차상ATC장치의 안전성 분석

Safety Analysis of Onboard ATC System

김경식* 이종성** 강리택*** 임연수****

Kim, Kyoung-Shik Lee, Jong-Seong Kang, Lee-Teag Lim, Yeon-Su

ABSTRACT

Onboard ATC performs the train speed ristriction function by receiving the speed limit on sections of track from wayside ATC. Onboard ATC can protect passenger from collision and derailment, and so on. So, the high level of safety and reliability for Onboard ATC is required, and by this reason, it is also required to improve the safety of Onboard ATC by applying the result of safety analysis on the Onboard ATC into its design and developing from the concept definition to the detailed desing phase. The paper introduces, when developing Onboard ATC, the safety improvement of Onboard ATC can be accomplished by applying system requirements from Risk Analysis into software and hardware.

1. 서 론

차상ATC장치는 지상의 ATC장치로부터 송신되는 구간의 제한 속도를 수신하여 열차를 제한 속도 이하로 운행하도록 하는 기능을 수행한다. 차상ATC장치는 이러한 기능을 수행함으로써 열차의 추돌 및 탈선 등으로부터 승객을 보호한다. 따라서 차상ATC장치는 안전성과 신뢰성이 요구되며, 이러한 이유로 개념정의 및 설계단계에서 안전성을 분석하여 시스템에 반영하여 개발함으로써 차상ATC 시스템의 안전성을 향상시키는 것이 필요하다.

본 논문에서는 차상ATC장치 개발 수행 시 위험도분석(Risk Analysis)을 통해 분석된 시스템 요구사항을 하드웨어 및 소프트웨어에 적용함으로써 차상ATC장치의 안전성 향상이 성취될 수 있음을 소개한다.

2. 본 문

2.1 적용 범위 및 적용 원칙 (Scope and Principle)

본 논문에 언급되는 종합안전대책기술서(Safety Case)는 차상 ATC 시스템에 요구되는 안전성 요구사항을 만족시키기 위한 안전관리 엔지니어링 업무를 서술한다. 이는 차상 ATC 시스템의 개발 초기부터 설계 단계까지의 안전성 관리 업무에 대해 적용된다. 제작 및 시험 단계에 대해서는 "차상 ATC 시스템 최종 종합안전대책기술서 (Final Safety Case)에 적용된다.

또한 본 종합안전대책기술서(Safety Case) 본질적으로 차상 ATC 시스템의 수명주기 중 설계 단계까지 진행된 안전성 관리 활동의 결과를 정리한 것으로, 본 종합안전대책기술서는 다음을 입증한다.

- 차상 ATC 시스템의 잠재적인 모든 위험요인(Hazard)이 식별됨

* (주)로템, 신호팀, 비회원
E-mail : holykim@rotem.co.kr
TEL : (031)460-1281 FAX : (031)460-1787
** (주)로템, 신호팀
*** (주)로템, 신호팀
**** (주)로템, 응용기술연구팀

- 식별된 모든 위험요인의 위험도(Risk)가 적절히 평가됨
- 평가된 각 위험요인의 위험도(Risk)가 수용 가능한 수준으로(ALARP) 저감됨
- 차상 ATC 시스템에 요구되는 안전성 요구사항을 위한 설계 관련 엔지니어링 기술들은 적합하며, 그러한 안전성 요구사항들이 충족됨

이를 위해 차상 ATC 시스템 안전성관리계획서에서 서술된 안전성 관리 절차에 따른 안전성 관리활동의 결과물을 통해 차상 ATC 시스템이 요구되는 안전성을 확보했음을 입증한다.

2.2 시스템 설계 목표

차상 ATC 시스템은 아래와 같은 시스템 설계 목표에 따라 설계되었다.

(1) 시스템 이중계 설계

철도차량 안전기준에 관한 규칙 제 81조 3항에 따라 ATC 장치는 하나의 장치가 작동하지 않더라도 다른 하나의 장치가 작동할 수 있는 이중구조로 구성되어야 한다. 따라서 차상 ATC 시스템은 동작 상태(Operating) ATC와 예비 상태(Hot Standby) ATC 시스템으로 이중계 설계되어 있다. 즉 완벽히 독립적으로 기능을 수행할 수 있는 두개의 차상 ATC 시스템이 선두차 운전실(Head car cab)과 후미차 운전실(Rear car cab)에 각각 설치되어 있어, 동작 상태(Operating)의 ATC에 이상 발생시 예비상태(Hot Standby)의 ATC가 요구되는 기능을 수행 할 수 있도록 설계 되어 있다. 뿐만 아니라 ATC 안테나, 속도 센서(Tachometer), 감속 체결 확인 장치 및 열차와 인터페이스 되는 출력 릴레이를 제외하고는 차상 ATC 시스템은 완벽하게 이중계로 설계되어 있다. 속도 센서(Tachometer)의 경우 차축에 1개의 속도센서(Tachometer)가 설치되기는 하지만, 각 ATC에 대해 전기적으로 분리된 채널 입력을 별도로 공급하도록 설계 되어 있다.

