Journal of the Korea Academia-Industrial cooperation Society
Vol. 18, No. 11 pp. 31-45, 2017

https://doi.org/10.5762/KAIS.2017.18.11.31
ISSN 1975-4701 / eISSN 2288-4688

철도신호시스템의 안전 설계를 위한 개선된 안전성 적용 조건 도출 방법

백영구, 이재천*
아주대학교 시스템공학과

An Improved Method of Developing Safety-Related Application Conditions for Safety Design of Railway Signalling Systems

Young-Goo Baek, Jae-Chon Lee*
Dept. of Systems Engineering, Ajou University

요 약 철도 분야에서의 최근 수년간의 사고 통계에 의하면, 관련 기술 발전과 안전정보 관리시스템의 구축으로 사고발생 빈도가 현저히 줄고 있다. 그럼에도 불구하고 운영 및 유지보수에서의 오류와 안전설계에서의 결함으로 인한 사고는 지속적으로 발생하고 있다. 이에 따라 철도사고를 예방하기 위해, 철도차량 개발 시 안전성을 고려하는 설계 및 제작을 위한 지침이 작성되었고, 이와 더불어 안전 설계에 대한 독립적인 안전성평가의 수행에 대한 요구가 제시되었다. 이를 충족시키기 위해 철도시스템 개발업체는 안전성 활동 산출물인 Safety Case를 작성해야 한다. 이에 따라 Safety Case의 주요 항목 중 하나인 안전성 적용조건 (SRAC: Safety-Related Application Conditions)의 도출 및 관리에 대한 중요성이 커지고 있다. 지금까지 보고된 SRAC에 관한 연구 결과에서는 도출 절차의 간략성과 설계단계에서의 특정 안전성 활동 분석 방법에만 초점을 맞추고 있다. 이러한 방법은 SRAC 항목 들을 빠르게 도출 할 수 있는 장점이 있지만, 안전성 측면에서 고려되어야 할 중요한 항목들이 누락될 위험이 존재한다. 이러한 문제를 해결하기 위하여 본 논문에서는 시스템 수명주기 전반에 걸쳐 안전성 설계 및 안전성 평가 활동을 수행하고 이를 기반으로 SRAC의 도출방법의 개선 방안을 제안한다. 이렇게 함으로써 SRAC를 보다 체계적으로 도출 및 관리를 수행할 수 있는데, 특히 설계 초기단계에서부터 SRAC를 고려함으로써 안전성 요구사항을 최대한 반영한 안전설계가 가능하다. 또한 철도신호시스템에 대한 적용사례 연구를 통하여 본 논문에서 제시하는 방법이 시스템 수명주기 전체에 걸쳐 SRAC를 고려함으로써 중요한 안전성 관련 항목들의 누락이 줄어들 수 있음을 보여준다.

Abstract According to the railway accident statistics in recent years, the frequency of accidents has been significantly reduced, due to the advance of related technologies and the establishment of safety information management systems. Nonetheless, accidents due to errors in the operation and maintenance phase and faults in safety design continue to occur. Therefore, to prevent accidents, guidelines for the safety design and manufacture of railway vehicles were established, and a request for the independent safety evaluation of safety designs was made. To respond to this, rail system developers must prepare safety cases as a safety activity product. One of the main items of these safety cases is the safety-related application conditions (SRAC) and, thus, the question of how to develop these SRAC is an important one. The SRAC studies reported so far focused only on the simplicity of the derivation procedure and the specific safety activities in the design phase. This method seems to have the advantage of quickly deriving SRAC items. However, there is a risk that some important safety-related items may be missing. As such, this paper proposes an improved method of developing the SRAC based on the idea of performing both the safety design and safety evaluation activities throughout the whole system lifecycle. In this way, it is possible to develop and manage the SRAC more systematically. Especially, considering the SRAC from the initial stage of the design can allow the safety requirements to be reflected to a greater extent. Also, an application case study on railway signaling systems shows that the method presented herein can prevent the omission of important safety-related items, due to the consideration of the SRAC throughout the system lifecycle..

Keywords : Railway Signalling System, Systems Safety, Safety Case, Safety-Related Application Conditions, IEC 62425, System Lifecycle Approach

본 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2015R1D1A1A01056730)
*Corresponding Author : Jae-Chon Lee(Ajou Univ.)
Tel: +82-31-219-3941 email: jaelee@ajou.ac.kr
Received September 25, 2017 Revised October 11, 2017
Accepted November 3, 2017 Published November 30, 2017

1. 서론

철도분야에서의 기술의 발전 및 철도안전정보관리시스템등의 구축으로 사고데이터 수집 및 관리가 이뤄짐으로써 사고의 발생빈도가 이전보다 현저히 줄고 있다. 그러나 최근 수년간의 철도사고 통계데이터에 근거할 때 철도운영직원의 운영 및 유지보수에서의 오류, 그리고 안전 측면에서 중요한 기능을 수행하는 안전 중시 시스템[1]의 기능 불능으로 인한 철도사고는 지속적으로 발생하고 있다. 또한 이러한 철도사고들은 열차의 충돌 및 탈선 등으로 인하여 인명 및 재산상의 큰 피해를 초래한다[2, 3].

이러한 철도사고를 예방하고 철도시스템의 안전성을 확보하기 위한 방안으로 철도차량 개발 시 안전성을 고려한 설계 및 제작에 관한 운영지침 등이 개발되었다[4]. 이와 더불어, 열차속도제어 및 진로제어 등을 포함한 안전한 열차운행을 보증하는 중요한 신호시스템인 열차제어시스템(Train Control System)과 열차위치검지와 관련한 트랜스폰더(Transponder) 등 안전 기능을 수행하는 시스템에 대한 독립안전성평가(Independent Safety Assessment)가 필수적인 활동으로 요구되고 있다[5, 6]. 이에 따라서 철도시스템 및 구성품 공급업체는 개발 장치의 안전성이 철도 안전성 표준 규격인 IEC 62425의 요구사항에 부합하는지 입증해야 한다. 이를 위해 철도시스템 및 구성품 공급업체는 안전성 활동 산출물(Safety Artefact)인 Safety Case 작성이 요구되고 있다[7].

Safety Case는 철도시스템 공급업체에서 작성하는 안전성 보증 근거 문서 중 하나로서, 이후 상위 수준의 시스템에서 해당 장치를 적용하고자 할 때 고려되어야 할 안전성 적용 조건(SRAC: Safety-Related Application Conditions)을 포함하여 작성할 것을 요구하고 있다[7]. 그러나 SRAC를 도출하기 위한 접근방법은 주로 설계단계에서 수행하는 안전성 분석(Safety Analysis)을 통해서만 도출되는 것으로 다루어져 왔다. 이와 같이 설계단계에서의 안전성 활동만 고려될 경우, 설계이전단계에서 SRAC를 어떻게 관리할 지, 안전성 분석을 위한 입력문서는 누락된 사항이 없는지, 최종 Safety Case에서 다루어져야 할 안전성 분석을 위한 입력문서가 적절한지 등이 간과될 수 있다. 따라서, SRAC 도출을 위해 접근하는 방식의 개선이 필요한 실정이다[8].

철도안전성 관련 규격인 IEC 62278과 IEC 62425는 설계단계와 시스템 양도이전 단계인 시스템 확인(System Validation) 단계에서 SRAC를 포함한 Safety Case를 제출하도록 기술하고 있다[7, 9]. 또한 IEC 62425에서는 공급업체가 개발하는 제품이 상위 수준의 시스템에 적용될 때 상위 시스템 수준의 사용자가 고려해야 하는 요구사항을 포함하여 SRAC 작성 시 포함해야 하는 항목들을 기술하고 있다[7].

이와 같이 표준에서 안전성 확보를 위한 중요항목으로 제시하고 있는 SRAC의 도출에 관한 연구가 수행되고 있다. John등 [10]은 SRAC를 포함한 Safety Case와 관련해서 자동차 분야 안전성 규격인 ISO 26262에 근거한 안전성 평가 측면에서의 SRAC 및 Safety Case의 역할에 대한 연구를 수행하였다. Westman등 [11]은 ISO 26262에 부합하는 안전성 요구사항을 구조화 하였다. 또한 IEC 62425의 상위 규격인 IEC 61508에 따른 수명주기 관점에서의 RAMS 활동과 엔지니어링 활동과의 통합적인 접근 및 제품의 안전성 확보를 위한 안전성 활동 수행 시 준수해야 할 기본적인 원칙 및 적용사례를 제시하였다[12].

