열차제어시스템(mock-up)의 위험원 분석을 위한 Type과 Technique의 선정에 대한 연구

A Study on selection of the Type and the Technique for the Hazard Analysis of the Train Control System(mock-up)

한찬희*	이영수**	안 진**	조우식**
Han, Chan Hee	Lee, Young Soo	Ahn, Jin	Jo, Woo Sic

ABSTRACT

It has been studying actively that the process and the methodology for the safety security of the system suggested from international standards and domestic/abroad materials in Korea. However, these process & methodology can generate a lot of errors and deficiencies because the system is applied without considering the system characteristics and its scope (such as hardware, software, interface, etc.).

Therefore, the type is defined as the safety process with the basis on general development process in this study, the potential hazards of the mock-up system which is developed are extracted thorough selecting a technique according to each type. In addition to it, the effect is compared and analyzed with various technique selection by each phase of the development process.

1. 서 론

안전성을 확보하기 위한 Safety Process 및 Technique는 각종 국제규격이나 특성화 된 지침서 등에서 제시하고 있으며, 국내에서도 다양한 연구체계와 사업으로 이에 대한 연구가 매우 활발히 이루어지고 있다. 각종 규격에서 제시 및 권고하고 있는 Safety Process 및 적용 Technique는 크게 다르지 않으며, 시스템에 대한 적용성에 대한 사항이 고려되지 않은 일반적 내용을 다루고 있다. 그렇기 때문에 개발하고자 하는 시스템의 특성 및 범위(하드웨어, 소프트웨어, 인터페이스 등)를 전혀 고려하지 않고 적용되어 시스템 위험원의 도출 및 분석에 많은 오류와 실패 그리고 위험원의 누락 등이 발생하게 된다.

본 연구에서는 국제규격에서 제시하는 일반적인 프로세스들을 수집.비교하여 개발하고자 하는 열차제어시스템인 mock-up시스템의 전체 Safety process로 적용하여 개발 프로세스에 접목시켰다.

또한 Safety Process를 진행하기 위해 필수적 요소인 Hazard Analysis를 위해 개발 프로세스를 Type으로 분류하였으며, 이러한 Type에 적합한 Technique를 선정하여 mock-up시스템의 Hazard Analysis에 적용하였다. 또한 상세설계 단계에서 적용 가능한 Technique인 SSHA와 FMEA의 특성을 비교 분석하여 그 적합성을 분석하였다.

* 대아티아이(주), 연구소, 주임연구원
E-mail : chaneess@daeati.co.kr
TEL : 032) 680-0895 FAX : 032) 680-0885

** 대아티아이(주), 연구소, 수석연구원

** 대아티아이(주), 연구소, 책임연구원

2. System Safety Process

System Safety Process는 개발되는 시스템이 내재하고 있는 잠재적인 위험이나 결함을 찾아 제거하거나 그 발생확률을 저감시키거나 치명도를 줄일 수 있도록 하드웨어, 소프트웨어, 설비, 환경, 운영, 문서 등을 고려한 모든 활동에 대한 체계 및 절차를 제공하는 것이다.

2.1 Safety Process 조정

System Safety Process는 하나의 팀에서 단독적으로 수행할 수 없으며, 개발하고자 하는 System Process에 따라 유동적으로 수행된다.

여기서 말하는 Process는 Lifecycle과 동일한 개념으로 적용하며, 수많은 System Process (System Lifecycle)는 System의 다양한 환경 및 조건에 따라 변경이 되므로, 우선적으로 System Process및 일정이 확정되면 이에 따라 적합하게 System Safety Process 및 일정을 조정하게 된다.

2.2 Safety Process 비교 및 정의

System Safety Process는 다음과 같은 국제표준 및 지침에서 정의하고 있다.

<그림 1. Safety Process 정의 규격>

본 연구에서는 미국의 국방규격인 MIL_STD_882D의 Safety Process와 IEC61508에서 제시하는 Safety Process를 비교하여 다음과 같이 표현하였다.