(2) Fail-safe 설계

차상 ATC 시스템은 시스템을 구성하고 있는 부품의 고장이 발생하더라도 운영상의 위험을 야기하지 않도록 Fail-Safe 개념을 적용하여 설계 되었다. 특히 비상제동 체결 명령을 차량으로 전달하는 Vital Output board의 경우, Vital 로직을 적용하여, 출력이 없을 경우에는 비상제동을 체결하도록 설계되어 있다.

(3) 신뢰성 설계

차상 ATC 시스템의 설계에는 하드웨어, 소프트웨어적으로 기 적용되어 신뢰성이 검증된 설계 기준을 반영하여 설계한다.

(4) 유지보수성 설계

검수원으로 하여금 유지보수가 용이하도록 하드웨어, 소프트웨어를 설계 한다.

(5) 호환성

기존 시스템과 전기적, 기계적으로 호환성을 유지하여야 한다.

(6) 소형화

최신 기술을 적용하여 장치의 크기를 소형화 한다.

(7) 소프트웨어 품질 관리

차상 ATC 시스템을 개발함에 있어 ㈜로템은 CMMI(Capability Maturity Model Integration) Level 2 프로세스에 따라 소프트웨어 품질관리를 수행하였으며, CMMI 공인심사원으로부터 CMMI Level 2를 인증받았다.

CMMI는 미국 카네기 멜론 대학의 소프트웨어 공학 연구소(SEI)가 개발한 소프트웨어와 시스템 엔지니어링을 위한 통합 프로세스 모델로, 우수 소프트웨어와 시스템 개발 업체를 객관적 기준으로 선정하

기 위해 개발되었으며, 주로 조직의 생산성과 품질향상을 위해 제시되는 모델로 활용되는 등 현재 국제 공인 평가지표로 사용되고 있다.

CMMI Level2 프로세스는 다음과 같이 7개 프로세스 영역에 대한 125개 실행 관행(Practice)이 있다.

- Requirement Management(REQM) : 요구사항 관리 및 양방향 추적 관리
- Project Planning (PP) : 프로젝트의 성공적 수행을 위해 개발활동과 프로젝트를 관리하기 위한 합리적인 계획 수립 활동
- Project Monitoring and Control (PMC) : 프로젝트의 진행 상태를 파악하고 계획 대비 실적의 차이가 현저히 나타날 때 이에 대한 적절한 시정조치 활동 수행
- Supplier Agreement Management (SAM) : 자격있는 협력업체 선정, 문서화된 합의, 협력업체를 효과적으로 관리하여 성공적인 공급자 관리 수행
- Measurement and Analysis (M&A) : 측정목표대비 측정지표를 설정하고 수집/분석하여 프로젝트의 건실성 확보
- Process and Product Quality Assurance (PPQA) : 프로젝트에 독립된 조직에 의해 품질보증 계획수립, 품질점검, 품질평가 등 프로젝트 품질보증 활동 수행
- Configuration Management (CM) : 프로젝트 수명주기 전 과정을 거치면서 변경 및 승인과 관련된 여러 활동을 체계적이고 일관성 있게 관리하고 통제함으로써, 프로젝트 산출물의 무결성 확보

Carnegie Mellon
Software Engineering Institute

CMMI

CERTIFICATE OF ACCOMPLISHMENT

This is to certify that

Rotem Company, R&D Center
Electric Equipment Development for
Rolling Stock / Signaling System &
System Development for Defense System

has successfully achieved

CMMI Maturity Level 2
May 28, 2007

This Class A appraisal was conducted in accordance with Standard CMMI℠ Appraisal Method for Process Improvement (SCAMPI℠), Version1.1: Method Definition Document using the Capability Maturity Model Integration (CMMI) SE/SW v1.1 Staged Representation.

SCAMPI Lead Appraiser, JoonKi Paek

May 28, 2007

®CMMI is registered in the U.S. Patent and Trademark Office.

그림1. CMMI 인증서

2.2 안전관리(Safety Management)

차상 ATC 시스템의 안전성을 보증하기 위해 차상 ATC 시스템의 개발에 적용한 안전관리절차에 대해 기술한다.

(1) 안전성 관리 목표 (Safety Target)

차상 ATC 시스템을 개발함에 있어 안전성 관리의 목표는 ATC 시스템의 전 수명주기 동안 차상 ATC 시스템과 관련된 모든 위험요인을 식별하고 위험도를 분석하여, 그 위험도가 ALARP원칙에 따라 잔존 위험도가 ALARP의 허용 가능한 범위로 저감되었음을 입증하는데 있다.

