Tool을 적용한 철도신호시스템 위험원 분석에 대한 연구

A Study on hazard analysis of railway signaling system applied for a tool

박성규* 한찬희** 조우식** 안진**

Park, Sung-Gue Han, Chan-Hee Cho, Woo-Sik An, Jin

ABSTRACT

In this study it is researched to the hazard analysis phase which is the core phase of the safety life cycle carried out by various systems in Korea.

At present diverse methods are utilized when the hazard analysis is performed. With the basis of these V&V activities are carried out.

In this study using FMEA which is one of the representative methods of the hazard analysis, the effective and viable result is derived. Also, it establishes the systematic base of the further phases of the safety life cycle such as the Hazard log, V&V, and the safety case.

---

1. 서론

철도신호시스템은 매우 복잡하고 다양한 조건에 의해 구현되기에 많은 특성들 중에서 안전성이 매우 중요한 시스템이다. 특히 소프트웨어의 신뢰성 및 가용성에 대한 정량적인 계산이 불명확하기에 소프트웨어의 안전성 확보는 더욱 중요시 되고 있으며, 그 방법과 프로세스에 대한 연구가 활발히 이루어지고 있다.

본 연구는 국내 다양한 시스템에서 수행되고 있는 안전성 라이프사이클 중 핵심적인 단계인 Hazard Analysis 단계에 대해 다루었다. 국내에서도 Hazard Analysis를 수행함에 있어 다양한 기법이 활용되고 있으며, 이를 기반으로 한 V&V활동이 여러 방면에서 수행되고 있다.

본 연구에서는 Hazard Analysis의 대표적 기법인 FMEA를 Tool을 적용하여 보다 효과적이고 가시적인 결과를 도출하고자 하였으며, 이는 안전성 라이프사이클의 차후 단계인 Hazard log, V&V 그리고 Safety case를 수행할 수 있는 체계적인 기반을 마련하였다.

* 책임저자 : 비회원, DaeaTI, R&D, 책임연구원
TEL : (032) 680-0895

** 비회원, DaeaTI, R&D, 연구원

2. 본문

2.1 배경

국내 여러 철도신호시스템 구축 사업이나 프로젝트에서 안전성을 확보하기 위해 다양한 표준 및 규격을 바탕으로 안전성 활동이 이루어지고 있다. 이러한 안전성 활동은 체계적인 프로세스에 따라 시스템에서 발생 가능한 잠재적 hazards를 도출하고 이에 대한 분석을 통해 제거 또는 저감대책을 수립하게 되며, 시스템의 운용에 이르기까지 테스트와 검증을 거쳐 안전성을 확보하게 된다.

현재 철도신호시스템에서 개발되고 적용되고 있는 철도신호 소프트웨어는 점점 복잡해지고 대형화 되고 있으며, 이러한 이유로 인해 소프트웨어에서의 error 및 장애가 발생할 경우에는 그 원인 및 장애지점을 찾아내기가 매우 어려워지고 있다. 따라서 위에서 제기한 안전성 프로세스를 소프트웨어에 적용할 경우, 보다 신중하고 세밀한 분석이 이루어져야 하며 체계적인 방법에 의해 소프트웨어를 개발하여 쉽게 결함을 검지하고 찾아낼 수 있도록 하여야 한다.

유럽에서는 CENELEC EN50128을 제정하여 철도 응용소프트웨어 개발절차를 정의하고 있으며, 독일에서는 MU8004를 제정하여 소프트웨어의 개발 및 검증 체계를 구축하고 있다.

기타 국내 및 국외 소프트웨어 관련 규격은 다음과 같다.

① 국내 규격

KS A IEC 60812	고장모드영향분석 (FMEA)
KS A IEC 61025	결함나무분석 (FTA)
KS X 2209	소프트웨어 테스트 문서화
KS X 2226	시스템과 소프트웨어 무결성 레벨

② 국외 규격

IEC 62279	철도신호분야 안전관련 소프트웨어
IEC 61882	HAZOP application
IEC 60812	고장모드영향분석 (FMEA)
IEC 61025	결함나무분석 (FTA)
IEEE std 830	Recommended practice for software requirement specification
IEEE std 1008	Standard for software testing

*** 출처 : 철도종합안전기술개발사업 - 철도소프트웨어 안전기준 체계구축. 2005. 8. 7

본 연구에서는 현재 설계 및 개발이 진행되고 있는 열차제어시스템을 대상으로 하고 있으며, 주된 안전성 활동은 소프트웨어에 맞춰 수행되었다.