상기에서 제시한 주요 선행연구에 의거할 때, 시스템의 안전성 확보를 위해서는 수명주기 관점에서 안전성 활동의 수행이 주요한 전제조건이다. 이를 기반으로 초기 요구사항 분석단계에서부터 명확한 요구사항을 도출 및 관리하고, 설계단계에서의 안전성 분석을 통한 요구사항의 검증(Verification)이 수행된다. 이후 최종 단계에서의 확인(Validation)활동 결과를 Safety Case에 명확하게 기술하는 안전성 활동을 수행해야 한다.

하지만 기존의 SRAC의 도출 방법은 일부 설계단계에서의 활동만을 주요하게 다루고 있다. 이로 인하여 SRAC 도출 활동을 수행할 때, SRAC 요소가 간과되거나 누락될 수 있는 가능성이 존재한다. 이를 개선하기 위해 본 논문에서는 시스템 엔지니어링과 철도시스템 개발 프로젝트 수명주기를 분석하고, 이를 통해 도출된 프로젝트 개발 수명주기 관점에서의 SRAC 도출을 위한 방법을 안전성 활동과 안전성 평가 관점에서 제안하였다. 또한 이를 통해 개선된 SRAC 항목이 안전한 시스템 설계에 기여함을 확인하였다.

본 논문의 구성은 다음과 같다. 본 서론에 이어 2장에서는 안전성 확보를 위한 SRAC의 중요성을 설명하고 선행연구분석을 통한 기존 SRAC 도출방법의 개선점을

분석하여 연구목표 및 연구개념도를 수립하였다. 3장에서는 시스템 수명주기 관점에서의 SRAC 도출방법을 안전성 활동 및 평가 측면에서 제안하고, 4장에서는 제안된 방법에 따른 개선된 SRAC를 도출하였으며, 5장에서는 사례분석을 통해 개선된 방법으로 도출된 SRAC가 철도신호시스템의 설계 안전성에 어떻게 기여 하는지를 검증하였다. 마지막으로 6장에서는 본 연구의 결과와 제안한 논제의 타당성 및 유용성에 대해서 정리 및 요약하였다.

2. 문제의 정의

2.1 안전성확보를 위한 SRAC의 중요성

SRAC에 대해서 IEC 62425 [7], Friedemann [8], 및 Nordland [13]는 Fig. 1과 같이 정의하였다. 대상 시스템이 시스템과 서브시스템 및 구성요소로 분류되었을 때, 특정 구성요소를 상위 수준, 더불어 사용자 수준에서 적용하고자 할 때, 안전성 측면에서 상위 수준에서 이행되어야 할 조건이라 정의하였다. 즉, 주변 구성요소 및 서브시스템과의 발생 가능한 인터페이스 관련 제약사항 등을 포함한 안전성 요구사항으로 SRAC를 정의하고 있다.

Fig. 1에 근거로, 예를 들면, 구성요소가 열차속도를 연산하는 CPU모듈이라고 할 때, 해당 모듈의 적용조건이 부적절하게 고려됨으로 인해 해당 모듈이 잘못된 연산을 수행하게 된다면 결과적으로 충돌 또는 탈선과 같은 열차운행의 치명적인 결과를 초래한다. 즉, 해당 모듈이 상위 서브시스템 및 시스템 수준에서 적용 된다고 할 때, 서브시스템 및 시스템 수준에서는 해당 구성요소 수준에서의 CPU모듈 입력전압 조건 및 다른 인접한 구성요소 즉, 입/출력 모듈과의 통신 프로토콜 등을 고려하여 적용해야 한다. 만약 이러한 조건들이 고려되지 않은 상태에서 다른 입력전압을 인가하거나 프로토콜이 일치하지 않는다면, 구성요소의 기능 불능으로 인해 안전에 치명적인 영향을 초래할 수 있다.

또한, 도출된 SRAC가 상위 수준에 제공되는 과정에서 각 시스템 수준 간 의사전달의 오류 또는 SRAC의 잘못된 해석과 해당 시스템 분류 수준을 포함한 최종 사용자 수준에서의 이해부족 등으로 인해 SRAC가 부적절하게 이행되거나, 이행되지 않음으로 인해 안전성에 영향을 초래할 수 있다. 일예로 작년 구의역에서 발생한 승강장스크린도어(PSD) 유지보수자의 인명사고가 운영 및 유지보수 측면에서 준수해야 할 SRAC(즉, 운영 및 유지보수 지침)를 운영기관이 무시함으로써 발생한 대표적인 사례라고 할 수 있다[14].

이와 같이 각 시스템 분류 수준 별로 상위 수준에서 고려해야 할 요구사항에 대해서는 SRAC 형태로 Safety Case에 포함하여 기술할 것을 IEC 62425에서는 요구하고 있다[7]. Fig. 2는 신호시스템 중 열차속도 및 열차운행방향의 진로를 제어하는 장치인 연동장치(Interlocking System)에 대해서 Fig. 1의 시스템 분류에 따른 각 시스템 분류 수준 별 Safety Case 및 SRAC와의 관계성을 도식화 한 것이다. 즉, 각 구성요소는 해당 수준에서의 Safety Case가 작성되며, 해당 Safety Case는 상위 수준에서 고려되어야 하는 안전성 요구사항 즉, SRAC를 포함한다.

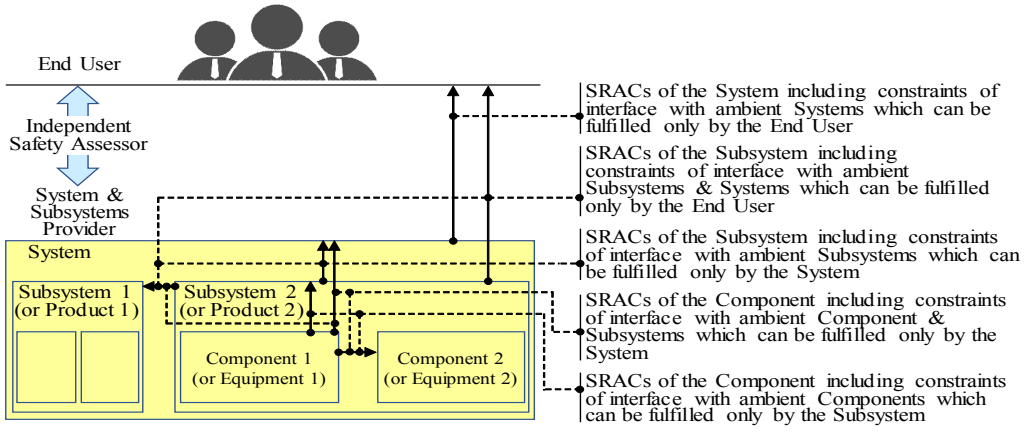

Fig. 1. SRAC Levels Identified for further Fulfillment

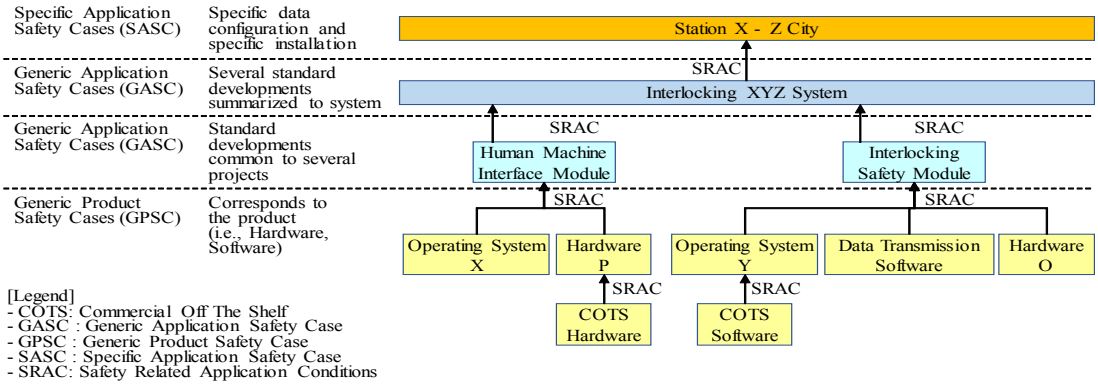

Fig. 2. Overall Safety Case(s) Structure including SRAC [15]

상기에서 기술한 바와 같이, 각 시스템 분류 수준에서의 제약사항 및 상위 수준에서 이행되어야 할 요구사항을 SRAC로 도출하여 상위 수준으로 이관한다. 이후 상위 수준으로 이관된 SRAC는 해당 수준에서의 시스템에 구현되고, 구현된 결과를 검증(Verification) 및 확인(Validation) 함으로써 시스템의 안전성을 확보한다. 또한 해당 수준에서 요구사항의 구현이 불가하거나 상위 수준에서 검증이 요구되는 SRAC 및 안전성 분석을 통해 신규로 도출된 SRAC에 대해서도 그 다음 상위 수준으로 이관되어야 한다. 결과적으로 최종 사용자 수준으로 이관된 SRAC에 대해서는 최종 사용자가 이행 가능한 방안을 수립하여 해당 시스템의 안전한 설계에 기반을 둔 운영측면에서의 안전성이 확보되도록 해야 한다. 다음 Fig. 3은 상기에서 설명한 SRAC 이관 및 관리에 대한 흐름을 도식화 한 것이다.