<표 1. Process 비교>

MIL_STD_882D			IEC 61508	
Safety Plan	1	→	1	Concept
Identify Hazard	2	→	2	Overall Scope Definition
Assess Hazard Risk	3	→	3	Hazard and Risk Analysis
Identify safety measures	4	→	4	Overall Safety Requirement
Reduce Risk	5	→	5	Safety Requirement Allocation
Verify Risk Reduction	6	→	6	Overall Planning
Review Hazard & Risk	7	→	7	Safety related systems E/E/PES
Track Hazard	8	→	8	Overall Installation
		→	9	Overall Safety Validation
		→	10	Overall Operation and Maintenance

위에서 제시된 규격에서의 Safety Process의 단계들 중 통합 또는 세분화 시켜야 할 단계를 구분하여 mock-up시스템에 적용할 수 있는 Safety Process를 다음과 같이 구성하였다.

- 1. System Definition
- 2. Safety Plan
- 3. Hazard and Risk Analysis

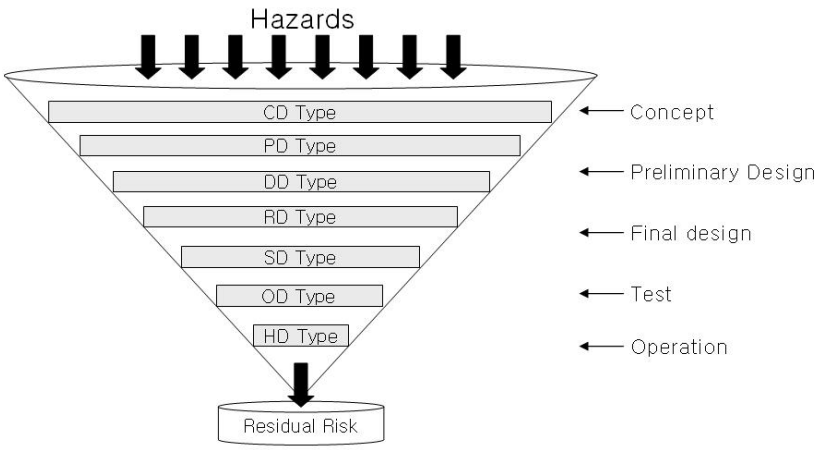
    - 3.1 Hazard Identification
    - 3.2 Consequence Analysis
    - 3.3 Risk Estimation
    - 3.4 THR Allocation
- 4. Safety Requirement
- 5. Hazard Control
- 6. Safety Test & Validation
- 7. Safety Case
- 8. Safety Assessment
- 9. Safety Approval

3. Hazard Analysis Type

Hazard Analysis를 수행하기 위해서는 시스템 개발Lifecycle의 각 단계에 적합한 분석기법을 적용해야 하는데, 이러한 분석기법도 다음과 같은 분석Type에 따라 7단계로 분류된다.

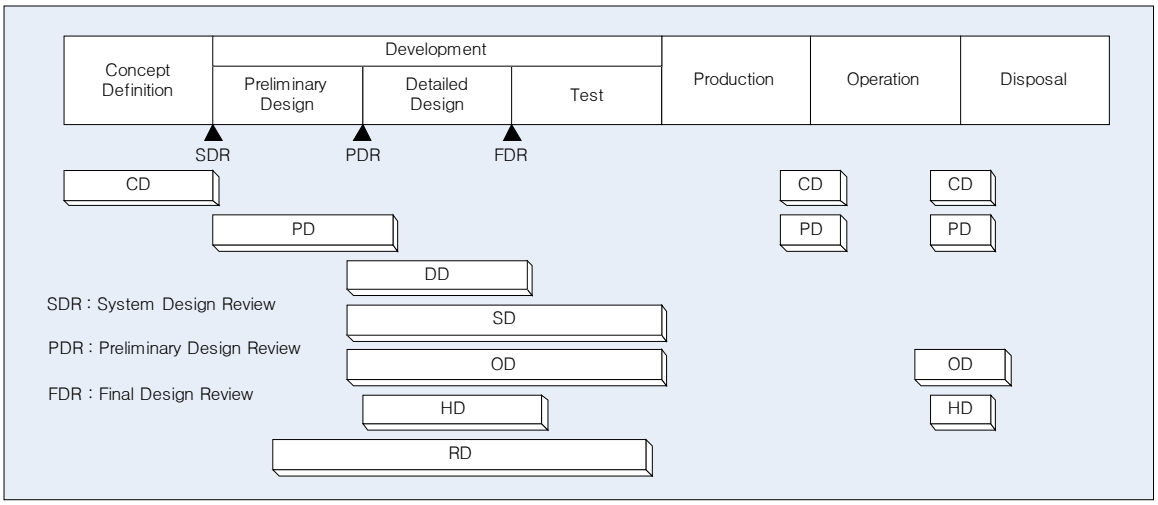
- Conceptual design hazard analyusis type - **CD** type
- Preliminary design hazard analysis type - **PD** type
- Detailed design hazard analysis type - **DD** type
- System design hazard analysis type - **SD** type
- Operations design hazard analysis type - **OD** type
- Health design hazard analysis type - **HD** type
- Requirements design hazard analysis type - **RD** type