대상 소프트웨어는 대부분 시스템에서 제어기능을 수행한다. 이는 다른 컴포넌트들과의 빈번한 인터페이스를 가질 뿐만 아니라 전기-기계식 컴포넌트의 기동과 컴포넌트들 간의 상호작용을 제어한다. 대부분의 사고가 컴포넌트들 간의 인터페이스와 상호작용에서 발생하기에 소프트웨어는 시스템 안전에 직접적이고 중요한 역할을 하며, 시스템 안전에서 빼 놓을 수 없는 요소이다. 소프트웨어가 안전하다는 것은 소프트웨어가 그 시스템 안에서 위험요소를 만들지 않고 실행하는 것을 의미한다. 소프트웨어는 두 가지 방식으로 시스템 안전에 영향을 미칠 수 있다.

- 시스템을 위험한 상태로 들어가게 하는 출력 값과 타이밍을 나타낼 수 있다.
- 제어 또는 응답하도록 요구되는 하드웨어 고장을 인식하거나 처리할 수 없게 된다.

본 논문에서는 위에서 정의한 안전에 영향을 미치는 조건들을 기반으로 열차제어시스템(소

프트웨어)에 대한 hazards를 도출하였으며, 이에 대한 분석을 '고장모드 영향분석(FMEA)'을 적용하여 수행하였다. 그러나 FMEA분석은 여러 표준이나 규격에서 제시하는 방법에 따라 작성하다보니 다음과 같은 어려움이 나타났다.

- 전체 대상 열차제어시스템의 주요 원인에 대한 파악이 어렵다.
- 주요(우선) 관리대상에 대한 파악이 어렵다.
- Hazards의 제거 및 저감을 위한 action에 대한 분류가 어렵다.
- 규격화된 sheet 작성으로 분석 결과에 대한 가시적 표현이 어렵다.

이와 같은 FMEA 작성 결과에 대한 다양한 어려움을 해결하기 위해 본 연구에서는 FMEA의 수행을 지원해 줄 수 있는 tool을 선정하여 적용하였으며, 그 특징으로는 다음과 같다.

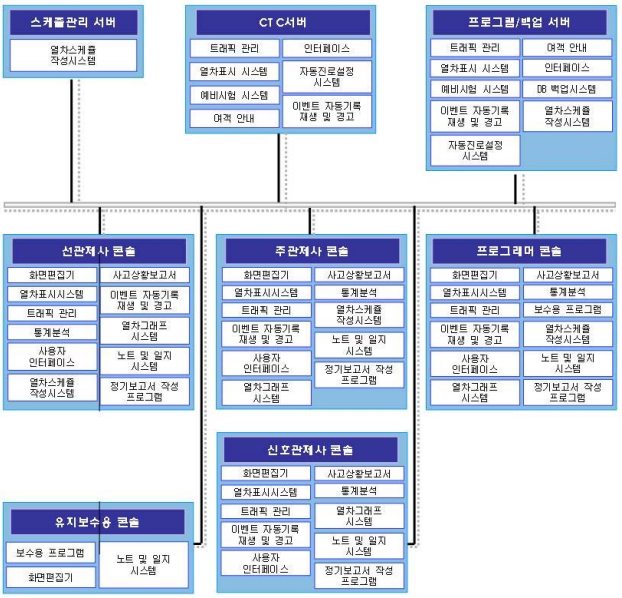
- 전체 또는 각 요소의 분석 결과에 대해 각 분류별 해석이 가능하다.
- 분석 결과에 대한 가시적 표현이 가능하여 보다 효과적으로 의사전달이 가능하다.
- 분석 결과에 대한 보고서를 표준 및 규격에 적합하도록 출력할 수 있다.
- 지속적인 관리가 용이하다.
- 차후 다른 시스템에 재활용 가능하여 Hazard(Risk) Analysis단계의 소요시간을 줄일 수 있다.