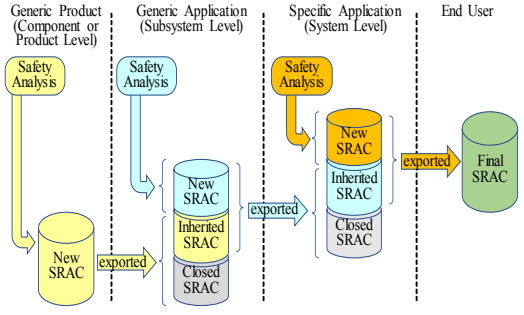

Fig. 3. Exported Constraints and SRAC Management [15]

2.2 기존 SRAC 도출방법 개선의 필요성

IEC 62425 [7]는 SRAC 도출을 위한 구체적인 방법 및 절차를 다루고 있지 않다. 다만, 도출된 SRAC가 Safety Case를 통해서 관리되어야 하며, 다음 항목들이 SRAC 기술시 고려되어야 함을 기술하고 있다[15].

- 현재 적용수준에 따른 구성요소(하드웨어 및 소프트웨어)의 형상정보
- 제작, 설치, 시험 및 시운전을 위한 제한사항(Limitations), 시스템 제약조건(Constraints) 및 가정 사항
- 운영절차에 대한 요구사항
- 유지보수를 위한 규정 및 방법에 대한 요구사항
- 알람 및 표시판 등의 사전경고 조치를 위한 안전 요구사항
- EMC 관련 사전조치에 대한 요구사항
- 유지보수를 수행함에 있어서 각종 툴 및 검·교정 장치의 안전 요구사항
- 시스템의 내구연한의 완료에 따른 해체 및 폐기시 고려되어야 할 요구사항

CLC/TR EN 50506-2 [15]에서는 Fig. 2와 Fig. 3에서 기술한 바와 같이, 시스템 분류수준 별 안전성 분석(Safety Analysis)을 수행하여 SRAC를 도출할 것을 제시하고 있다. 추가로 이 보고서는 IEC 62425에 근거하여 안전성 활동을 수행 시 내부 또는 외부 안전성 평가자가 시스템 수명주기 단계 중 초기단계인 시스템 요구사항 분석 및 설계단계에서 수행되어야 할 내용에 대해서는 별도 언급이 없이 설치단계에서만 도출된 SRAC를 평가하도록 기술하고 있다.

Friedemann [8]등은 SRAC를 도출함으로써 가져오는 이점과 실제 도출하면서 현실적으로 겪게 되는 어려움을

토대로, SRAC를 도출할 때 고려해야 하는 항목들을 제시하였다. 또한, 도출된 SRAC가 적절하고 타당한지를 평가하기 위한 평가기준(Quality Criterion)을 제시하고 있다. 하지만, SRAC를 도출하기 위한 방법에 대해서는 위험원(Hazard) 식별에 따른 Hazard Log와 SRAC 관계성을 다루고 있으나, SRAC가 Hazard Log와 어떠한 상관관계를 갖는지, SRAC가 어떻게 관리가 되는지는 다루고 있지 않다.

상기 선행연구사례에 의거할 때, SRAC가 안전성 측면에서 중요한 요구사항으로 다루어지고 있으며, 도출을 위한 간략한 절차와 주요 활동에 대해서 언급하였다. 하지만 구체적으로 시스템 개발 또는 구축하는 과정에서 시스템의 안전설계를 위한 방안으로는 미흡한 것으로 판단된다. 즉, 안전성 분석을 수행하도록 언급은 되어있으나, 시스템 수준에 따라서 어떠한 안전성 분석기법을 적용해야 하는지, 중요하게 다루어져야 할 설계 이전 단계에서의 활동이 무엇인지에 대한 기술이 누락되었다. 이로 인하여 SRAC 항목들이 간과 될 수 있다. 예를 들어, Specific Application (SA) 수준의 시스템을 개발한다고 가정한다면, 기존의 절차 및 방법으로는 다음과 같은 항목들이 누락될 수 있다.

- Generic Application (GA) 수준에서 안전성 활동 및 평가를 수행한 장치의 경우, 이미 관련문서(예: Safety Case 또는 안전성 평가 보고서 등)에 초기 SA수준에서 시스템 설계 시 고려되어야 할 안전성 요구사항이 간과 됨.
- 설계이전의 계획단계에서의 SRAC가 고려되지 않아 단편적인 분석활동에 근거한 SRAC만 다룸.
- SRAC가 도출 시 예상 가능한 유형을 사전에 고려하지 못함으로써 간과할 수 있는 항목이 존재함.

2.3 연구목표 및 범위

기존 선행연구 분석 결과에 따르면, 설계단계에서의 안전성 분석 및 간략한 절차에 따라서 SRAC가 빠르게 도출될 수 있다는 장점이 있다. 하지만, 상기에서 언급한 것처럼 안전성 측면에서 고려되어야 할 주요 항목이 간과 될 수 있다. 따라서 본 논문에서는 기존 설계단계에서의 활동을 개선하기 위한 시스템 수명주기 전반에 걸친 안전성 활동에 따른 SRAC 도출방법을 제안하고자 한다. 또한 안전성 활동뿐만 아니라 안전성 평가 활동에 대해서도 설치 단계를 포함한 전체 수명주기에 걸친 SRAC 도출 활동을 제안하였다. 이를 통해서 SRAC를 보다 체계적으로 도출 및 관리 할 수 있으며 수명주기 초기분석단계에서 부터 SRAC를 고려함으로써 안전 요구사항을 반영한 설계가 가능하다.

본 논문에서는 다음의 두 가지 연구목표를 수립하였다.

첫째, 시스템 수명주기 관점에서의 안전성 활동 및 평가활동을 반영한 개선된 SRAC 도출방법 제안

둘째, SRAC 도출방법에 따른 개선된 SRAC 도출

상기 연구목표를 달성하기 위하여,

1) INCOSE System Engineering Handbook에 근거하여, 시스템 엔지니어링 표준 규격인 ISO 15288과 철도 안전규격인 IEC 62278, IEC 62425에 제시된 수명주기 모델을 비교 분석 후, 시스템 개발 프로젝트 수행 단계를 정의하였다.
2) 프로젝트 수행단계에 따른 안전성 활동 및 안전성 평가 활동 절차를 제안하였으며, 단계 별 SRAC 도출을 위한 활동과 산출물과의 관계 및 안전성 평가 측면에서의 SRAC 도출을 위한 활동 및 산출물과의 관계를 도식화함으로써 상호 관계성(Relationship)을 명확히 하기 위한 목적으로 SysML 기반의 Activity Diagram을 활용하였다.

