철도시스템 설계시 안전성 확보를 위한 메타모델에 관한 연구

On the Meta Model to Assure Safety in the Design of Rail Systems

김영현*†, 이재천*

Young-Hyun Kim*†, Jae-Chon Lee*

Abstract Due to the rapid advance of technology, systems are becoming more complex. As such, the systems failure caused by the design errors can possibly result in an increase in terms of both frequency and impact of accidents. Therefore, a special care must be taken on assuring safety in the systems development. In this study, a model-based approach using SysML is discussed on how to incorporate safety concerns in the rail systems design. To do so, by analyzing both system design data and safety data related to rail systems, a meta model for system and safety data is obtained. Using the meta model, a rail system design process model is presented using SysML. When the rail systems are designed with safety assurance needed, the models presented in the study can be useful.

Keywords **:** Rail System Safety, Safety Standard, Meta-Model, SysML, System Engineering

초 록 기술의 급격한 발전으로 인해 시스템은 점차 대형화, 복잡화되고 있어서 이로 인해 시스템 설계 오류 등으로부터 발생할 수 있는 사고나 고장의 위험 또한 증대하고 있다. 시스템의 안전성 확보를 위해 시스템 설계 활동부터 여러 안전 표준을 적용해서 설계를 할 필요가 있다. 본 연구에서는 철도시스템의 설계에서 관련 안전 표준들을 체계적으로 반영하여 안전성의 확보를 달성하기 위한 하나의 방안을 연구하였다. 특별히 철도시스템의 안전 설계 데이터를 분석하여 철도시스템 특성에 맞게 안전 표준 메타모델을 생성하였다. 또한, 시스템 모델링 표준 언어인 SysML을 기반으로 철도시스템 안전 표준에서 제시하고 있는 시스템 설계 프로세스 모델을 제시하였다. 철도시스템 설계에서 안전 표준 메타모델을 활용함으로써 설계에서 필요한 안전관련 정보 및 자료를 일관적으로 관리하거나 효과적으로 구성할 수가 있어 철도시스템 설계에서 안전성 확보에 도움이 된다.

주요어 : 철도 안전, 안전 표준, 메타모델, SysML, System Engineering

1. 서 론

오늘날 기술 발전으로 인해 시스템이 점차 대형화, 복잡화되고 있다. 이로 인해 시스템 설계 오류 등으로부터 발생할 수 있는 사고나 고장의 위험 또한 점차 증대하고 있다. 특히 국방, 항공기, 철도 등 안전이 중시되는 시스템들은 사고나 고장 발생 시 막대한 재산피해나 인명피해로 이어지게 된다. 이러한 이유로 안전이 중시되는 각 산업분야에서는 안전과 관련한 표준을 제정하고 있고 이를 준수하도록 권장하고 있다. 대표적인 안전 표준의 예로는 전지/전자/프로그램이 가능한 전자장치 시스템의 기능안전을 다루고 있는 IEC 61508을 중심으로, 자동차 전장품의 기능안전을 다루고 있는 ISO 26262, 철도 RAMS를 다루고 있는

† 교신저자: 아주대학교 공과대학 시스템공학과 (gkyhg@ajou.ac.kr)
* 아주대학교 공과대학 시스템공학과

EN 50126등이 있다. 이처럼 기능 안전의 대표적인 표준인 IEC 61508부터 각 산업분야의 안전 표준들이 제정된 것은 그만큼 기능안전이 중요해졌다는 것을 의미한다[3]. 기능안전이 중요해진 이유로는 처음에 기술한 내용처럼 기술 발전으로 인해 전장품의 증가로 기능의 역할 또한 증대했고 여기에서 발생하는 위험 또한 증가했기 때문이다. 시스템의 안전성 확보를 위해 시스템 설계 활동부터 기능안전을 포함한 여러 안전 표준을 적용해서 설계를 할 필요가 있다.

본 연구에서는 철도시스템의 설계에서 관련 안전 표준들을 체계적으로 반영하여 안전성의 확보를 달성하기 위한 하나의 방안을 연구한다. 철도시스템의 안전 설계 데이터를 분석하여 철도시스템 특성에 맞게 안전 표준 메타모델을 생성하고, 시스템 모델링 표준 언어인 SysML을 기반으로 철도시스템 안전 표준에서 제시하고 있는 시스템 설계 프로세스 모델을 제시하였다. 안전 표준 메타모델을 철도시스템 설계에서 활용함으로써 설계에서 필요한 안전관련 정보 및 자료를 일관적으로 관리하거나 효과적으로 구성할 수 있기 때문에 철도 시스템 설계 시 안전성 확보에 도움이 된다.

본 논문의 구성은 제1장에서는 서론을 기술하고, 제2장에서는 철도 시스템 특성을 반영한 안전 표준 메타모델을, 제3장에서는 안전 표준 메타모델을 적용한 모델기반 철도 설계 프로세스를 기술한다. 제4장에서는 결론을 기술하였다.

2. 철도 시스템 특성을 반영한 안전 표준 메타모델

2.1 안전 표준 메타모델 특징

참고문헌[1]에서는 안전 표준 37개를 참고하여 안전 관련 데이터 및 정보를 관리하기 위한 메타모델을 제시했다[1]. 선행연구에서 제시하고 있는 안전 표준 메타모델은 크게 7가지로 구성이 되어 있다. 구성요소로는 Requirement, Activity, Role, Artefact, Technique, CriticalityKind, ApplicabilityKind를 제시하고 있다.