2.2 대상시스템(소프트웨어)

대상시스템은 예비관제시스템으로 국내 철도교통을 관제하고 있는 철도교통관제센터의 비상 상황이나 장애 발생 시 신속한 운용체계의 변환으로 관제업무의 연속성을 유지할 수 있도록 지원하는 백업시스템으로서의 기능뿐만 아니라 평상시 예비관제실 상시 근무자를 위한 철도교통관제의 모니터링 기능을 갖추고 있는 시스템이다.

예비관제시스템 중 소프트웨어적인 기능적 범위는 다음과 같다.

- CTC기본 소프트웨어 기능
- 열차운행관리 소프트웨어 기능
- 업무지원 소프트웨어 기능
- 상호운용을 위한 추가 소프트웨어 기능



<그림 1. 예비관제시스템 소프트웨어 구성도>

예비관제시스템의 소프트웨어 구성은 <그림1>에서와 같이 총 8개의 서버 및 콘솔에 탑재되며, 4개의 주요상위기능과 74개의 세부하위기능으로 구성된다. 본 연구에서는 74개의 세부하위기능에 대한 FMEA를 수행하여 세부하위기능에서 발생할 수 있는 에러 및 고장에 대한 제거 및 저감대책을 수립하였으며, 이에 대한 안전성 관리가 지속적으로 수행될 수 있도록 문서화 하였다.

2.3 FMEA Analysis

2.3.1 FMEA 사전정의 사항

대상시스템의 FMEA를 수행하기 위한 sheet 구성은 다음과 같다.

Function	Failure	Effect	Si	Cause	Oi	Di	RPNi	Control	Control type	Action	Sr	Or	Dr	RPNr

위험도 우선 수(RPN:Risk Priority Number)는 자동차와 소프트웨어 개발분야, FMEA를 단순한 위험도 평가방법으로 확장시키는 분야 등에서 적용되는 기법으로서 FMECA로 산출되기도 한다. RPN의 출발점은 시스템 정의 혹은 시스템 요소들에 대한 규명이다. 그런 다음, 상상가능한 모든 고장과 그에 대한 결과를 조사하고, 조사 결과를 도표로 기록한다. 이때 상상가능한 모든 고장모드 i와 그 치명도 Si, 발생가능성 Oi, 해당 고장을 발견할 가능성 Di를 필요로 한다.

$$RPNi = Si \cdot Oi \cdot Si$$

RPN은 간단하기 때문에 활용률이 매우 높다. 그런데 PRN을 활용하는 기법은 다음과 같은 점에서 위험도 분석과 구분된다.

-RPN 기반 기법에서는 실제적인 부분 위험도 R나 한계 위험도의 준수 여부를 도출할 수 없다.

-위험노출시간이나 위험잠복기등의 주요 변수들이 고려되지 않는다.

-감소지수(변수O)가 너무 개략적으로 반영된다.

-부분 위험도는 대개 통합적으로 고려되어야 하지만 본 기법에서는 독립적으로 관찰된다.

RPN은 지금까지 FMECA의 틀 내에서 사용되어 온 것처럼 위험도의 상대적 비교(우선순위를 결정하기 위한 비교)에만 적합하고, 위험도 분석의 주변요건이 매우 단순할 경우에만 적용되고 있다. 이러한 이유로 인해 향후 연구사항으로 BP risk라는 새로운 개념의 위험도 분석 기법에 접근하여 RPN의 단점을 해결할 예정이다.

RPN의 값을 산출하기 위해서는 Severity, Occurrence, Detection의 변수에 대해 산출하여야 한다. 각 변수의 값은 다음과 같이 설명된다.