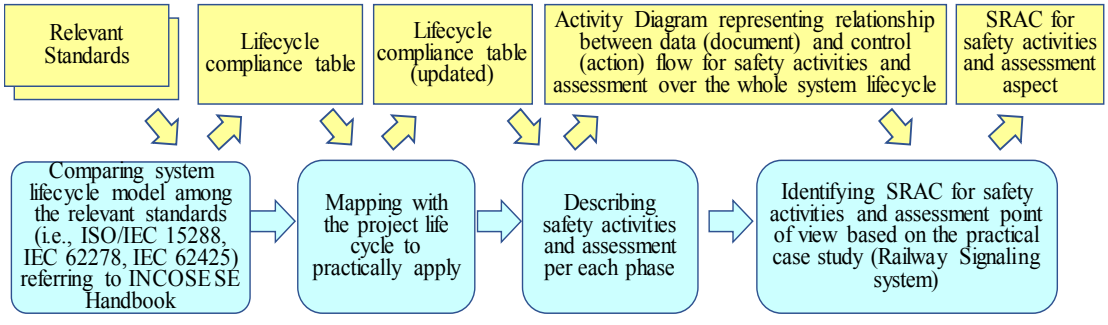

Fig. 4. Concept of Research Approach adopted in this Paper

3) 사례연구에서는 제안한 절차에 근거하여 실제로 개선된 SRAC를 도출하였고, 이를 통해서 연구목표의 효용성 및 유효성을 입증하였다.

다음 Fig. 4는 위에서 언급한 연구 개념을 도식화 한 것이다.

3. 시스템 수명주기 관점에서의 개선된 SRAC 도출 방법

3장에서는 시스템 수명주기 관점에서의 개선된 SRAC도출 방법을 제안한다. 이를 위해서 INCOSE System Engineering Handbook 및 시스템 엔지니어링 관련 규격(ISO/IEC 15288)과 철도 안전성 관련 규격(IEC 62278, IEC 62425)에 기술된 단계별 활동과의 분석을 통해 철도신호시스템 개발에 적용을 위한 수명주기 단계를 Fig. 5와 같이 정의하였다.

Fig. 5에서 8단계(운영 및 유지보수 단계 제외)로 정의된 프로젝트 또는 제품 개발 수명주기는 이후 각 단계별 활동을 안전성 활동과 평가 측면에서 SRAC 도출을 위한 기준으로 활용된다. 이를 근거로, SRAC 도출을 위한 활동 및 산출물 간의 상호관계 분석을 수행하였다.

3.1 안전성 활동에 따른 SRAC 도출 방법

본 절에서는 수명주기 별 안전성 활동에 근거하여 3장에서 기술한 프로젝트 개발 수명주기 별 SRAC 도출을 위한 방법을 제안하였다. 즉, 기존 방식에서는 시스템 전체 수명주기가 아닌 일부단계 즉, 설계단계에 국한하여 SRAC를 도출하였기에 시스템 전체수명주기 관점에서 어떠한 안전성활동이 수행되는지, 이러한 안전성활동이 SRAC와 어떠한 연관성이 있는지를 제안하였다. Fig. 6은 전체 수명주기 관점에서의 시스템 개발을 위한 안전성 활동과 산출물과의 상관관계를 분석한 결과이다. 또한 Fig. 6에는 수명주기에 따른 활동 간의 상관관계, 활동에 따른 산출물이 기술되어있다.

이러한 활동은 기본적으로 철도 규격인 IEC 62278[9]를 근거로 수행되었다. 해당 규격에서는 단계 별 활동수행을 위한 요구사항 만을 명시하고 있을 뿐 상세활동에 대해서는 다루고 있지 않다. 그렇기 때문에, 해당 규격에서 제시하고 있는 단계별 요구사항을 목록화 하고 이에 대응하는 안전성 활동을 매핑함으로써 관련된 안전성 활동을 도출하였다.

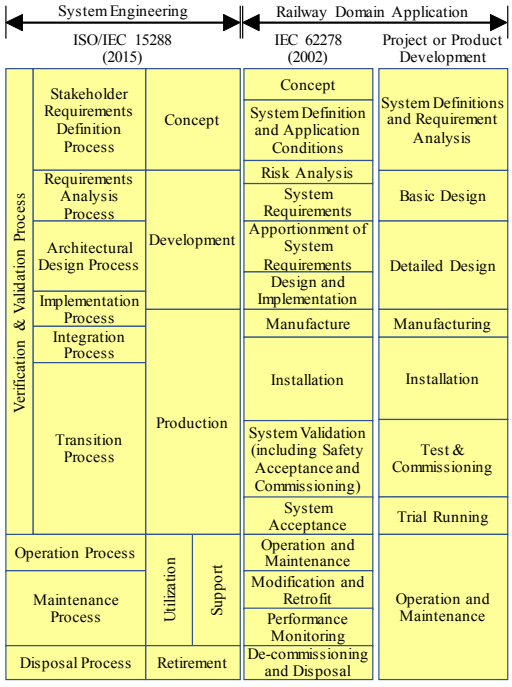

Fig. 5. Relationship of System Lifecycles among Relevant Standards

그리고, 활동 간의 상관관계 및 활동에 따른 산출물간의 상관관계는 국내/외 철도 시스템의 적용사례(예: 매트로 전동차(EMU), 열차제어시스템(TCS) 및 전자연동장치(IXL) 등)를 근거로 하였으며, IEC 62278에서 요구하는 단계별 안전성 요구사항을 충족하는 활동과 산출물의 부합성 검토를 통하여 도출 하였다.

Fig. 6에 근거하여, 프로젝트 수명주기 별 안전성 활동 수행 시 SRAC 도출을 위한 활동을 정의하여 Table 1에 기술하였다.

일례로, 'Basic Design Phase' 에서 수행되는 'Identifying safety requirements' 활동은 SRAC 도출을 위해 다음의 목적을 갖는다.

- 예비 위험원 분석을 수행 시, 해당 제품의 다른 프로젝트에서의 안전성 활동에 따른 Safety Case에 포함된 SRAC 확인
- SRAC에 근거한 요구사항을 도출 후 본 프로젝트 수준에 적용가능유무 식별 후 요구사양서의 입력정보로 활용

이렇게 식별된 SRAC 항목들은 향후 SRAC 도출을 위한 목적으로 활용이 된다. 즉, 상기 항목에 근거하여

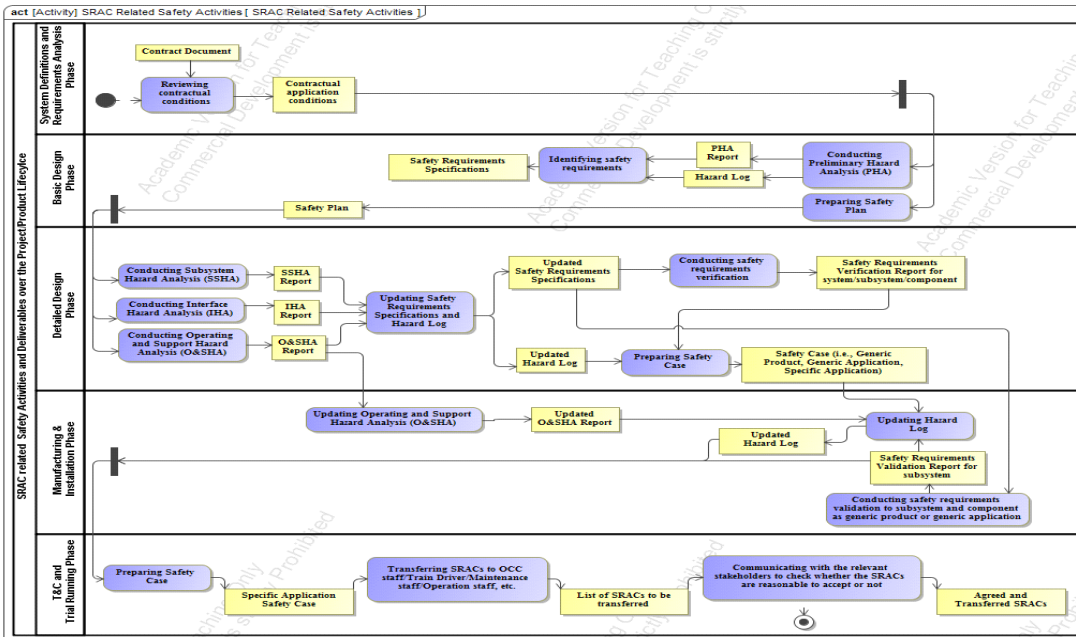

Fig. 6. Activity Diagram to Present Tasks and Deliverables for Elicitation of SRAC over the Development Life Cycle on Safety Activities Aspect

Table 1. Safety Activities for Identification of SRAC Related Items Over the Project Life Cycle