이를 위해 식별된 모든 위험 요인이 어떻게 관리 되었는지를 기록하는 "차상 ATC 시스템 위험 기록서(Hazard Log)"를 사용하였으며, 위험 기록서를 보완하기 위해 정량적 위험도 분석 기법인 "차상 ATC 시스템 고장 유형, 결과 및 치명도 분석(FMECA)" 및 "차상 ATC 시스템 고장나무 분석(FTA)" 이 사용되었다.

다시 말해, 차상 ATC 시스템 개발 프로젝트의 안전성 관리의 목표는 차상 ATC 시스템에 잠재되어 있는 모든 위험요인을 식별하고 위험 기록서(Hazard Log)에 기록하여 각각의 위험도를 모두 수용 가능한 영역(Ud, Ar) 또는 명확한 수용 영역(Ac)로 저감 시키는데 있다고 할 수 있다. 위험요인의 심각도 및 발생빈도 분류와 ALARP 원칙에 따른 위험도 분류표는 아래 표를 참조한다.

표 1. 위험요인의 심각도 분류(유럽규격 EN50126의 Table3적용)

심각도	승객 또는 환경에 미치는 영향	서비스운행에 미치는 영향
치명적인 위험 (Catastrophic) 4	인명의 사망, 시스템의 손실 또는 심각한 환경상의 피해를 유발하는 위험	서비스 불가
중대한 위험 (Critical) 3	심각한 인명의 상해, 직업상의 질병 및 중요한 시스템 또는 환경상의 피해를 초래하는 위험	주요 시스템의 기능 상실
중요하지 않은 위험 (Marginal) 2	최소한의 상해, 직업상의 질병 및 최소한 시스템 또는 환경상의 피해를 초래하는 위험	심각한 시스템 피해
사소한 위험 (Negligible) 1	최소한의 상해, 직업상의 질병 보다 작고, 최소한의 시스템 및 환경상의 피해보다 작은 영향을 초래하는 위험	사소한 시스템 피해

표 2. 위험요인 발생빈도 분류(유럽규격 EN50126의 Table2 적용)

발생빈도	설 명	위험상태의 빈도
빈번한 발생 (Frequent) A	수명주기 동안 빈번하게 발생할 가능성이 있음	위험상태가 항상 지속
가능성 있는 (Probable) B	수명주기 동안 여러 번 발생할 가능성이 있음	위험상태가 빈번히 발생
종종 발생 (Occasional) C	수명주기 동안 가끔 발생할 가능성이 있음	위험상태가 가끔 발생
발생가능성이 미약 (Remote) D	수명주기 동안 한두 차례 발생할 가능성이 있음	일반조건에서 위험상태가 발생할 수 있음을 대할 수 있음
발생가능성이 없음 (Improbable) E	수명주기 동안 발생할 가능성은 있지만, 발생하지 않음	위험상태가 예외적으로 발생할 것임을 가정할 수 있음
발생가능성이 거의 희박 (Incredible) F	발생가능성도 희박하며, 절대 발생하지 않음	위험상태가 일어나지 않을 것으로 가정할 수 있음

표 3. 위험도 분류표(Risk Matrix)(유럽규격 EN50126의 Table6적용)

설명	치명적인 위험 (Catastrophic) 4	중대한 위험 (Critical) 3	중요치 않은 위험 (Marginal) 2	사소한 위험 (Negligible) 1
빈번한 발생 (Frequent) A	Un	Un	Un	Ud
가능성 있는 (Probable) B	Un	Un	Ud	Ar
종종 발생 (Occasional) C	Un	Ud	Ud	Ar
발생가능성이 미약 (Remote) D	Ud	Ud	Ar	Ac
발생가능성이 없음 (Improbable) E	Ar	Ar	Ac	Ac
발생가능성이 거의 희박 (Incredible) F	Ac	Ac	Ac	Ac

여기서 Un : Unacceptable 반드시 저감되어야 함

Ud : Undesirable 위험도 감소가 현실적으로 불가능하고 운영기관이 적절하게 동의를 할 때는 이를 수용함

Ar : Acceptable with technical Review 적절한 통제 및 운영기관의 동의로 수용할 수 있음

Ac : 조건 없이 수용가능 함

2.3 시스템 수명 주기 및 안전성 관리 활동 (Lifecycle and Safety Tasks)

ATC 시스템의 안전성은 EN 50126 및 국제전기협회 규격 IEC 62278의 5.2항에서 규정하고 있는 시스템 수명 주기(System Life Cycle)에 따라 관리되었으며, 향후에도 아래의 시스템 수명주기에 따라 관리 될 것이다.

앞에서도 설명한 바와 같이 본 "차상 ATC 시스템 설계종합안전대책기술서"는 전체 시스템 수명주기의 왼쪽에 기술되어 있는 개념단계에서 설계 및 수행단계까지의 안전성 관리 활동에 대해 설명하며 , 전체 시스템 수명주기는 다음과 같다.