① Severity

Value	Description	Criteria
1	No effect	시스템 또는 승객에 전혀 영향을 미치지 않음.
2	Slight effect	승객에 대한 영향은 발생하지 않지만, 항상 인지할 수 없는 미세한 정도의 Nonvital한 결함 발생
3	Minor effect	승객은 약간의 불편함을 느낄 수 있으며, 항상 인지할 수 있는 Nonvital한 결함이 발생하지만 수리 및 유지보수가 필요치 않은 경우.
4	Significant effect	승객은 불안 및 불편함을 느낄 수 있으며, 시스템의 성능을 낮추지만 운영은 계속 할 수 있는 경우. 필요시 수리 및 유지보수 가능.
5	Major effect	승객의 부상이 발생하며, 시스템에 심각한 영향을 미쳐 수리 및 유지보수가

		반드시 필요하며 운영이 불가능한 경우.
6	Extreme effect	승객의 사망이 발생하며, 시스템에 극단적인 영향을 미쳐 장기간 수리 및 유지보수가 반드시 필요하며 운영이 불가능한 경우.

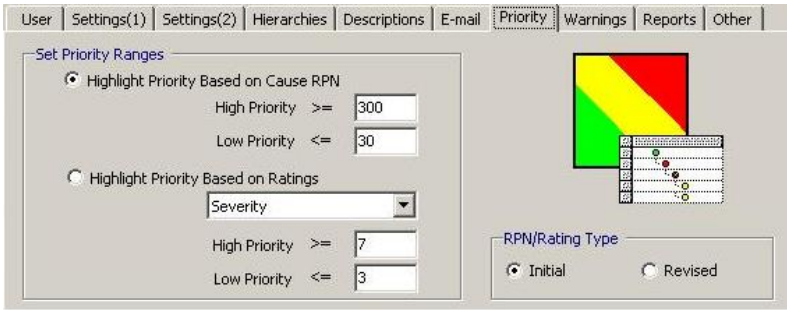
② Occurrence

Value	Description	Criteria
1	Almost never	발생가능성이 희박하며, 지금까지 발생한 기록이 없음.
2	Remote	발생가능성은 있지만, 시스템 수명동안 발생하지 않음.
3	Low	발생할 수 있으며, 시스템 수명동안 1~2회 발생함.
4	Medium	시스템 수명동안 가끔 발생함.
5	High	시스템 수명동안 여러차례 발생함.
6	Very high	시스템 수명동안 빈번하게 발생함.

③ Detection

Value	Description	Criteria
1	Almost certain	신뢰할 수 있는 검지 프로세스를 통해 대부분의 결함 및 실패는 검지할 수 있음.
2	High	높은 수준의 결함 검지
3	Medium	적당한 수준의 결함 검지
4	Low	낮은 수준의 결함 검지
5	Remote	매우 낮은 수준의 결함 검지

위에서 정의된 각 변수들에 의해 RPN이 정의되면 적용된 tool에서는 <그림.2>에서와 같이 허용가능 범위에 대해 정의하여야 한다.



<그림 2. RPN 허용범위 정의>

FMEA sheet에서의 기타 사항은 다음과 같이 정의하였다.

① Control type : Detection, Prevention

② Action Category

1	Design
2	Documentation
3	Manufacturing
4	Quality assurance
5	Support
6	Testing
7	Verification

2.3.2 FMEA 수행

대상시스템의 FMEA는 총 74가지의 소프트웨어 기능에 대해 수행하였으며, 본 절에서는 하나의 기능에 대한 sheet입력상황과 분석결과 그리고 도표해석의 예시를 보여준다.

ex) CTC 기본 소프트웨어 - 트래픽관리 - 시스템 상태조회

다음의 그림은 '시스템 상태조회' 기능에 대한 FMEA sheet입력 상황이다.

