원자력 발전소 안전 필수 시스템의 FMEA 분석 결과의 적정성 평가를 위한 템플릿

정세진 *, 유준범 *, 이장수 **

* 건국대학교 컴퓨터공학과
** 한국 원자력 연구원

{jsjj0728, jbyoo}@konkuk.ac.kr
{jslee}@kaeri.re.kr

Safety-critical system의 위해도 분석

- Safety-critical system should be certificated before used
  - 원자력 발전소의 시스템에는 여러 표준들이 적용되어 인증을 필요로 함

  - Hazard analysis는 시스템의 사용을 위한 certification 및 개발에 중요한 역할을 담당
    - Functional safety standard – safety requirements 할당을 위한 분석
    - Safety assessment 자체로 사용

원자력 소프트웨어 표준 체계

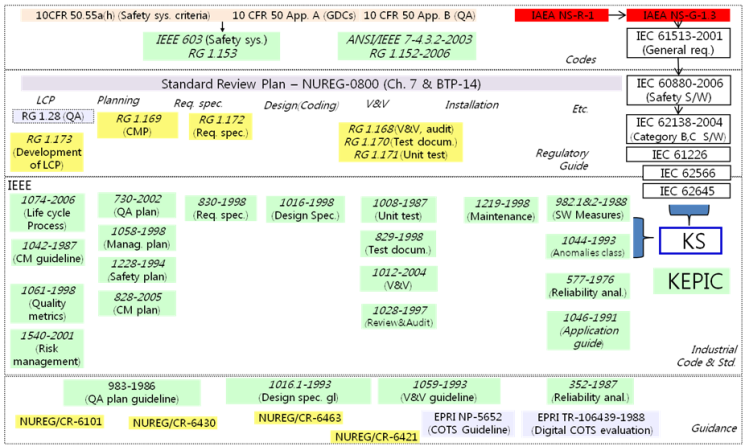
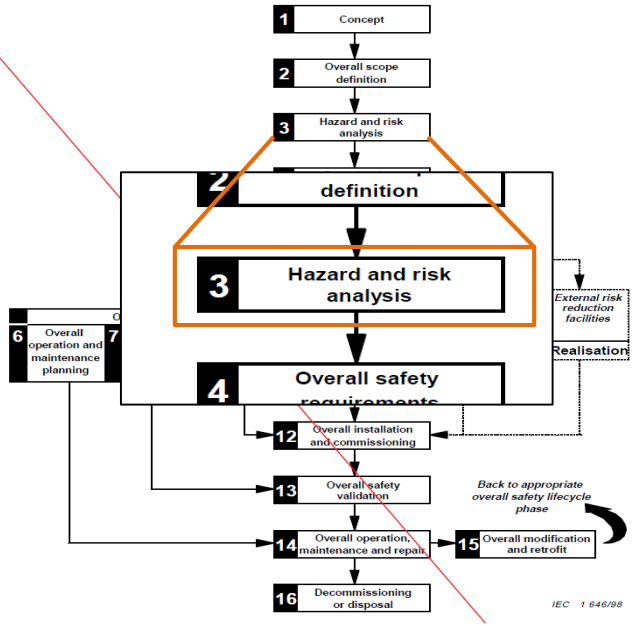


Table E.10 – Functional safety assessment (see clause 8 of IEC 61508-3)

	Technique/measure	Ref	SIL2	Interpretation in this application
1	Checklists	B.2.5	R	Used
2	Decision/truth tables	C.6.1	R	Used to a limited degree
3	Software complexity metrics	C.5.14	R	Not used for limited variability programming
4	Failure analysis	Table B.4	R	Cause-consequence diagrams at system level, but otherwise, failure analysis is not used for limited variability programming
5	Common cause failure analysis of diverse software (if diverse software is actually used)	C.6.3	R	Not used for limited variability programming
6	Reliability block diagram	C.6.5	R	Not used for limited variability programming



Safety-critical system의 위해도 분석 – FMEA

- FMEA is an one of the most used techniques in safety system traditionally
  - System/software의 function, item, component 등의 고장모드로 부터 그 영향 분석
  - 아래의 worksheet을 이용

  - **Component 의 single failure** 분석에 용이
  - **분석 時 failure mode 설정이 중요 : failure mode 로 부터 effect를 분석하는 기법이기 때문**