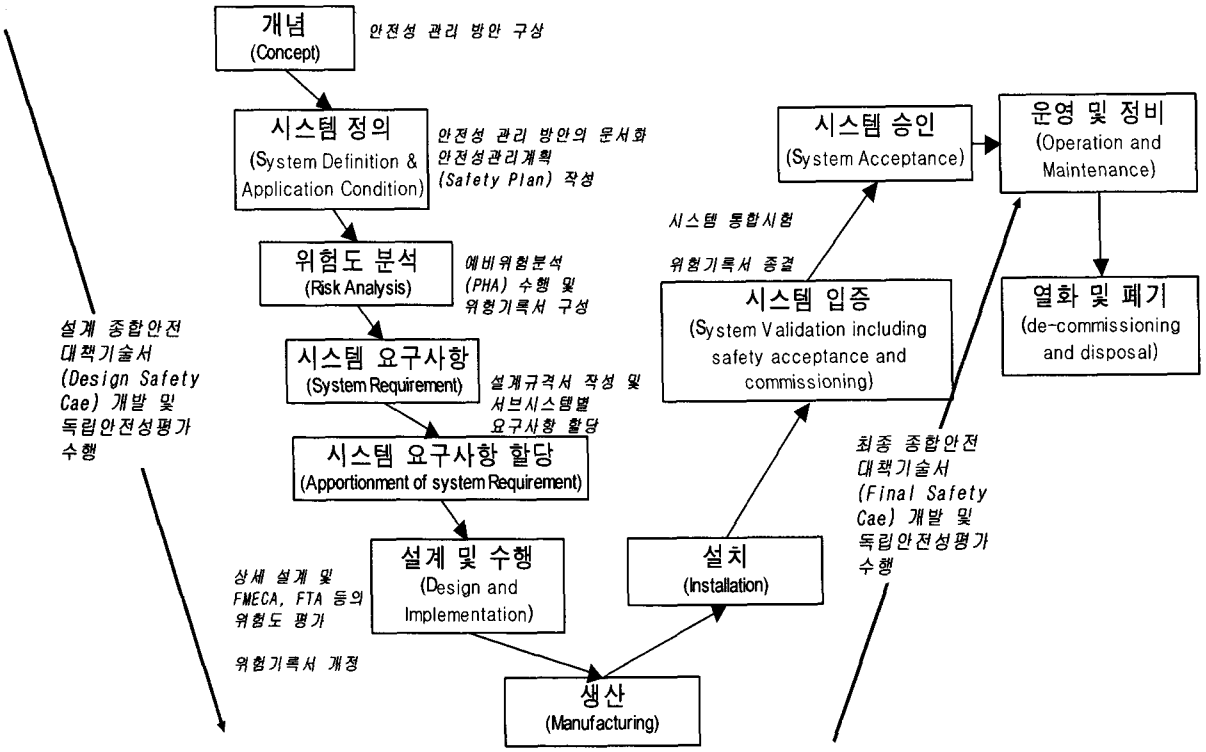

그림2. 시스템 수명주기(IEC62278 Fig.10참조)

위의 그림에서 설명된 바와 같이 개념(Concept) 단계에서는 안전성 관리 방안을 구상하였으며, 시스템 정의(System Definition and Application Condition) 단계에서는 개념 단계에서 구상한 안전성 관리 방안을 "차상 ATC 시스템 안전성 관리 계획" 으로 문서화 하였으며, 위험도 분석(Risk Analysis)단계에서는 예비 위험 분석 기법을 적용하여 "차상 ATC 시스템 예비 위험 분석(PHA)" 을 작성하였으며, 이를 바탕으로 위험 기록서(Hazard Log)를 작성하였다. 또한 시스템 요구사항(System Requirement) 및 시스템 요구사항 할당(Apportionment of System Requirement) 단계에서는 예비 위험 분석에서 작성된 예비 위험 목록을 통해 식별된 위험 저감책으로서의 설계 요구사항을 식별하여, 각 서브시스템 설계 규격서에 반영하였으며, 설계 및 수행(Design and Implementation) 단계에서는 정량적 위험도 분석 기법인 차상 ATC 시스템 고장 유형, 결과 및 치명도 분석(FMECA)" 및 "차상 ATC 시스템 고장나무 분석(FTA)" 을 사용하여 차상 ATC 시스템으로 인해 발생 할 수 있는 치명적인 위험 요인에 대한 발생 빈도를 정량적으로 평가하였으며 그 결과를 반영하여 "차상 ATC 시스템 위험 기록서(Hazard Log)" 를 개정하였다.

2.4안전성 관련 결과물 (Safety Related Deliverable)

위에서 설명한 차상 ATC 시스템의 전체 수명주기 중 설계단계까지 아래와 같은 안전성 관련 결과물이 작성되었으며, "차상 ATC 시스템 최종 종합안전대책기술서(Final Safety Case)" 는 시스템 입증단계에서의 시험을 통해 시스템의 안전성이 최종적으로 입증되면 작성될 것이다.