System Hierarchy

Item Name
CTC기본 소프트웨어
트래픽 관리
시스템 상태조회
통합관제시스템 상태조
프로세스 상태감시 및 제어
로그정보 관리
계정 관리
관제센터간 제어권 관리
운영모드 관리
진로제어
신호기제어
선로전환기 제어
LDTS계정관

FMEA WorkSheet - 시스템 상태조회

Failure	Effect	Si	Cause	Oi	Di	RPNi	Control	Control Type	Action	Sr	Or	Dr	RPNr
서버별 상태조회 실패	CTC유지보수 지연으로 발생한 열차운행 관제지장에 따른 열차충돌, 열차지연	4	서버상태 정보 수신처리 오류	4	2	32	운영전 인터페이스 테스트 수행	Detection	Testing	3	3	1	9
			통신라인 불량	3	2	24	통신라인 이중화	Prevention	Design		2	2	12
			통신서버 이상	3	2	24	시스템 이중화 구현	Prevention	Design		2	2	12
LDTS상태조회 실패	열차운행 관제지장에 따른 열차충돌, 열차지연	4	LDTS상태조회 정보 수신처리 오류	4	2	32	운영전 인터페이스 테스트 수행 수신 데이터 유효성 검사	Detection	Testing	3	2	1	6
			현장상태 정보 미수신	3	2	24	현장점검 및 통합관제 실과의 인터페이스 점검	Detection	Testing		1	1	3
			통신라인 불량	3	2	24	통신라인 이중화	Prevention	Design		2	1	6
			통신서버 이상	3	2	24	시스템 이중화 구현	Prevention	Design		2	1	6

<그림 3. '시스템 상태조회' FMEA sheet>

적용 tool의 사용자 인터페이스에서 보여지는 바와 같이 좌측엔 기능(item)이 위치하며, 우측엔 선택된 하나의 기능에 대한 FMEA sheet가 위치하게 된다. sheet엔 failure내역과 그 effect와 causes, control 전 RPN, control과 action, control 후 RPN을 엔지니어에 의해 입력하게 되는데, '시스템 상태조회'는 3가지의 고장이 도출되었다.

- 서버별 상태조회 실패
- LDTS상태조회 실패
- 운영자 콘솔 상태조회 실패

적용 tool에서는 입력된 사항에 대한 분석을 <그림.4>에서와 같이 Analysis Check기능을 이용하여 수행할 수 있으며, 설계반영 또는 테스트 수행 여부에 대해 확인할 수 있다.

Analysis Check Results | FMEA Checks

Check Effects:
1.1.1 - CTC유지보수 지연으로 발생한 열차운행 관제지장에 따른 열차충돌, 열차지연
: The Revised Severity rating is different than the Initial Severity rating for this Effect, This usually requires a design change.
1.2.1 - 열차운행 관제지장에 따른 열차충돌, 열차지연: The Revised Severity rating is different than the Initial Severity rating for this Effect, This usually requires a design change.
1.3.1 - 열차지연, 열차충돌: The Revised Severity rating is different than the Initial Severity rating for this Effect, This usually requires a design change.

Check Causes:
3 Causes have the same Description (통신라인 불량).
3 Causes have the same Description (통신서버 이상).

Check Controls and Actions:
2 Controls have the same Description (시스템 이중화 구현).
2 Controls have the same Description (시스템 이중화 구현
).
2 Controls have the same Description (운영전 인터페이스 테스트 수행
수신 데이터 유효성 검사).
3 Controls have the same Description (통신라인 이중화).
4 Actions have the same Description (Testing).
6 Actions have the same Description (Design).
6 Actions have the same Description (Design).
4 Actions have the same Description (Testing).
4 Actions have the same Description (Testing).
6 Actions have the same Description (Design).
6 Actions have the same Description (Design).
4 Actions have the same Description (Testing).
6 Actions have the same Description (Design).
6 Actions have the same Description (Design).

그림 4. '시스템 상태조회' Analysis Check

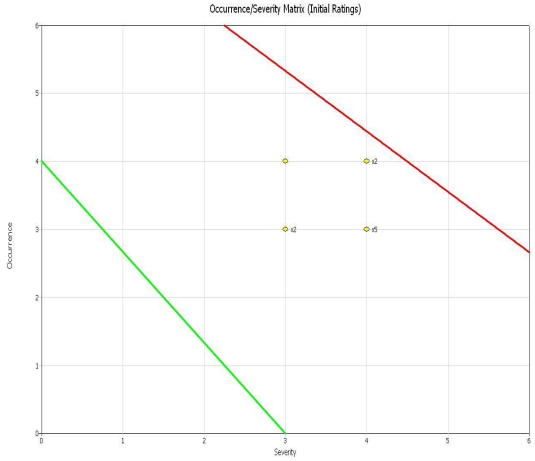
또한 <그림.5>에서와 같이 Failure-Cause Matrix에 대한 결과를 나타낼 수 있다.