Phase	Safety Activities Tasks Description	SRAC Related Tasks Description
System Definitions and Requirements Analysis Phase	Reviewing contractual conditions	Checking the level of system development and application Checking the list of deliverables with regard to safety activities
Basic Design Phase	Conducting Preliminary Hazard Analysis (PHA)	Checking safety requirements (e.g., O&M, Interface, Environment, EMI/EMC etc.,) to be transferred into higher level or adjacent systems Checking the existing SRAC had been already transferred into high level or adjacent systems Checking safety evidences already applied to other application conditions
	Identifying safety requirements	
	Preparing Safety Plan	Preparing the contents of SRAC to be included into Safety Case when safety plan is prepared
Detailed Design Phase	Conducting System Hazard Analysis (SHA) or Subsystem Hazard Analysis (SSHA), Interface Hazard Analysis (IHA), Operating and Support Hazard Analysis (O&SHA)	Identifying safety requirements to be transferred after elicitation of safety requirements according to hazard analyses
	Conducting safety requirements verification	Exporting safety requirements to corresponding system supplier who is in charge of fulfillment Discussing safety requirements with the corresponding system supplier
	Updating Safety Requirements Specification and Hazard Log	Updating exported safety requirements and Checking the status of fulfillment
	Preparing Safety Case	Checking the exported safety requirements to secure the safety and constraints related to design
Manufacturing & Installation Phase	Updating Operating and Support Hazard Analysis (O&SHA)	Identifying safety requirements to be transferred after elicitation of safety requirements according to hazard analyses (if necessary)
	Updating Hazard Log	Updating exported safety requirements and Checking the status of fulfillment
	Conducting safety requirements validation to subsystem and component as generic product or generic application	Validating the exported safety requirements from Generic Product and Generic Application system to the higher level system
T&C and Trial Running Phase	Preparing Safety Case	Checking the safety requirement to be exported and safety verification & validation results
	Communicating with the relevant stakeholders to check whether the SRACs are reasonable to accept or not	Establishing the way to fulfil the safety requirements after the discussion on the requirements to be exported
	Transferring SRACs to OCC staff/Train Driver/Maintenance staff/Operation staff, etc.	Exporting finally agreed safety requirements to the corresponding system supplier or higher level

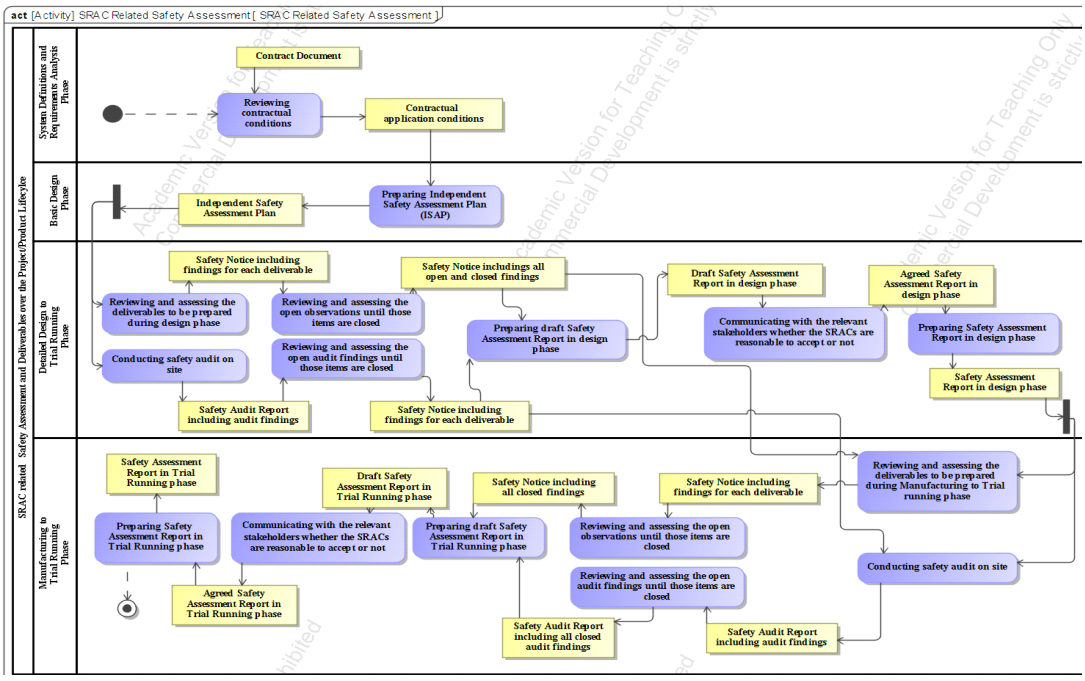

Fig. 7. Activity Diagram to present tasks and deliverable for Elicitation of SRAC over the Development Life Cycle on Safety Assessment Aspect

예를 들면, 초기 시스템 개발 시 상세설계가 확정되기 이전에 예비 위험원 분석을 수행하는 과정에서 적용 대상 시스템이 타 프로젝트에서 개발되어 현장에 설치된 이력이 있거나, 안전성 활동 결과물이 존재한다면, 해당 납품실적, 고장이력데이터 및 안전성 근거문서(예: Hazard Log 및 Safety Case)를 참고하여 근거문서에 기술된 안전성 제약사항 또는 SRAC등을 기본 설계단계에서 안전성 요구사항에 추가하여 설계에 반영될 수 있도록 관리하기 위함이다.

3.2 안전성 평가에 따른 SRAC 도출 방법

본 절에서는 수명주기 별 안전성 평가에 근거하여 3장에서 기술한 프로젝트 개발 수명주기 별 SRAC 도출을 위한 방법을 제안하였다. Fig. 7은 전체 수명주기 관점에서의 시스템 개발 주체인 공급업체가 수행하는 안전성 활동에 대한 내부 또는 외부 독립조직의 안전성 평가 활동을 다루고 있다. Fig. 7에는 수명주기에 따른 안전성 평가 활동 간의 상관관계와 평가 활동에 따른 산출물이 기술되어있다.

이러한 활동은 기본적으로 철도 안전성 승인 관련 규격 IEC 62425 [7] 및 철도 안전성 활동 관련 규격 IEC 62278 [9]을 근거로 도출되었다. 해당 규격에서는 단계별 안전성 활동수행을 위한 요구사항 만을 명시하고 있을 뿐 평가를 위한 상세활동에 대해서는 다루고 있지 않다. 하지만, 안전성 평가 활동은 규격에서 요구하는 안전성 승인을 획득하기 위한 중요한 활동으로써, 안전성 분석을 수행한 결과에 근거하여 단계별 안전성 평가 활동을 도출하였다.

그리고, 활동 간의 상관관계 및 활동에 따른 산출물간의 상관관계는 국내 철도 신호 시스템의 독립안전성평가(ISA) 활동사례(Generic Application 수준의 전자폐색장치, Specific Application 수준의 열차제어시스템 등)를 분석하여 도출 하였다.

Fig. 7에 기반하여, 수명주기에 따른 SRAC 도출을 위해 수명주기 별 안전성 평가과정에서 도출 가능한 SRAC 관련항목들을 Table 2에 기술하였다.

일예로, System Definitions and Requirements Analysis Phase에서 수행되는 Reviewing contractual conditions 활동을 수행함에 있어 SRAC 측면에서 다음을 확인해야 한다.