표 4. 안전성 관련 결과물 목록

차상 ATC 시스템 안전성 관리 계획서
차상 ATC 시스템 예비위험분석보고서
차상 ATC 시스템 위험 기록서(Hazard Log)
차상 ATC 시스템 고장 유형, 결과 및 치명도 분석(FMECA)
차상 ATC 시스템 고장 나무 분석(FTA)
차상 ATC 시스템 설계 종합안전대책기술서(Design Safety Case)
차상 ATC 시스템 최종 종합안전대책기술서(Final Safety Case)

2.5 안전성 분석 및 평가 절차 (Safety Analysis and Assessment)

(1)위험요인 식별 (Hazard Identification)

안전성 분석 및 평가 절차의 첫번째 단계인 위험요인 식별 단계에서는 예비위험분석(PHA, Preliminary Hazard Analysis)기법을 활용하여, 차상 ATC 시스템 설계 초기 단계에서 해당 시스템이 가지고 있을지도 모르는 잠재적 위험요인을 식별하였다. 이러한 활동은 차상 ATC 시스템 전문가들의 Brain storming 또는 유사 시스템의 과거 기록 등을 참고하여 이루어졌으며, 예비위험분석을 통해 식별된 위험요인 들은 예비위험목록(PHL, Preliminary Hazard List)에 기록되었으며, 위험도 평가의 입력자료로 활용되었다.

(2) 위험도 평가 (Risk Assessment)

위험도 평가 단계에서는 위험요인 식별 단계에서 예비위험분석을 통해 식별된 예비위험목록을 가지고 위험요인의 상세 분석을 수행하는 단계이다. 특히 이 단계에서는 위험요인이 가지고 있는 잠재적인 위험도(Risk)를 위험요인의 발생빈도(Frequency, Probability)와 위험요인이 야기할 수 있는 결과의 위험도(Severity)를 가지고 평가하였다.

위험도 평가는 크게 정성적 위험도 평가와 정량적 위험도 평가로 나눌 수 있으며, 각각의 내용은 다음과 같다.

정성적 위험도 평가 (Qualitative Risk Assessment)

정성적 위험도 평가는 상세 위험분석의 한 절차로, 예비위험목록에 기초한 상세 위험요인 식별 이후, 각각의 상세 위험요인의 발생빈도(Frequency, Probability)와 심각도(Severity)를 발생빈도 및 심각도 분류에 따라 정성적으로 평가한 후, 이 둘을 조합하여 각 상세 위험요인의 위험도를 평가하는 활동을 의미한다.

여기서 상세 위험요인을 식별할 때에는 차상 ATC 시스템 및 하위 부품의 고장이나 동작 이상(서브시스템위험분석, Sub-system hazard analysis(SSHA))뿐 아니라 지상신호장치, 차량 시스템 등과 같은 주변 시스템과의 인터페이스(인터페이스위험분석, Interface hazard analysis(IHA))와 운행 또는 시스템 정비에 발생할 수 있는 위험상황(운영 및 지원위험분석, Operating & supporting hazard analysis(O&SHA))까지도 고려하였다.

위의 위험요인 심각도 분류 및 발생빈도 분류표에서도 알 수 있듯이, 정성적 위험도 평가는 각 위험요인의 심각도와 발생빈도를 분류하여 위험도를 평가한다. 이러한 정성적 위험도 평가 방법은 위험도에 기초한 위험분석에서 각 위험요인의 위험도를 개략적으로 평가하기 위한 대표적인 위험도 분석법으로, 각 위험요인의 상대적인 위험도 순위를 알 수 있게 해 준다. 또한 이를 통해 각 위험요인의 위험도가 허용 가능한 수준(ALARP)인지, 아니면 추가적인 위험 저감책이 필요한지를 판단할 수 있게 해준다. 뿐만 아니라 이러한 정성적 위험도 평가는 추가적인 정량적 위험도 평가가 필요한지 아닌지를 알 수 있게 해 준다.

정성적 위험도 평가 결과는 모두 위험 기록서(Hazard Log)에 기록되었으며, 전 수명주기동안 계속적으로 개정되어 유지될 것이다.

정량적 위험도 분석(Quantitative Risk Assessment)

정량적 위험 분석은 앞서 설명한 정성적 위험 분석의 보조 수단으로, 정성적 위험 분석의 결과, 안전에 차명적인 영향을 미칠 수 있는 위험요인(Safety Critical Hazard)의 위험도를 정량적으로 평가하여 그 위험 요인의 위험도가 허용 가능한 범위(ALARP)로 관리되었는지를 판단할 수 있게 해준다.