	1	2	3	4	5	6	7
1		통신라인 불량	통신서버 이상	LDTS상태조회 정보 수신처리 오류	서버상태 정보 수신처리 오류	콘솔 상태 정보 수신처리 오류	현장상태 정보 미수신
2	서버별 상태조회 실패	X	X		X		
3	운영자 콘솔 상태조회 실패	X	X			X	
4	LDTS상태조회 실패	X	X	X			X

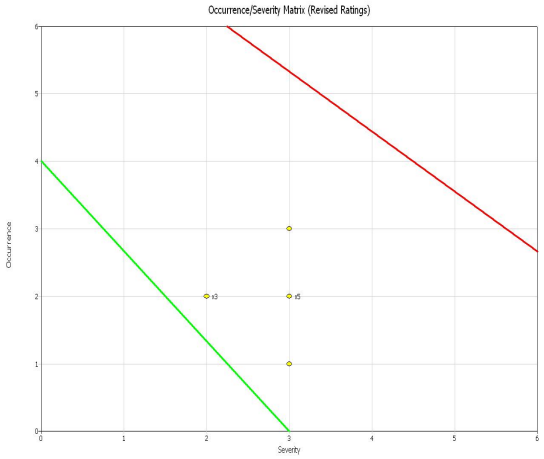
그림 5. '시스템 상태조회' Failure-Causes Matrix

위의 Analysis Check와 Failure-Cause Matrix로 시스템 상태조회 기능에서 발생할 수 있는 고장과 그 원인에 대해 쉽게 파악할 수 있다.

또한 tool을 사용하여 가시적으로 결과를 표현하여 이해도를 높일 수 있다. 우선 시스템 상태조회 기능의 RPN허용범위와 대책 전 RPN 그리고 대책 후 RPN에 대해서는 다음과 같이 나타난다.



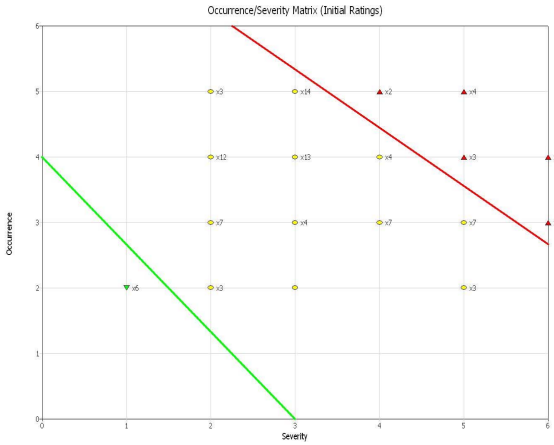
<그림 6. 대책 전 RPN>



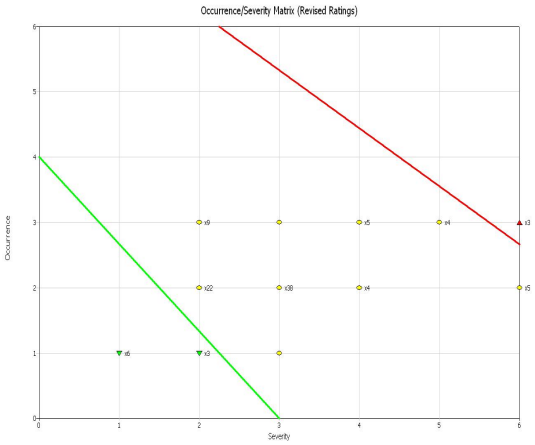
<그림 7. 대책 후 RPN>

control을 수행하기 전에 위치한 RPN수치들이 control하고 난 후 RPN수치들이 감소한 것을 확인할 수 있다. 만약 상단의 RPN 허용범위를 벗어난 값들은 최우선적으로 안전관리대상이 되며 허용범위내로 감소시키기 위한 추가적인 대책안을 필요로 함을 알 수 있다.