- 시스템의 개발수준 확인
- 계약범위에 포함한 시스템 형상정보 확인

Table 2. Safety Assessment Activities for Identification of SRAC Related Items Over the Project Life Cycle

Phase	Task Description	SRAC Related Tasks Description
System Definitions and Requirements Analysis Phase	Reviewing contractual conditions	Checking the existing history regarding safety assessment
Basic Design Phase	Preparing Independent Safety Assessment Plan (ISAP)	Preparing the way to elicit and control of SRAC on assessment point of view
Detailed Design Phase	Reviewing and assessing the deliverables to be prepared during design phase	Eliciting SRAC on the way to review safety artefacts(deliverables)
	Reviewing and assessing the open observations until those items are closed	
	Conducting safety audit on site	Eliciting SRAC on the way to conduct safety audit
	Reviewing and assessing the open audit findings until those items are closed	
	Preparing draft Safety Assessment Report in design phase	Preparing the SRAC elicited on the safety assessment
	Communicating with the relevant stakeholders whether the SRACs are reasonable to accept or not	Assigning the corresponding system supplier or high level to fulfill the SRAC after discussion who is in charge of the each SRAC
	Preparing Safety Assessment Report in design phase	Preparing the SRAC elicited on the safety assessment based on the document assessment and audit results Reviewing the results of validation of SRAC exported into higher level system from the lower level system
Manufacturing to Trial Running Phase	Reviewing and assessing the deliverables to be prepared during Manufacturing to Trial running phase	Reviewing applicability of elicited SRAC in design phase Eliciting the SRAC on the way to review the safety artefact (deliverables) in manufacturing to Trial running phase
	Reviewing and assessing the open observations until those items are closed	
	Conducting safety audit on site	Reviewing applicability of elicited SRAC from safety audit in design phase
	Reviewing and assessing the open audit findings until those items are closed	Eliciting the SRAC on the way to conduct safety audit in manufacturing to Trial running phase
	Preparing draft Safety Assessment Report in Trial Running phase	Preparing the SRAC elicited on the safety assessment
	Communicating with the relevant stakeholders whether the SRACs are reasonable to accept or not	Assigning the corresponding system supplier or high level to fulfill the SRAC after discussion who is in charge of the each SRAC
	Preparing Safety Assessment Report in Trial Running phase	Preparing the SRAC elicited on the safety assessment based on the document assessment and audit results Reviewing the results of validation of SRAC exported into higher level system from the lower level system

• 안전성 활동 여부확인에 따른 SRAC 존재여부 확인 등

이렇게 식별된 SRAC 관련항목들은 향후 SRAC 도출을 위한 목적으로 활용이 된다. 즉, 일예로, 시스템 개발 수준 확인을 통해 SRAC를 포함해야 하는 최종 Safety Case가 어느 수준(예: GPSC, GASC, SASC 등)을 대상으로 작성되어야 하는지 사전에 인지할 수 있도록 하기 위함이다.

4. SRAC 도출 방법에 따른 개선된 SRAC 도출

3장에서 제안한 단계별 안전성 활동과 안전성 평가에 근거하여, SRAC를 다음 Table 3과 Table 4와 같이 도출하였다. 즉, Table 3은 Table 1에서 제시한 단계별 안전성 활동 수행시 SRAC 도출을 위해 확인되어야 할 항목을, 실제 안전성 활동에 적용함으로써 도출된 SRAC를 기술한 것이다. 이와 마찬가지로, Table 4는 Table 2에 제시된 안전성 평가 측면에서 확인되어야 할 항목을, 실제 안전성 평가에 적용함으로써 도출된 SRAC를 기술한 것이다. 추가로, 안전성 활동과 평가를 통해 단계별 도출된 SRAC가 어떠한 유형으로 분류되는지 Table 3과 Table 4 에 기술하였다.

SRAC 유형은 Safety Case 작성 시 가이드 역할을 한다. 즉, 이는 SRAC 유형을 참고하여 실제 안전성 활동 및

Table 3. Elicitation of SRAC of Railway Signalling System on the Safety Activities Aspect

Related Phase	Description	Classification
System Definitions and Requirements Analysis Phase	The communication path from/via specific equipment to a receiving unit must comply with relevant parts of EN50159-1.	Communication
	The system architecture shall be defined, and thequantity and type of generic components to be used shall be specified. The functions specified in the requirements shall be allocated to components and the physical location of each component shall be defined.	Configuration
	The specific equipment must be designed to apply fail-safe principles.	Operation
	The specific items shall be required to ensure that the relevant items can be used for safety-related applications.	Configuration
	The ambient temperature to apply this equipment shall be between －25°C and +70°C.	Environment
	The voltages mentioned shall be always in specific range.	Environment
	The humidity rate to apply this equipment shall never exceed specific range without condensing.	Environment
Design Phase	The specific cable shall be used for the specific interface.	Interface, Communication
	The external signalling system to interface must fulfil specific interface specifications.	Interface
	Failures in the signalling circuit must be handled by an adjacent or high level system.	Interface
	The access to the specific item shall be restricted to only authorised personnel.	Security
	The maximum ripple allowed on the supply is limited to specific voltage (peak/peak).	Environment
	In the system, the correct interpretation of the specific module input and output bit patterns shall be implemented.	Network
	Between optical input and optical output, the retransmission delay shall be lower than specific time.	Network
	The contact of the specific relay_dBm shall be closed when the optic power on the optical input is lower than －42 dBm.	Interface
	The specific module shall display on LEDs the correct working status of its internal power supplies.	Maintenance
Manufacturing, T&C Phase	The equipment shall be installed according the installation and adjustment manuals.	Installation
	When the equipment is installed, it shall be confirmed that if the equipment is connected correctly or not, by using drawings and labeling, and the connection state.	Quality
	The link cable between specific modules shall be never exceeded given distance.	Installation
	Periodic inspection and maintenance works must be conducted to obtain the specific data.	Maintenance
	The operator must ensure that the residual risk, associated to an item inducing the perturbation of the input signal of the specific card, is acceptable.	Operation
	The appropriate warning signage on the hot spot of the specific equipment must be attached.	Operation
	Maintenance works must be conducted by a person who has an enough competency to do.	Operation & Maintenance
	The volume of alarm and brightness of the light during operation for a specific equipment and maintenance shall be controlled by maintenance staff.	Environment
	The status of wiring of specific equipment must be checked by operator and maintenance staff through the visual inspection.	Operation
	The status of communication between two equipment must be always checked.	Communication

Table 4. Elicitation of SRAC of Railway Signalling System on the Safety Assessment Aspect

Related Phase	Description	Classification
System Definitions and Requirements Analysis Phase	The specific items must be excepted in the scope of safety activities and assessment since the ultimate client has not included them.	Configuration
	The evidence of quality management activities shall be established through the regular quality audit and quality management	Quality
	O&M regarding other operation and the safety rules shall be compliant to the domestic rules and regulations for safety operation.	O&M
	The train shall include onboard signaling system which is compliant to the reference operational conditions.	Environment
Design Phase	Failures and defects of the components which interface with the relevant components shall be treated in fail-safe way by themselves. Considering the domestic operation environment, the relevant specifications shall be satisfied.	Interface
Manufacturing, T&C Phase	O&M regarding Train Control System shall be compliant to the O&M manual provided by the supplier.	Operation & Maintenance
	Periodic inspection and test according to the environmental condition changes considering in the specific items characteristics shall be conducted during the operation.	Environment

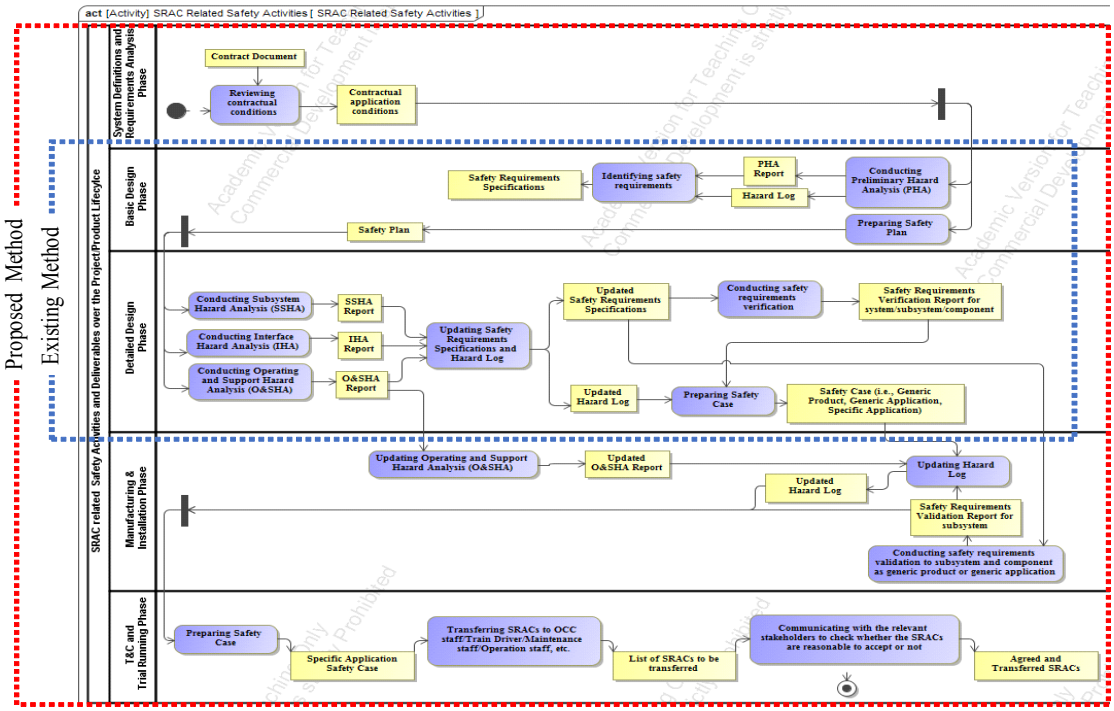

Fig. 8. Comparison the scope of Elicitation of SRAC between Existing method and Proposed Method (e.g., Safety Activities Aspect)

안전성 평가 시 필수적으로 확인해야 할 항목을 식별하여 분류한 것이다. 기존방식에서는 시스템 형상 (Configuration), 운영 및 유지보수(Operation & Maintenance)와 같은 SRAC의 유형이 제시되었다.