이번 차상 ATC 시스템 개발 프로젝트에서는 정성적 위험도 평가 결과에 따라 고장 유형, 결과 및 치명도 분석(FMECA)와 고장 나무 분석(FTA)의 정량적 위험도 평가를 수행하였다. 특히 고장나무분석(FTA)의 경우 ㈜로템에서 개발하는 차상 ATC 시스템 운용시 발생할 수 있는 치명적인 위험요인

(Critical Hazard)인 차량 충돌 및 출입문 동작오류로 인한 승객 추락에 대해 수행되었다.

(3) 위험요인 위험도 관리 (Hazard Risk Control)

각 위험요인은 위험도 평가 단계를 통해 잠재되어 있는 초기 위험도(Initial Risk)가 평가되었다. 이 위험도 평가 결과에 따라 각 위험요인이 허용 가능한(ALARP) 위험요인인지, 아니면 추가적인 위험 저감책의 적용이 필요한 위험요인인지가 결정되었다. 추가적인 위험 저감책이 필요한 경우, 해당 저감책을 식별/적용하고 그에 따른 저감된 잔존 위험도를 초기 위험도와 동일한 방법으로 평가하여 위험 기록서(Hazard Log)에 기록하였다. 이러한 과정은 안전성 목표인 ALAPR 원칙에 따라 식별된 모든 위험요인의 잔존 위험도가 허용 가능한 수준으로 저감될 때까지 반복되었다.

(4) 검증 및 타당성 검사 (Verification and Validation)

모든 안전성 관리 활동과 그에 따른 결과물인 각종 위험분석 자료들은 안전성 관리자(Safety Manager)에 의해 검증(verification)되고, 타당성이 검사(Validation)되었다.

이를 위해 안전성 관리자(Safety Manager), 안전성 전문가(Safety Specialist), 설계/개발총괄(PE, Project Engineer), 설계 관리자(Design Manager), 설계 담당자(Design Engineer)로 구성된 안전보증기능그룹(Safety Cross Functional Working Group)이 안전성 관리자(Safety Manager)에 의해 구성되었으며, 안전보증기능그룹은 주기적인 회의를 통해 "차상 ATC 시스템 안전성 관리 계획서" 에 따른 안전성 관리 활동이 이루어지고 있는지 검증(Verification)하고, 안전성 분석활동이 적절히 이루어 졌는지 타당성 검사(Validation)를 수행하였다.

이때, 기초자료로 활용된 것이 위험 기록서(Hazard Log)이다. 위험요인 식별, 위험도 평가, 위험도 저감책의 적용 등, 식별된 모든 위험요인에 대한 위험분석 결과는 모두 위험 기록서(Hazard Log)에 기록되며, 또한 이 위험 기록서(Hazard Log)는 차상 ATC 시스템의 전 수명주기동안 유지될 것이며, 식별된 각종 위험요인에 대한 저감책들이 어떻게 반영되었는지를 입증하는 자료로 활용된다.

(5) 안전성 감사 및 안전성 평가 (Safety Audit and Safety Assessment)

차상 ATC 시스템의 전 수명주기 동안 수행하는 안전성 관리 활동 및 안전성 분석 결과는 모두 종합안전대책기술서(Safety Case)에 정리되어 기술될 것이며, 종합안전대책기술서(Safety Case)를 바탕으로 독립 안전성 평가기관에 의해 안전성 감사 및 안전성 평가가 수행될 것이다.

종합안전대책기술서는 시스템 수명주기에 따라 설계 및 수행(Design and Implementation) 단계까지의 활동을 통합하는 설계 종합안전대책기술서(Design Safety Case, 본 문서)와 생산 단계 이후의 활동을 통합하는 최종 종합안전대책기술서(Final Safety Case)로 분류하여 작성될 것이며, 이에 따라 안전성 감사(Safety Audit)과 안전성 평가(Safety Assessment)도 분류하여 수행될 것이다.

안전성 감사(Safety Audit)란 안전성 관리 절차가 안전성 관리 계획서에 따라 수행되었는지를 검토하는 활동으로, ㈜로템의 안전성 관리자(Safety Manager)에 의해 설계 조직의 활동이 1차로 검증(Verification)되며, 종합안전대책기술서(Safety Case)에 기록될 1차 검증(Verification) 결과를 독립 안전성 평가기관이 2차로 감사(Audit)하는 활동이다.

또한 안전성 평가(Safety Assessment)란 안전성 분석 활동이 적절히 이루어져서 식별된 모든 위험요인의 위험도가 위험도 허용 가능 기준(Risk tolerability criteria) 이하로 저감되었는지를 평가하는 활동으로 안전성 감사(Safety Audit)과 마찬가지로 ㈜로템의 안전성 관리자(Safety Manager)가 1차로 타당성을 검사(Validation)하고 종합안전대책기술서(Safety Case)에 기술될 1차 타당성 검사(Validation)결과를 독립안전성 평가기관이 2차로 평가하는 활동이다.

본 차상 ATC 시스템 개발 프로젝트의 독립 안전성 감사 및 평가 기관으로 ㈜마이크로트랙을 선정하였다.