- **현재 위해도 분석에 대한 요구사항만 있을 뿐 분석 결과의 평가를 위한 방법은 부족**

위해도 분석 결과의 적정성 평가는
***'일정 수준 이상의 분석 결과를 포함하고 있음을 확인'* 으로 정의 할 수 있음**

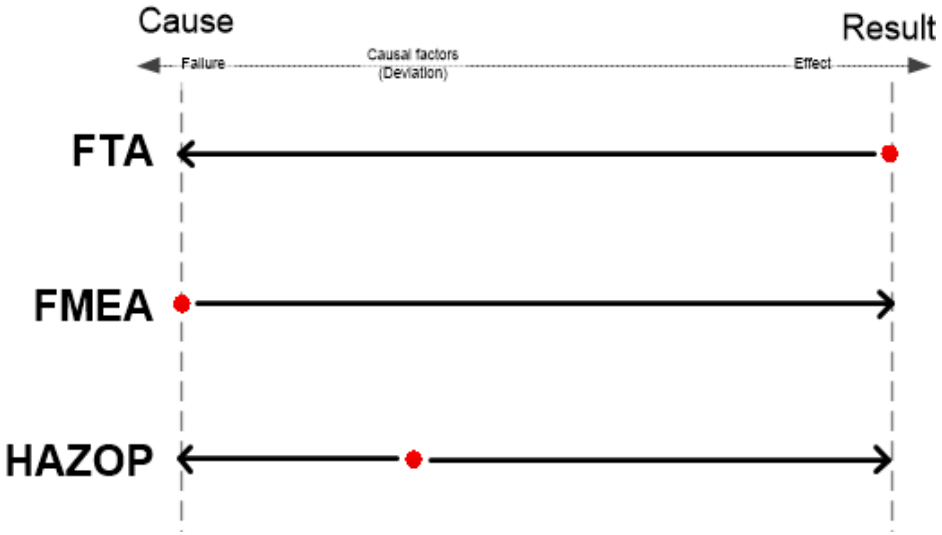
Failure Mode and Effects Analysis										
System: (1)				Subsystem: (2)				Mode/Phase: (3)		
Item	Failure Mode	Failure Rate	Causal Factors	Immediate Effect	System Effect	Method of Detection	Current Controls	Hazard	Risk	Recomm Action
(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)

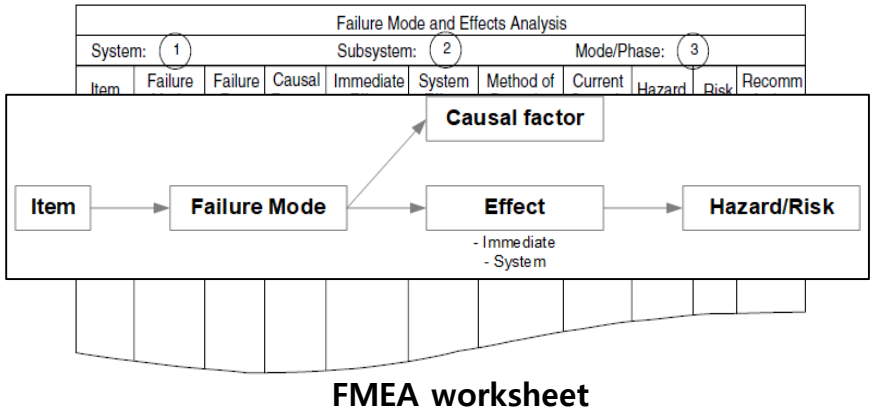
FMEA worksheet

시작점 분석

- FMEA는 cause (failure mode)로 부터 result (effect)를 분석하는 기법
  - '일정 수준 이상'의 기준이 될 수 있는 지점 판별을 위함
  - ('올바른 내용' 을 가지고 분석을 시작했는가를 확인하는 **시작점**)

FMEA의 시작점은 올바른 '고장 모드'의 확인
-> 이런 고장 모드 (failure mode)를 기준으로 생각





FMEA worksheet

FMEA 분석을 위한 템플릿 – 시작점 분석

- FMEA의 시작점인 '고장 모드'의 확인, 평가와 관련해 고려할 만한 사항들 존재
  - IEEE 379, "IEEE Standard of single failure criterion"
    - 표준화된 기초적인 failure criteria 제공: 기본적 내용으로 사용 가능
  - RIL 1002, "Identification of Failure Modes in Digital Safety Systems – Expert Clinic Findings"
    - 다양한 failure mode들에 대한 분석 보고서

Analysis of portions of systems in IEEE 379	
1. Interconnections between redundant channels	다른 채널과의 연결 부 확인 (data logger, test circuit 등)
2. System logic	System 기능
~~3. Actuation devices~~	
4. Electrical power supplies	전원 관련 분석
5. Auxiliary supporting features	보조 시스템 관련 분석
6. Sensing lines	Sensor 관련 분석