Table 3에 기술된 SRAC의 유형은 기존방식의 SRAC 유형을 근거로, 제안한 방식에 따라 도출된 SRAC의 유형을 분류한 결과이다. 그러나, 유형을 분류하는 과정에서 기존의 유형만으로는 제안한 SRAC의 분류가 불가능하기에 추가적으로 SRAC 유형을 정의하였다.

추가적으로 도출된 SRAC 유형은 기존에 정의된 SRAC유형으로 분류할 수 없는 SRAC들의 핵심 키워드를 분석하고 그룹화 함으로써 정의하였다. 따라서 추가적인 SRAC의 유형이 정의됨으로써, 추가된 SRAC의 유형이 Safety Case를 작성 시 안전성 관점에서의 추가적인 요구사항으로 식별되고, 이러한 요구사항이 안전성 측면에서의 향상에 기여한다. 추가된 SRAC 유형은 5가지 항목 즉, 통신 또는 네트워크, 환경, 설치, 품질 및 보안 등이며, 이는 Table 3에 기술된 SRAC의 유형을 분류하는 데 활용되었다.

5. 철도신호시스템 사례적용 – 기존 SRAC와 제안된 SRAC 도출방식에 따른 비교

5장에서는 기존의 안전성 활동(Safety Activities)만을 고려한 설계단계에서의 SRAC 도출을 위한 접근방법(Existing Method)과 본 연구에서 제안하는 전체 수명주기에 걸친 안전성 활동과 평가(Safety Activities and Assessment)를 통한 SRAC 도출을 방법(Proposed Method)을 비교하기 위하여 Fig. 8과 같이 도식화 하였다.

또한, 본 연구에서 제안하는 접근방법이 실제 철도신호시스템의 적용을 통해 어떻게 도출되는지를 기존 접근을 통한 도출항목과 제안방법에 따른 도출항목을 시스템 수명주기 별 항목으로 기술하였다.

이를 위해, 4장의 Table 3, Table 4에서 도출된 수명주기 단계별 SRAC를 근거로, 철도신호시스템의 안전성 활동과 안전성 평가에 적용한 SRAC를 Table 5에 도출하여 기술하였다. 즉, Table 5는 기존 방법에 따라 도출된 SRAC와 제안한 방법에 따른 안전성 활동과 평가를 통해 도출된 SRAC를 비교한 것이다. Table 5에는 도출된 SRAC 들이 기술되어 있고, 이러한 항목들이 제안한

Table 5. The Result of Comparison of SRAC Elicitation between Existing Method and Proposed Method

Phase	SRAC Description	Classification	Existing method	Proposed Method	Remarks
System Definitions and Requirements Analysis Phase	The communication path from/via signalling system to a receiving unit must comply with relevant parts of EN50159-1.	Communication	X	O	Safety Activities
	The system architecture shall be defined, and the quantity and type of generic components to be used shall be specified. The functions specified in the requirements shall be allocated to components and the physical location of each component shall be defined.	Configuration	O	O	Safety Activities
	Point mechanisms and detectors (position and locking of the frogs and blades) must be designed to apply fail-safe principles.	Operation	O	O	Safety Activities
	The MY2K relay (latching relay) shall be required to ensure it can be used for safety-related applications.	Configuration	O	O	Safety Activities
	The ambient temperature to apply Data Link Module shall be between －25℃ and +70℃.	Environment	X	O	Safety Activities
	The voltages mentioned shall be always in the range +/- 10 %.	Environment	X	O	Safety Activities
	The humidity rate to apply Input /Output module shall never exceed 95% without condensing.	Environment	X	O	Safety Activities
	The proven used items must be excepted in the scope of safety activities and assessment since the ultimate client has not included them.	Configuration	O	O	Safety Assessment
	The evidence of quality management activities shall be established through the activities referring to ISO 9001.	Quality	X	O	Safety Assessment
	O&M regarding other operation and the safety rules shall be compliant to the rule of Korail and/or Metro.	O&M	O	O	Safety Assessment
	The train running on double track railway where train control system (ATP) installed shall include onboard signalling system which is compliant to ETCS Level1.	Environment	X	O	Safety Assessment
Design Phase	The communication cable shall be used to comply with interface communication protocol.	Interface, Communication	X	O	Safety Activities
	The external signalling system to interface with Lineside Equipment must fulfil Interface ‘S’ specifications.	Interface	X	O	Safety Activities
	Failures in the signal output circuit must be handled by the interlocking system.	Interface	X	O	Safety Activities
	The access to the Signaling Equipment Room shall be restricted to only authorised personnel.	Security	X	O	Safety Activities
	The maximum ripple allowed on the supply is limited to 5 V (peak/peak).	Environment	X	O	Safety Activities
	In the IXL system, the correct interpretation of the Point Module input and output bit patterns shall be implemented.	Network	X	O	Safety Activities
	Between optical input and optical output, the retransmission delay shall be lower than 200 ns.	Network	X	O	Safety Activities
	The contact of the relay AL_dBm shall be closed when the optic power on the optical input is lower than －42 dBm.	Interface	X	O	Safety Activities
	The optical data link module shall display on 3 front face green LEDs the correct working status of its internal power supplies (+5 VD, +5 VA & -5 VA).	Maintenance	O	O	Safety Activities
	Failures and defects of ABS or EI which interface with LEU shall be treated in fail-safe way by themselves. Considering the domestic operation environment, the relevant specifications shall be satisfied.	Interface	X	O	Safety Assessment
Manufacturing, T&C Phase	The signalling equipment shall be installed according the installation and adjustment manuals.	Installation	X	O	Safety Activities
	When the remote control unit is installed, it shall be confirmed that if the Unit is connected correctly or not, by using drawings and labeling, and the connection state.	Quality	X	O	Safety Activities

Phase	SRAC Description	Classification	Existing method	Proposed Method	Remarks
	The link cable between the Data link module and the Trackside module shall be never exceeded 1.05 m.	Installation	X	O	Safety Activities
	Periodic track inspections and maintenance works are performed to obtain the track geometry, minimum adherence factor and shunting properties.	Maintenance	O	O	Safety Activities
	The operator must ensure that the residual risk, associated to a broken cable inducing the perturbation of the input signal of the relay circuit board, is acceptable.	Operation	O	O	Safety Activities
	The appropriate warning signage on the hot spot of the safety equipment must be attached.	Operation	O	O	Safety Activities
	Maintenance works must be conducted by a person who has an enough competency to do.	Operation & Maintenance	O	O	Safety Activities
	The volume of alarm and brightness of the light during operation and maintenance for a safety equipment shall be controlled by maintenance staff.	Environment	X	O	Safety Activities
	The status of wiring of specific equipment of integrated control equipment must be checked by operator and maintenance staff through the visual inspection.	Operation	O	O	Safety Activities
	The status of communication between remote monitoring device and rail temperature monitoring device must be always checked.	Communication	X	O	Safety Activities
	O&M regarding this train control system (ATP) shall be compliant to the O&M manual provided by the supplier.	Operation & Maintenance	O	O	Safety Assessment
	Periodic test considering track characteristics changes according to track characteristics and environment changes in tunnel shall be conducted during the operation.	Environment	X	O	Safety Assessment

방법과 기존 방법 중 어느 방법에 의해 도출 되는지를 표기하였다. 또한, 도출된 SRAC가 어느 유형에 속하는지를 평가하여 표시하였다. 그리고, 비고란(Remarks)에는 본 논문에서 제안한 두 가지 측면에서 SRAC가 안전성 활동과 평가 중 어느 항목에 포함되는지를 표기하였다.