2.6 기술 안전 보고 (Technical Safety Report)

차상 ATC 시스템 개발 프로젝트에 적용했던 안전성 관리 절차에 따라 분석된 안전성 분석 결과와 차상 ATC 시스템의 안전성이 허용 가능한 수준으로 저감되었음을 입증하는 기술적인 증빙자료에 대해 기술한다.

(1) 예비위험분석 (PHA)

설계 초기에 차상 ATC 시스템에 잠재되어 있는 일반적인 위험요인을 식별하기 위한 분석으로 차상 "차상 ATC 시스템 예비위험분석" 에 상세 내용이 포함되어 있다.

(2) 위험기록서 (Hazard Log)

예비위험분석 결과를 바탕으로 차상 ATC 시스템에서 발생할 수 있는 상세 위험요인을 식별하고 이를 정성적 평가방법에 따라 위험도를 평가한 목록표로 상세 내용은 "차상 ATC 시스템 위험 기록서 (Hazard Log)" 에 기록되어 있다. 예비 위험 분석을 바탕으로 식별된 차상 ATC 시스템과 관련된 총 20항의 위험 요인의 위험도는 모두 적절한 저감책(Safeguard)에 의해 허용 가능 수준으로 저감되었음을 알 수 있다.

(3) 고장 유형, 결과 및 치명도 분석 (FMECA)

정성적 위험도 평가인 예비 위험 분석과 위험 기록서를 보완하기 위해 정량적 위험도 평가 기법이 적용되었으며, FMECA는 대표적인 정량적 위험도 평가 기법으로 시스템을 구성하고 있는 각 구성품의 고장이 어떠한 영향을 미치는가를 분석하는 기법이다.

㈜로템은 차상 ATC 시스템의 고장 유형과 그 결과를 평가하기 위해 각 구성품의 고장이 차상 ATC 시스템의 기능에 어떠한 영향을 미치는가를 분석하는 구성품 FMECA(Part Level FMECA)와 각 기능 고장이 차상 ATC 시스템의 운영에 어떠한 영향을 미치는지를 분석하는 기능 FMECA(Functional FMECA)를 수행하였으며, 각 상세 내용은 "차상 ATC 시스템 고장 유형, 결과 및 치명도 분석(FMECA)" 에 포함되어 있다.

고장 유형, 결과 및 치명도 분석의 결과로 도출된 각 기능 고장의 발생 확률(고장율)은 위험 기록서의 발생빈도에 반영되었다.

(4) 고장나무분석 (FTA)

정량적 위험도 분석의 또 하나의 대표적인 기법인 고장 나무 분석(FTA)은 예비위험분석, 위험기록서 등 정성적 위험도 분석을 통해 식별된 안전상의 치명적인 영향을 줄 수 있는 일반 사고유형에 대해 그 발생 확률을 논리 구조를 통해 계산하는 기법으로 본 차상 ATC 시스템 개발 프로젝트에서는 아래와 같은 일반 사고유형을 최상위 사상(Top Event)로 선정하여 그 발생 확률을 분석하였다.

- 차상 ATC 시스템의 오류로 인한 열차 충돌
- 차상 ATC 시스템의 오류로 인한 승객 추락

(5) 기술적 입증 자료 (Technical Evidence)

이번 항에서는 앞서 설명 정성적/정량적인 위험도 평가 기법에 따라 식별된 각위험 요인의 위험도를 저감시키기 위한 저감책(Safeguard)이 설계에 어떻게 반영되어 있는지를 보여주는 기술적 입증 자료에 대해 설명한다.

표 5. 기술적 입증자료 (Technical Evidence)