이와 같은 방법으로 전체 시스템에 대한 FMEA분석을 수행하여 아래와 같은 결과를 도출하였다.



<그림 8. 대상시스템 대책 전 RPN>



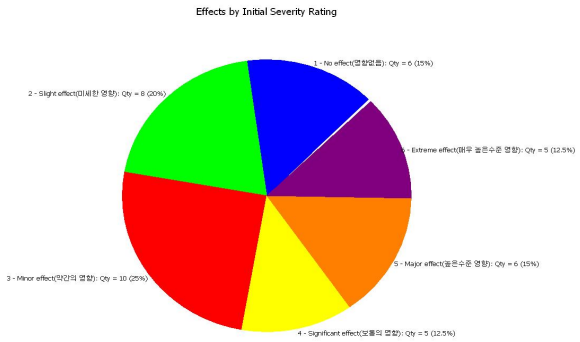
<그림 9. 대상시스템 대책 후 RPN>

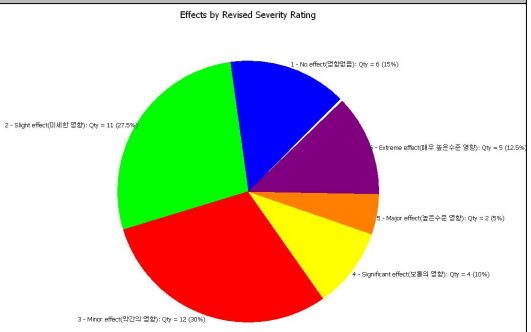
대상시스템의 대책 전 RPN을 살펴보면, 허용범위를 벗어난 17개의 기능이 존재함을 확인할 수 있다. 이러한 기능은 우선 관리 대상이 되며, 대책 수립 후에도 허용범위 밖에 존재하는 3개의 기능은 치명도를 낮출 수 있는 대책이나, 발생빈도를 줄일 수 있는 대책을 수립해야 함을 알 수 있다.

FMEA sheet에 작성된 Effect Severity와 Causes Occurrence에 대해서도 다음과 같은 결과를 나타내었다.

① Effect Severity pie

Effect (initial)	Effect (revised)





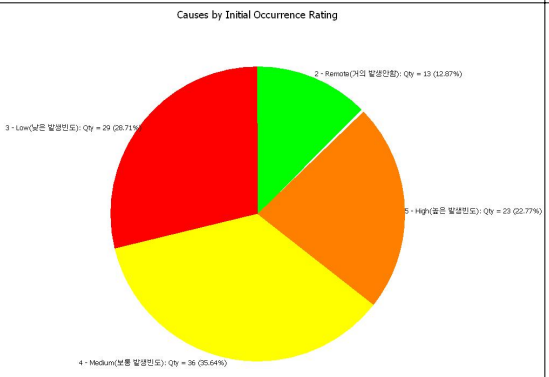
No effect	6 (15%)
Slight effect	8 (20%)
Minor effect	10 (25%)
Significant effect	5 (12.5%)
Major effect	6 (15%)
Extreme effect	5 (12.5%)

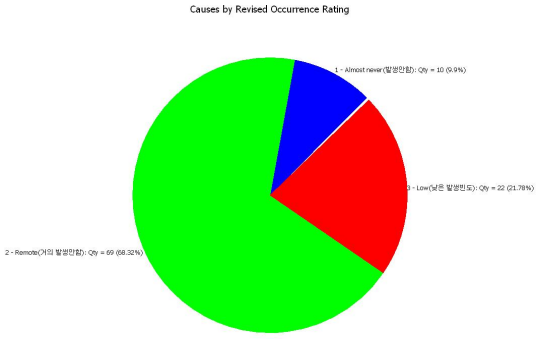
No effect	6 (15%)
Slight effect	11 (27.5%)
Minor effect	12 (30%)
Significant effect	4 (10%)
Major effect	2 (5%)
Extreme effect	5 (12.5%)

대상시스템 전체에서의 영향과 치명도의 관계를 나타낸 그림으로서, Major급 영향이 대책 수립 후엔 현격히 줄어들었으며, Slight effect가 증가하였음을 확인할 수 있다.