위와 같은 분석Type의 순차적인 수행은 전체 시스템에서 발생할 수 있는 잠재적인 Hazard를 필터링하여 보다 완벽하게 안전성을 확보할 수 있다.
다음의 그림은 Hazard analysis Type으로 인한 필터링에 대한 개략도를 보여준다.



<그림 2. Hazard filters >

Hazard Analysis type은 전체 시스템 개발 Lifecycle에서 다음과 같이 배치된다.



<그림 3. Lifecycle과 Type>

4. Hazard Analysis Technique

Hazard Analysis Technique은 매우 다양하며, 고유의 분석 특성을 지니고 있다. 그렇기에 개발 시스템에 적용되는 Technique은 시스템의 특성과 Technique의 특성에 맞게 선별하여 적용하여야 한다.
유럽규격인 EN50129에서는 Software의 Hazard Analysis Technique으로 다음과 같이 SIL에 따라 권고하고 있다.

<표 2. EN50129 권고 Technique>

방법	SIL 1	SIL 2	SIL 3	SIL 4
PHA	HR	HR	HR	HR
FTA	R	R	HR	HR
Markov diagrams	R	R	HR	HR
FMEA(FMECA)	R	R	HR	HR
HAZOP	R	R	HR	HR
Cause-consequence diagrams	R	R	HR	HR
ETA	R	R	R	R
Reliability block diagram	R	R	R	R
Zonal analysis	R	R	R	R
Interface hazard analysis	R	R	HR	HR
Common cause failure analysis	R	R	HR	HR
Historical event analysis	R	R	R	R

위의 규격에서 권고되고 있는 사항 이외의 Technique을 추가하여 적합한 Type과 특성들을 정리하면 다음과 같다.

<표 3. Technique별 특성 비교>

Technique	Type	Identify Hazard	Identify Root Causes	Lifecycle Phase	Qualitative/ Quantitative	Level of Detail
PHL	CD	Y	N	CD~PD	Qualitative	Minimal
PHA	PD	Y	P	CD~PD	Qualitative	Moderate to in-depth
SSHA	DD	Y	Y	DD	Qualitative	In-depth
SHA	SD	Y	Y	PD~DD~Test	Qualitative	In-depth
O&SHA	OD	Y	Y	PD~DD~Test	Qualitative	In-depth
HHA	HD	Y	Y	PD~DD~Test	Qualitative	In-depth
FTA	SD, DD	P	Y	PD~DD	Qualitative/quantitative	Moderate to in-depth
ETA	SD	P	P	PD~DD	Qualitative/quantitative	Moderate to in-depth
FMEA	DD	P	P	PD~DD	Qualitative/quantitative	In-depth
HAZOP	SD	Y	P	PD~DD	Qualitative	Moderate to in-depth
FaHA	DD	P	P	PD~DD	Qualitative	In-depth
FuHA	SD	P	P	CD~PD~DD	Qualitative	Moderate to in-depth

위와 같은 Technique의 특성을 고려하여 열차제어시스템인 mock-up시스템에 다음과 같이 적용하였다.