번호	위험저감대책	예비위험 목록 참조 번호	예비위험 저감대책 참조 번호	위험기록서 참조 번호	기술적 증빙자료
1	차상 ATC 시스템의 이중계 설계	PHA_111, PHA_112, PHA_113, PHA_114, PHA_115, PHA_121, PHA_122, PHA_210, PHA_220	SG026	ATC_001, ATC_002, ATC_003, ATC_004, ATC_005, ATC_006, ATC_007, ATC_008, ATC_009, ATC_010, ATC_011, ATC_012, ATC_013, ATC_014, ATC_015, ATC_016, ATC_017, ATC_018	도면 SGP00257
2	소프트웨어 개발 관리 및 통합시험을 통해 소프트웨어 무결성 보증	PHA_111, PHA_112, PHA_113, PHA_114, PHA_115, PHA_121, PHA_122, PHA_210, PHA_220	SG027	ATC_001, ATC_002, ATC_003, ATC_004, ATC_005, ATC_006, ATC_007, ATC_008, ATC_009, ATC_010, ATC_011, ATC_012, ATC_013, ATC_014, ATC_015, ATC_016, ATC_017, ATC_018	CMMI를 적용한 소프트웨어 관리 단위기능시험 REDV100171 구성품기능시험 REDE101696
3	DSP 모듈에 속도코드 해석오류 처리 기능 부여	PHA_111	SG001	ATC_001	단위기능시험 REDV100171 구성품기능시험 REDE101696
4	AM 신호 중첩시 무코드 처리로 상용제동 체결	PHA_111	SG002	ATC_002	단위기능시험 REDV100171 구성품기능시험 REDE101696
5	CPU에서 운행중(비 test mode시) 출력 차단	PHA_111	SG003	ATC_002	단위기능시험 REDV100171 구성품기능시험 REDE101696
6	Wheel Dia.의 입력 유효범위 설정	PHA_112	SG004	ATC_003	소프트웨어기능설명서 REDE100678
7	Wheel Dia. 설정단계를 17단계로 세분화	PHA_112	SG005	ATC_003	소프트웨어기능설명서 REDE100678
8	CPU 전면 VFD를 통해 Wheel Dia.값을 표시하여 검수원 확인 유도	PHA_112	SG006	ATC_003	도면 SGP00244
9	속도 pulse 생성 이중계 설계	PHA_112	SG007	ATC_004, ATC_005	도면 SGP00257
10	두개의 속도채널의 입력을 비교하여 오류 발생시 비상제동 체결	PHA_112	SG007	ATC_004, ATC_005	소프트웨어기능설명서 REDE100678
11	주간제어기 입력으로 No motion time out고장 검지하여 비상제동 체결	PHA_112	SG008	ATC_004, ATC_005	소프트웨어기능설명서 REDE100678
12	속도 유효성 판정하여 오류 발생시 비상제동 체결	PHA_112, PHA_121	SG009	ATC_006, ATC_013, ATC_014	소프트웨어기능설명서 REDE100678
13	No welding type Relay 사용	PHA_113, PHA_115, PHA_210	SG010, SG015, SG021	ATC_007, ATC_009, ATC_016	도면 SGP00250

번호	위험저감대책	예비위험 목록 참조 번호	예비위험 저감대책 참조 번호	위험기록서 참조 번호	기술적 증빙자료
14	VI2 board를 통해 US/EB/VZ신호 feed back하여 CPU board에서 이상유무 검증하여 오류발생시 시스템 차단	PHA_113, PHA_115, PHA_210	SG011, SG017, SG022	ATC_007, ATC_008, ATC_009, ATC_010, ATC_016, ATC_017	단위기능시험 REDV100171 구성품기능시험 REDE101696
15	Vital Logic으로 비정상 출력시(출력없음) CPS Board의 PLD 파트를 통해 출력전원 차단	PHA_113, PHA_115, PHA_210	SG012, SG018, SG023	ATC_008, ATC_010, ATC_017	하드웨어상세설계 규격서 REDD100097
16	EB Relay 이중계 설계	PHA_115	SG016	ATC_009	도면 SGP00257
17	속도입력과 비교하여 이상 검지시 BA오류 검지후 비상제동 체결	PHA_114	SG013	ATC_011	소프트웨어기능설명서 REDE100678
18	매뉴얼에 주기적인 가속도계 수평 검사 표기	PHA_114	SG014	ATC_012	차상 ATC 시스템 매뉴얼
19	CPU에서 VI입력 검증하여 오류시 VI board 고장처리 및 비상제동 체결	PHA_122, PHA_220	SG019, SG024	ATC_015, ATC_018	하드웨어상세설계 규격서 REDD100097 소프트웨어기능설명서 REDE100678
20	EMC 시험을 통한 전자파 적합성 입증	PHA_131	SG020	ATC_019	전자파 시험 REDE101696
21	운전실에 차상 ATC 시스템 설치	PHA_310	SG025	ATC_020	도면 목록
22	차상 ATC 시스템에 non-halogen cable 사용	PHA_310	SG025	ATC_020	제작규격서 REDE100678

3. 결 론

상기 본문에서는 (주)로템이 차상 ATC 시스템을 개발함에 있어 적용한 '위험도 분석에 기초한 안전성 관리 활동'을 종합안전대책기술서의 내용을 바탕으로 간략히 소개 하였다.

다시한번 요약하자면, 차상 ATC 시스템의 안전성 향상을 위해 IEC 62278에따른 안전성 관리 활동을 규정하고, 이에 따른 안전성 관리 활동의 결과로 작성된 다양한 안전성 분석 결과를 토대로, EN 50129에 따라 설계 종합안전대책기술서를 작성하고 이에 대한 제3 인증기관의 평가를 완료하였다.

즉, 설계 측면에서의 안전성 활동과 종합안전대책기술서 수립을 통해 규명 가능한 모든 위험요인이 규명되었으며, 그에 따른 적절한 안전 대책을 설계상에 반영함으로써 차상 ATC 시스템의 안전성이 향상되었으며, 차상 ATC 시스템에 기대되는 안전성 수준에 적합하게 설계된 것으로 평가된다.