Analysis of portions of systems in IEEE 379	**Failure modes in RIL 1002**
Interconnections between redundant channels	K.8 (K.9)
System logic	K.1, K.2, K.3 K.4, K.5, K.6, K.7
~~Electrical power supplies~~	
~~Auxiliary supporting features~~	
Sensing lines	-

ID	Failure Mode	Elaboration	Remarks/Mapping
K.1	No output upon demand	Includes no change in output or no response for any input	⇒A.2
K.2	Output without demand	e.g.: Unwanted response	⇒A.3
K.3	Output value incorrect	Incorrect response to input or set of inputs	⇒A.2 Includes: • Value too high or too low; Value stuck at previous value, e.g.: ON, OFF
K.4	Output at incorrect time	Too early; Too late.	⇒A.1

FMEA 분석을 위한 템플릿

- 기존의 failure mode를 분석하여 카테고리화
  - 대부분의 결과 보고서는 failure mode를 대상 컴포넌트의 실패 경우로만 정의하고 있음

- 추가적으로 원자력 발전소의 소프트웨어 기반 시스템의 특징을 위한 추가 내용 포함
  - 9 번 세분화
  - 10번 추가

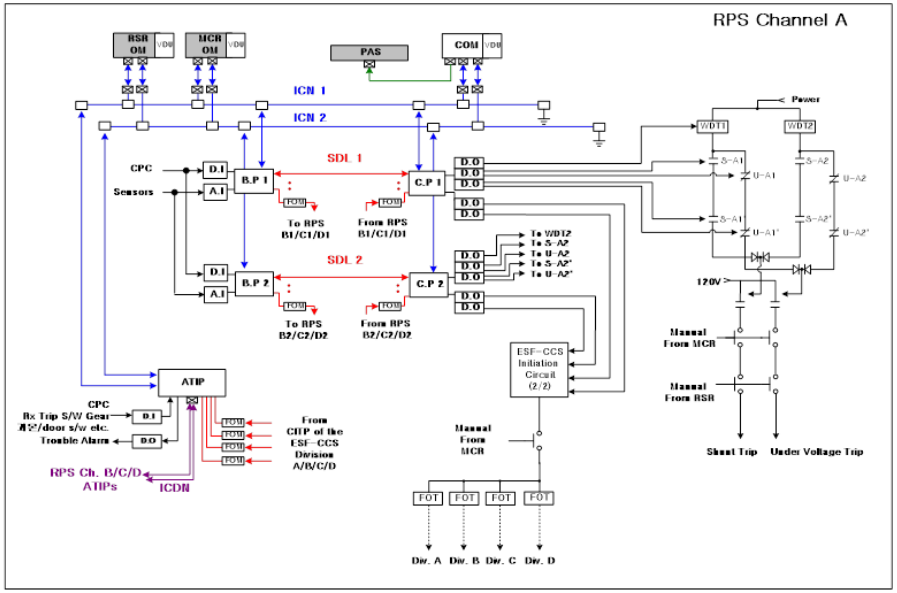
ID	Failure Mode
1	No output upon demand
2	Output without demand, unwanted response
3	Output value incorrect
4	Output at incorrect time
5	Output duration too short or too long
6	Output intermittent
7	Output flutters
8	Interference
9	Input failure
9-1	No input is inserted
9-2	Input value incorrect
9-3	Input at incorrect time or duration
10	Physical failure of component

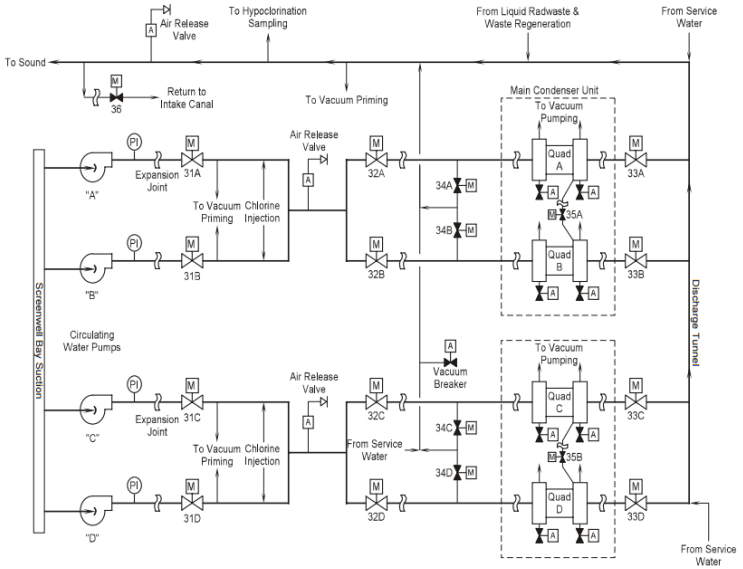
사례 연구

- 기존의 분석 사례를 이용해 template의 적정성 확인 및 보완 수행
  - 각 항목을 failure mode화 하여 template과 비교

