.06.02	Total number of page	p. 156
Open	Open(<input type="radio"/>), Closed (<input type="radio"/>)		Reference	Tabs. (20) Figs. (42) Refs. (38)	
Classified	Restricted(<input type="radio"/>), __Class Document				
Abstract (15–20 Lines)					
<p>In this research, the operational process of the CNS system in HANARO research reactor which caused major spurious reactor trip events during last decade was modelled based on STAMP/STPA framework, STAMP/STPA method provides a framework that can analyze hazard factors including not only the component failures that would affect system safety, but also the unsafe interaction between normal component or related systems, human error, external factors.</p> <p>The STPA analysis procedure conducted in this research includes 1) system familiarization, 2) Review on documentations regarding system operation, 3) system STPA model development, 4) system UCA analysis. The control action in the STPA model was developed based on the operation procedures which states the component operation (valve, pump) during normal and emergency situations. Based on the control action list, UCA list was developed based on six UCA categories and examined with expert elicitation and third party review.</p> <p>In order to demonstrate the effectiveness of the proposed framework, the derived UCAs were compared with the actual spurious trip causal analysis reports. As a result, all reactor trip histories were included in the derived UCAs. Although the scope of this research is limited to UCA analysis, by conducting the causal factor analysis utilizing FMEA result, more systematical improvement strategies can be identified. In addition, if the control structure for CNS system is improved by introducing other information (field operator task, operators' command line), more detailed operation process and hazard analysis can be conducted.</p>					
Subject Keywords (About 10 words)	HANARO Research Reactor, Operational Safety Assessment, STAMP, STPA				