<표 4. mock-up시스템 적용 Technique>

Analysis Type	Coverage	Hazard Focus	Primary Analysis Technique
CD	Conceptual design	System hazards	PHL
PD	Preliminary design	Systems hazards	PHA
DD	Detailed subsystem design	Subsystem hazards	FMEA, SSHA
DD, SD	Detailed subsystem design/ Integrated system design	Subsystem hazards/ Integrated system hazards	FTA
SD	Integrated system design	Integrated system hazards	ETA, SHA, HAZOP
OD	Operational design	Operational hazards	O&SHA

본 연구에서 수행된 Analysis Technique은 FMEA와 SSHA의 비교이다. 그 이유는 적용되는 mock-up시스템은 소프트웨어의 위험원을 분석하여 안전성을 확보하는 것이 목표이기 때문에, 일반적으로 하드웨어에 적합한 FMEA가 어느정도의 정확성과 신뢰성을 가지고 소프트웨어에 적용할 수 있는지 SSHA의 결과와 비교해야 하기 때문이다.

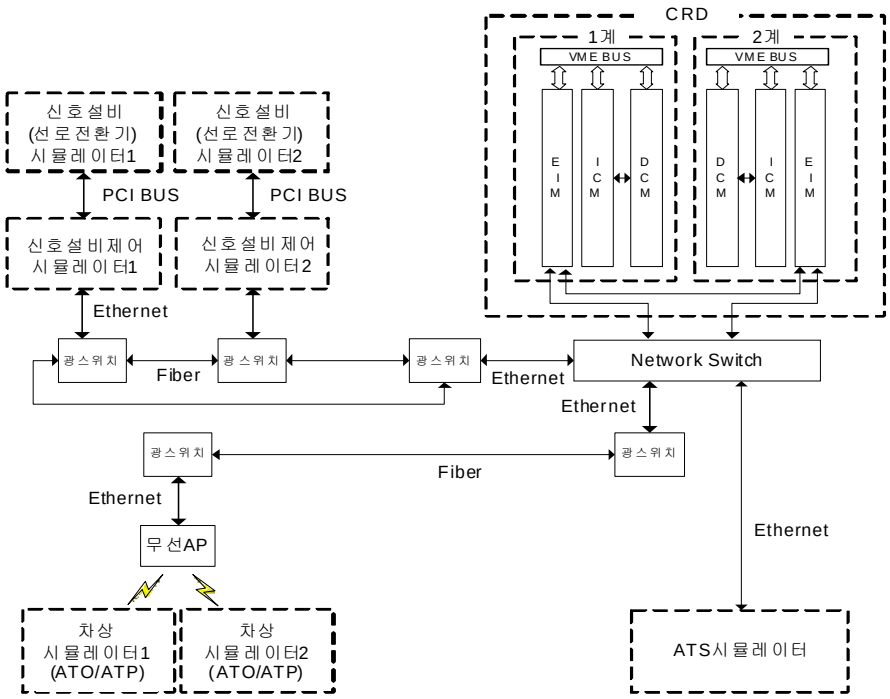
5. 적용사례

5.1 mock-up시스템

5.1.1 mock-up시스템 구성

mock-up시스템의 범위는 연동기능과 열차간격제어를 위한 Control Route Distance 시스템과 자동열차감시장치인 ATS시뮬레이터, 실제 차상장치 기능을 구현하기 위한 차상시뮬레이터와 현장신호설비 기능을 구현하기 위한 신호설비제어시뮬레이터 및 신호설비(선로전환기)시뮬레이터로 구성된다.

안전성활동은 mock-up시스템 중 진로제어 및 간격제어를 담당하고 있는 CRD(Control Route Distance) 시스템으로 한정하며, 타 구성 시스템과의 인터페이스도 안전성활동에 포함시켰다.



<그림 4. mock-up시스템 구성>

5.1.2 기능

CRD의 기능은 크게 진로설정제어부와 열차간격제어부로 나뉜다. 다음은 CRD의 주 기능에 대한 사항이다.

<표 5. mock-up시스템 기능>

1. 진로설정제어		2. 열차간격제어	
1.1	진로설정명령 처리	2.1	열차간격제어
1.2	진로취소명령 처리	2.2	열차위치확인
1.3	전체진로취소명령 처리	2.3	열차이동/방향 감시
1.4	선로전환기 제어명령 처리	2.4	임시속도제한명령 처리
1.5	현장신호설비상태 처리	2.5	블록개방/폐쇄명령 처리

5.2 SSHA (Subsystem Hazard Analysis)

mock-up시스템의 SSHA는 CRD의 진로설정제어부와 열차간격제어부의 세부 주기능에 대한 분석으로 수행되었다. 우선 SSHA의 결과를 간략하게 요약하면 다음의 표와 같다.