- 원자력 발전소를 대상으로 한 두 종류의 분석 보고서 이용
  - KNICS-RPS-AR102, "원자로 보호계통 고장유형 및 영향분석 보고서"

  - Hazard analysis results of HPCI RCIC Governor Design in EPRI "Hazard analysis method for digital instrumentation and control systems"





사례 연구를 통한 확인

- 대부분의 case가 template 범위 내에 포함됨을 확인

Component	Failure Modes	Template No.
main control room and remote Shutdown panel flow indicating cont rollers	Output fails offscale low	3
	output fails offscale high	3
	output fails as-is	6
Hand-Switch	fail open	2
	fail closed	1
magnetic pickup	output fails offscale high	3
	output fails offscale low	3
	excessive drift	-
24 VDC Power	voltage below specification	3, 9-1
	voltage above specification	3, 9-1
Positioner	shorted output	5
	Open input	5
Steam admission valve limit switch	fail open	2
	fail closed	1
Governor program interface	inadvertent logic change	8
Governor	output fails offscale high	3
	output fails offscale low	3
	output fails as-is	6
	output high rate of change	3
Resolver Feedback	output fails offscale high	3
	output fails offscale low	3
	inaccurate signal	3
	failed mechanical connectio n between actuator and go vernor valve	9-2
24 VDC Power	voltage below specification	3, 9-1
	votage above specification	3, 9-1

Failure Mode	발생 장치 (component)	Template No.
고 신호 유지 (설정치 이상)	아날로그 입력	9
저 신호 유지 (설정치 이하)	아날로그 입력	9
ON 상태 고장	디지털 입력	9
OFF 상태 고장	디지털 입력	9
출력 OFF	전원 입력 장치	1
출력 HIGH	전원 입력 장치	9-2
서지보호가 안됨 (기능이상)	서지전압보호기	1
잡음제어가 안됨 (기능이상)	잡음제어기	1
개방불능	차단기	1
개방	차단기	2
팬 고장 탐지 불능	팬 고장 감시장치	1
ON 고장	스위치	1
OFF 고장	스위치	2
작동고장	팬	1
프로세서 정지 고장	프로세서 모듈, 통신 프로세서 (152, 153), 통신 드라이버 (154, 155)	1, 4
프로그램 고장	프로세서 모듈, 통신 프로세서 (152, 153), 통신 드라이버 (154, 155)	-
표시고장	LED	1
주 전원공급기 고장 탐지 못함	전원고장경보모듈	1
보조 전원공급기 고장 탐지 못함	전원고장경보모듈	1
출력 Too High	주 전원 공급 모듈, 보조 전원 공급 모듈	9-2
팬 1,2,3,4의 고장감시 회로로 전원공급 불능 고장	팬 고장 감시 장치	2
단선, 단락	퓨즈	9-1
단락 또는 과부하시 전원차단불능	퓨즈	9-1
시간측정 느림	감시 타이머	5
시간측정 빠름	감시 타이머	5
단일 입력점 고 고장	아날로그 입력 모듈	9
단일 입력점 저 고장	아날로그 입력 모듈	9
단일 입력점 ON 고장	디지털 입력 모듈	9
단일 입력점 OFF 고장	디지털 입력 모듈	9
Close 고장	연계계전기	1
Open 고장	연계계전기	2
ON 고장	광전송기	1
OFF 고장	광전송기	2
단일 출력점 고 고장	아날로그 출력모듈	3
단일 출력점 저 고장	아날로그 출력모듈	3
출력 on 고장	감시 타이머	4
출력 off 고장	감시 타이머	4
장치 전체 고장	아날로그 출력모듈, 디지털 출력모듈	1
AD 변환값이 부정확	아날로그 입력모듈	9
단일 출력점 ON 고장	디지털 출력 모듈	1
단일 출력점 OFF 고장	디지털 출력 모듈	1
AD 변환값이 부정확	아날로그 출력모듈	3

결론 및 향후 연구

- FMEA 분석 결과의 평가를 도울 수 있는 템플릿 개발
  - Failure criteria 및 시작점 분석을 통한 failure mode들 이용
  - 필요한 사항들을 보완 및 추가
  - 실제 제시된 FMEA 분석 결과를 이용한 case study 수행
- 현재 software-based control system의 system 적인 측면에 더 초점을 맞추고 있음
  - 향후, software 중심적인 내용에 대한 연구 수행 예정
  - 다른 다양한 기법들의 템플릿 및 해당 기법들과 연계해 분석, 평가할 수 있는 방법 연구 중