Table 5에서 확인할 수 있듯이, 제안된 방식에 따라 도출된 SRAC는 기존 방식에 따라 도출된 SRAC를 모두 포함하고 있으며, 추가적으로, 더 많은 항목의 SRAC가 도출된 것을 알 수 있다. 즉, 기존방식을 통해 도출된 SRAC는 12개 항목이며, 제안방식을 통해 도출된 SRAC는 33개이다. 33개항목 중 안전성 평가를 통해 도출된 항목이 7개이다. 또한 제안방식을 통해서만 도출된 SRAC가 21개로 확인되었다. 추가된 21개의 SRAC는 안전 관련 요구사항으로 시스템 설계에도 반영(10개 요구사항) 될 뿐만 아니라, 시험 및 시운전과 운영 및 유지보수 단계에 반영(12개 요구사항)되어 안전 확보에 기여한다.

그리고, 제안된 방식을 통해 신규로 도출된 SRAC 들은 기존의 SRAC유형으로는 분류할 수 없으며, 4장에서 제안한 새로운 5가지의 SRAC유형으로 분류될 수 있음을 확인하였다.

따라서, 신규로 도출된 SRAC 유형이 향후 제안한 방법에 따른 SRAC 도출 시 가이드 역할을 해줄 수 있음을 확인하였다.

이와 같이 추가적으로 도출된 SRAC 항목 및 유형이 시스템 설계에 적용됨으로써, 기존에 고려하지 못했던 안전성 요구사항이 시스템 개발 초기단계에서부터 안전성 요구사항으로 고려됨으로써 시스템의 안전설계에 반영된다. 즉, 이는 더 많은 안전관련 항목들이 시스템 설계 초기단계부터 반영됨으로써 향후 시스템 개발과정에서의 설계 안전성을 확보하는데 기여한다.

6. 결론

철도시스템의 안전한 설계를 위한 활동으로 SRAC를 포함한 Safety Case의 작성이 요구되고 있으며, SRAC의 도출 및 관리가 일부단계에 국한되어 적용됨으로써 누락될 수 있는 안전성 요구사항을 확인하기 위하여 SRAC 도출방법의 개선이 요구되어지고 있다.

이를 달성하기 위해 본 논문에서는 다음을 수행하였다.

1) 시스템 수명주기 관점에서 접근하기 위해 시스템

엔지니어링 표준인 ISO/IEC 15288과 철도안전 표준을 비교분석함으로써 프로젝트 개발에 적용을 위한 시스템 수명주기를 정의하였다.

2) 시스템 수명주기 관점에서 안전성 활동 및 평가활동이 어떻게 수행되는지 단계별 활동을 도출하고, 그에 따른 활동과 활동 간의 상호관계, 활동과 산출물간의 상호관계를 기술하기 위하여 Activity Diagram을 활용하여 도식화 하였다.

3) SRAC 도출을 위한 개선된 방법을 제안하기 위하여 수명주기별 안전성 활동과 평가 측면에서 SRAC 도출방법을 기술하였으며, 이를 기반으로 SRAC를 도출하였다. 또한 SRAC의 도출에 따른 SRAC의 유형을 분류하고 이를 기존방법에서 제시한 유형과 비교함으로써 새롭게 도출된 SRAC 유형이 향후 제안한 방법에 따른 SRAC 도출 시 가이드 역할을 해 줄수 있음을 확인하였다.

4) 철도신호시스템에서의 사례 연구를 통하여 본 논문에서 제시하는 방법이 수명주기 전체에 걸친 SRAC의 도출 및 관리를 수행함으로써 누락의 위험이 줄어든 SRAC의 도출 및 관리가 가능함을 보여주었다.

본 연구결과에 따르면, SRAC 도출 시 보다 체계적으로 도출 및 관리 할 수 있으며, 설계 초기단계에서부터 SRAC를 고려함으로써 안전성 측면의 요구사항을 최대한 반영한 안전설계가 가능하다.

References

[1] C. A. Ericson, *Hazard Analysis Techniques for System Safety. 1st ed*. Hoboken, MA: John Wiley & Sons, Inc., 2005.

[2] Korea Transportation Safety Authority, *Transportation Accident Status and Statistical Analysis on 2016 Year*, pp. 04-14, Korea Transportation Safety Authority, Korea, Analysis Report, Apr. 2016.

[3] Korea Transportation Safety Authority, *Transportation Accident Status and Statistical Analysis on the First Half of 2017 Year*, pp. 04-11, Korea Transportation Safety Authority, Sep. 2017.

[4] Rolling Stock Maintenance Department, *Rolling Stock RAMS Operation Guideline*, pp. 1-7, Ministry of the interior and Safety, Korea, Regulations, Dec. 2014.

[5] Korea Railroad Research Institute, *Notice to Tenderers for Independent Safety Assessment on 400km/h Railway Transponder*, pp.21, Jun. 2014.

[6] D. W. Kim, K. Y. Song, *Application on train control system certified by Independent Safety Assessment to suseo high speed train*, pp.1, Korea Rail Network Authority, 2016.

[7] Railway Applications - Communications, Signalling and Processing Systems - Safety Related Electronic Systems for Signalling, International Electrotechnical Commission Standard, IEC 62425, 2007.

[8] B. Friedemann, F. Ulrich, and G. Huw, "Safety-related application conditions - A balance between safety relevance and handicaps for applications," *Proc. Computer Safety, Reliability, and Security: 28th International Conference, SAFECOMP 2009*, pp. 32-45, Sep. 2009.

[9] Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), International Electrotechnical Commission Standard, IEC 62278, 2002.

[10] B. John, R. Roger, H. Ibrahim, B. Ben, B. John, H. Dave, J. Peter, M. Helen, P. Robert, "Safety cases and their role in ISO 26262 functional safety assessment," *Proc. Computer Safety, Reliability, and Security: 32nd International Conference, SAFECOMP 2013*, pp. 154-165, Sep. 2013.

[11] J. Westman, M. Nyberg, M. Törngren, "Structuring safety requirements in ISO 26262 using contract theory," *Proc. Computer Safety, Reliability, and Security: 32nd International Conference, SAFECOMP 2013*, pp. 166-177, Sep. 2013.

[12] M. Rausand, I. B. Utne, "Product safety - Principles and practices in a life cycle perspective," Safety Science, vol. 47, no. 7, pp. 939-947, Oct. 2009.
DOI: https://doi.org/10.1016/j.ssci.2008.10.004

[13] O. Nordland, "Safety case categories - Which one when?," *Proc. Current Issues in Safety-Critical Systems: Proceedings of the Eleventh Safety-critical Systems Symposium*, pp. 163-172, Feb. 2003.

[14] Public Policy Institute for People, *Why the accident at Gui Station was happened? Organizational thinking approach*, pp. 95-102, Public Transportation Network, Dec. 2016.

[15] European Committee for Electrotechnical Standardization, *Railway applications – Communication, signalling and processing systems - Application guide for EN 50129 - Part 2: Safety assurance*, European Committee for Electrotechnical Standardization, CLC/TR 50506-2, Dec. 2009.

백 영 구(Young-Goo Baek) **[정회원]**

- 2001년 8월 : 서울과학기술대학교 안전공학과 (공학사)
- 2003년 2월 : 광운대학교 제어계측과 (공학석사)
- 2012년 3월 ~ 현재 : 아주대학교 시스템공학과 (박사과정)

<관심분야>
시스템공학 (SE), 모델기반 시스템공학 (MBSE), Railway System & Safety Assurance, Modeling & Simulation 등.

이 재 천(Jae-Chon Lee) **[정회원]**

- 1977년 2월 : 서울대학교 공과 대학 전자공학과(공학사)
- 1979년 2월 / 1983년 8월 : KAIST 통신시스템 (석/박사)
- 1984년 9월 ~ 1985년 9월 : 미국 MIT Post Doc 연구원
- 1985년 10월 ~ 1986년 10월 : 미국 Univ. of California 방문연구원
- 1990년 2월 ~ 1991년 2월 : 캐나다 Univ. of Victoria (Victoria, BC) 방문교수
- 2002년 3월 ~ 2003년 2월 : 미국 Stanford Univ. 방문교수
- 1994년 9월 ~ 현재 : 아주대학교 시스템공학과 정교수

<관심분야>
시스템공학 (SE), Model-Based SE (MBSE), Systems Safety, System T&E, Modeling & Simulation