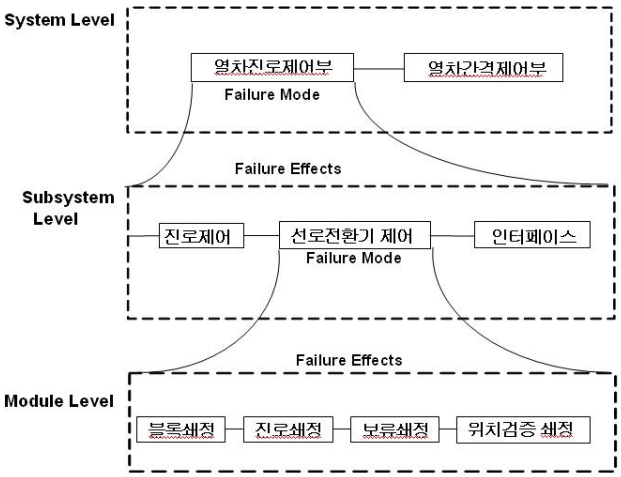
<표 6. mock-up시스템 SSHA>

No.	Hazard	Causes
SSHA-1	진로설정명령 처리 오류	비정상적인 진로설정 명령 데이터
		비정상적인 진로설정 명령
		진로-큐 입력 실패
		진로-큐 용량 초과
		선로전환기 상태 오류
		진로설정명령 출력 실패
SSHA-2	진로취소명령 처리 오류	비정상적인 진로취소 명령
		허용이동권한 설정 실패
		진로-큐 삭제 실패
		진로취소명령 출력 실패
SSHA-3	선로전환기 상태정보 처리 오류	Database 업데이트 오류
		외부시스템으로 메시지 전송 처리 실패
SSHA-4	비정상적인 ICM전원공급	과전압, 과전류
		불안정한 전원
SSHA-5	제어명령 수신 실패	EIM 모듈 오류
SSHA-6	현장정보 수신 실패	EIM 모듈 오류
SSHA-7	현장정보 송신 실패	EIM 모듈 오류
SSHA-8	제어명령 송신 실패	EIM 모듈 오류
SSHA-9	허용이동권한 설정 오류	허용이동권한설정을 위한 정보 부족
		허용이동권한 Red설정 오류 및 실패
SSHA-10	비정상적인 열차위치	차상시뮬레이터와의 무선통신 실패
		열차위치 오류
SSHA-11	열차이동/방향 감시 오류	열차위치 비교분석 실패
		열차위치 오류
SSHA-12	열차임시속도제한 명령 처리 오류	비정상적인 임시속도제한 명령
		임시속도제한명령 출력 실패
SSHA-13	블록 개방/폐쇄 오류	열차분실시 자동 블록폐쇄 실패
		인접블록 허용이동권한 설정 오류
		해당블록 개방 가능유무 확인 실패
SSHA-14	비정상적인 DCM 전원공급	과전압, 과전류
		불안정한 전원
SSHA-15	블록 제어명령 수신 실패	EIM 모듈 오류
SSHA-16	열차정보 수신 실패	EIM 모듈 오류

SSHA의 결과 CRD시스템의 Hazard는 총 17개, 각 Hazard에 따른 원인이 중복을 제외하고 25개가 도출되었다. SSHA는 DD-Type에서 수행되는 Technique으로서 도출된 Hazard 및 Causes는 SD-Type이나 OD-Type에서 세분화 되고 구체적인 분석이 수행된다.

5.3 FMEA (Failure Mode & Effect Analysis)

FMEA는 다층구조로 분석하는 기법으로써, 시스템레벨의 고장모드가 하위시스템레벨에서는 고장의 결과가 되는 구조이다. 다음은 CRD시스템의 선로전환기에 대한 FMEA 구조를 설명한 그림이다.



<그림 5. mock-up시스템 FMEA 구조 예>

FMEA의 결과는 다음과 같다.