② Causes Occurrence pie

Causes (initial)	Causes (revised)





Almost never	0 (0%)
Remote	13 (12.87%)
Low	29 (28.71%)
Medium	36 (35.64%)
High	23 (22.77%)
Very high	0 (0%)

Almost never	10 (9.9%)
Remote	69 (68.32%)
Low	22 (21.78%)
Medium	0 (0%)
High	0 (0%)
Very high	0 (0%)

대상시스템 전체에서의 원인과 빈도간의 관계를 나타낸 그림으로서, 높은 빈도의 요소들이 모두 낮은 빈도로 떨어졌음을 확인할 수 있다.

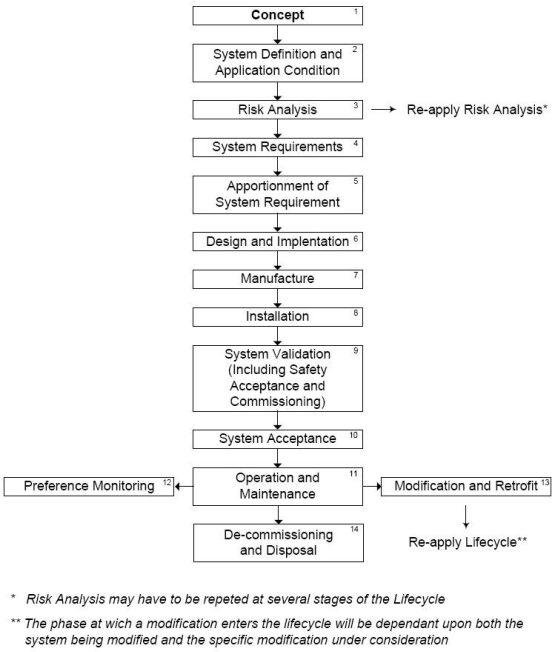
3. 결론

본 논문은 시스템(소프트웨어)의 Lifecycle중에 Risk Analysis단계에서 수행해야 하는 FMEA기법을 기존의 sheet에 문자로만 입력하던 방식에서 벗어나 tool을 사용하여 보다 효과적이고 신속한 분석이 수행됨을 증명하였다.

대상시스템인 예비관제CTC 소프트웨어는 매우 방대한 양의 기능과 다양한 인터페이스로 인한 복잡성을 가지고 있어, 내부에 잠재되어 있는 Hazards를 예상하기가 매우 어렵다.

또한 안전성 관리자는 잠재적 Hazards를 분석한 후, 구현과 테스트 그리고 운용까지 Hazards를 관리하기가 쉬운 일이 아니기에 본 논문에서는 적합한 tool사용을 권장하고자 한다.

적합한 tool사용으로 인해 안전성 관리자가 설계 및 개발 엔지니어에게 제시하고자 하는 방향을 보다 쉽게 이해시킬 수 있으며, 지속적인 Hazards 관리로 인해 Hazard log, Test, Safety Case 등의 차후활동에서도 이를 기반으로 작성 및 수행할 수 있다.



<그림 10. Lifecycle>

무엇보다도 재활용성이 높아 차후 프로젝트에서는 보다 신속하게 분석결과를 도출할 수 있는 장점을 가지고 있다.

본문에서도 언급되었듯이 RPN은 단지 관리 우선순위를 나타내는 것이기 때문에 Hazard나 Failure등의 Risk 평가를 위해서는 보다 정량적이고 체계적인 방법을 적용해야 하는 문제점을 가지고 있다. 따라서 향후 연구는 이를 해결하기 위한 평가방법에 대해 구체적인 활동이 이루어져야 할 것이다.

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. 철도종합안전기술개발사업, 철도소프트웨어 안전기준 체계구축, 2005.8, 철도기술 연구원
5. BS EN 50129, Railway applications-communication, signaling and processing systems-safety related electronic systems for signaling, 2003.