<표 7. mock-up시스템 FMEA 고장모드>

Level	Item(Function)	Failure Mode
System Level	연동	열차 탈선
		열차 충돌
		...
	열차방호	열차 탈선
		열차 충돌
		...
	인터페이스	열차 지연
Subsystem Level_1	진로제어	잘못된 진로로 열차 진입
		중복된 진로설정
		...
	선로전환기제어	잘못된 방향으로 선로전환기 전환
		선로전환기 쇄정/해정 실패
		...
	열차간격제어	열차위치 오류 및 확인실패
		열차이동 방향 오류
		...
	열차감시	열차위치 검증 실패
		임시속도 제한명령 처리 실패
		...
	가상블록처리	인접블록 결정 오류
		열차검지 처리 실패
		...
Subsystem Level_2	선로전환기 쇄정/해정	블록쇄정/해정 실패
		진로쇄정/해정 실패
		보류쇄정/해정 실패
		위치검증 쇄정/해정 실패
	ATS시스템 인터페이스	메시지 미송신
		불완전한 메시지
		...
	신호설비제어시뮬레이터 인터페이스	메시지 미송신
		불완전한 메시지
		...
	열차이동권한정보 처리	진로설정상태 오류
		선로전환기 상태 오류
		...
	차상시뮬레이터 인터페이스	메시지 미송신
		불완전한 메시지
		...

CRD시스템의 FMEA는 13가지의 Item(Function)에 대해 Failure Mode를 고려하였으며, 각 Failure Mode에 따른 원인과 영향의 도출과 대책/권고조치사항에 대해 작성되었다.

6. 결과

mock-up 시스템의 CRD시스템에 대한 안전성 활동을 위해 Lifecycle 단계를 Type으로 분류하였으며, 각 Type에 적합한 Technique을 선정한 결과 DD-Type에서는 SSHA와 FMEA 두 기법이 선정되었다. 그러나, CRD시스템에 대한 안전성 활동은 CRD 소프트웨어와 소프트웨어적인 인터페이스로 범위를 한정하였기에, SSHA와 FMEA의 두 기법의 비교를 통해 소프트웨어에 더욱 적합한 기법에 대해 알아보았다. 그 결과, 두 기법의 장단점은 다음과 같다.

<표 8. SSHA와 FMEA 장단점 비교>

Technique	SSHA	FMEA
장 점	• PHL, PHA와 연계적으로 수행이 가능함. • 단기간 수행이 가능함. • 기능에서 발생할 수 있는 Hazard 도출이 비교적 쉬움. • 차후 진행되는 SHA와 연계적 수행이 가능함.	• 시스템 레벨에 따른 고장모드 선정으로 인해 상하위 레벨간 관계성이 높음. • 체계적인 분석이 가능함. • 차후 진행되는 ETA, FTA와 연계적 수행이 가능함.
단 점	• 복잡한 시스템에 내재되어 있는 잠재적인 위험원을 도출하기 어려움. • 레벨에 따른 Hazard의 관계성이 떨어짐.	• 많은 시간을 필요로 함. • 규모가 큰 시스템일 경우 분석이 복잡해 짐.

SSHA와 FMEA 모두 소프트웨어 안전성 분석에는 크게 문제될 사항은 없었다.
단지, 지속적인 안전성 활동을 위해 연계적으로 수행되는 기법에 따라 선택하는 것이 중요하다. 즉, DD-Type 이후의 SD-Type을 고려해야 한다. FMEA의 방법론은 ETA와 FTA를 연계적으로 수행하기에 적합한 방법임이 많은 연구논문에서 제시되기도 하였으며, 정량적인 결과를 도출하기에 적합하다.

참고문헌

1. Clifton A. Ericson, Hazard Analysis Techniques for System Safety, 2005, pp.5-11, 31-54
2. Jens Braband, Railway Automatic Hazard Analysis.
3. Jeffrey W.Vincoli,CSP, Basic Guide to system safety, second edition, 2006.
4. 김병석, 나승훈, 시스템 안전공학, 형설출판사,2002.
5. BS EN 50129, Railway applications-communication, signaling and processing systems-safety related electronic systems for signaling, 2003.