Requirement는 안전 설계 활동 시 수행해야만 하는 요구사항을 나타내고, Activity는 안전 설계 활동 요소를 나타낸다. Role은 Activity를 하게 될 구성원 정보를 나타내고, Artefact는 설계 활동에서 관리해야 하는 데이터 요소를 나타낸다. Artefact의 예로는 EN 50126이나 ISO 26262에서 제시하고 있는 Safety Plan이 있다[2]. Technique는 앞에서 제시한 Activity 수행과 Artefact 생산에 대해 구체적으로 필요한 기술 또는 방법을 나타낸다. 참고문헌[1]에서 제시하고 있는 안전 표준 메타모델에서 안전과 관련된 가장 중요한 요소는 CriticalityKind와 ApplicabilityKind가 있다. CriticalityKind는 리스크 감소를 위한 기준을, ApplicabilityKind는 받아들일 수 있는 리스크 수준이 되었는지를 나타낸다.

Fig 1.에서는 SysML Diagram중에 구조 다이어그램에 해당되는 Block Definition Diagram을 활용하여 안전 표준 메타모델을 모델링했다. 안전 표준 메타모델 구성요소 뿐만 아니라 구성요소 사이의 관계까지 모델링되어 있는 것을 확인할 수 있다.

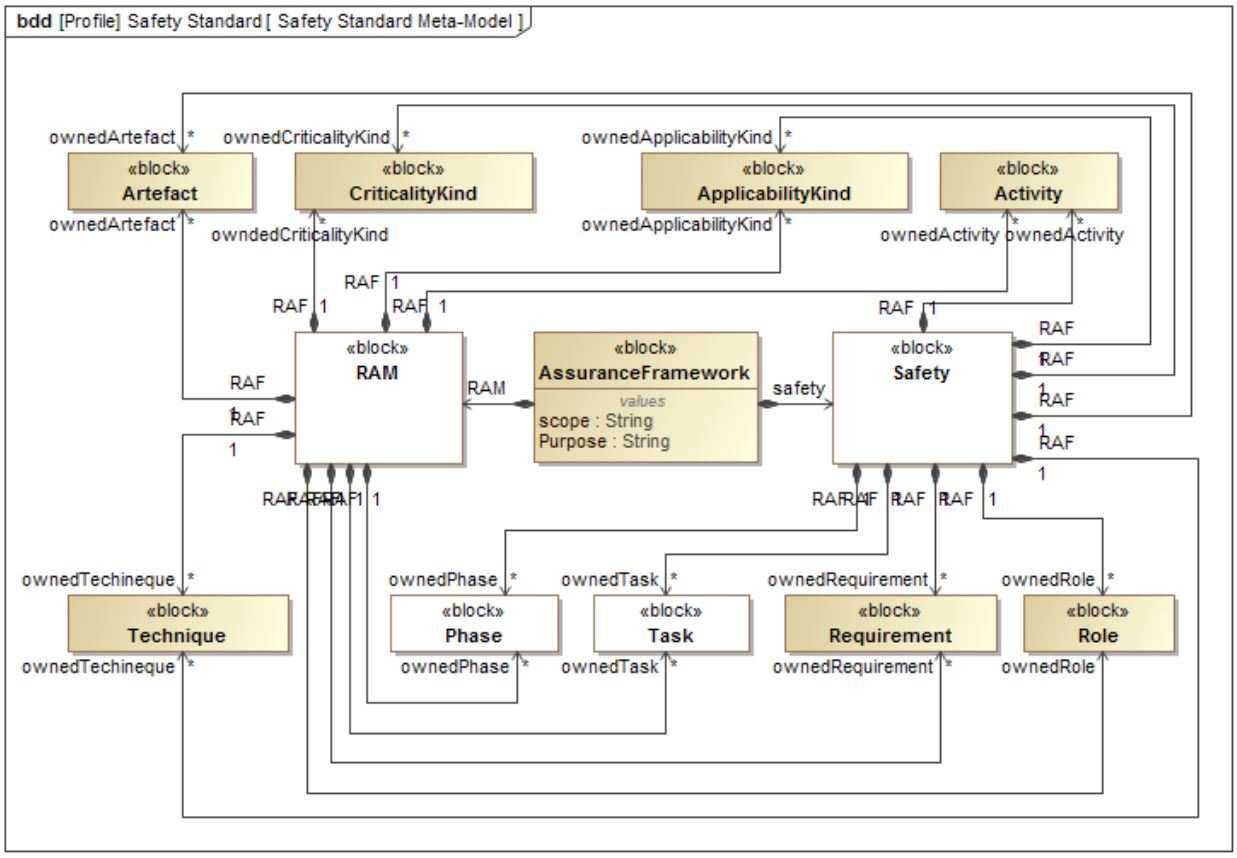

Fig. 1 Safety Standard Meta-Model

2.2 철도 시스템 특성을 반영한 안전 표준 메타모델

철도 표준인 EN 50126에서는 철도 시스템의 신뢰성, 가용성, 유지보수성, 안전성 간의 상호작용 관점에서 RAMS를 정의하고, 시스템 수명 주기와 그 주기에 포함되어 있는 활동에 근거하여 RAMS를 관리하기 위한 절차를 정의하고 있다[2].

기존 안전 표준 메타모델에서는 안전을 한가지의 관점으로 구성했다면, 철도 표준에서는 RAM과 Safety로 구분해서 각각의 활동을 정의하고 있다. 이러한 내용을 반영하기 위해 기존 메타모델에 구성요소 상위에 RAM과 Safety를 추가했다.

안전 표준들의 특징 중에 하나는 시스템 생명주기 관점에서 안전 활동을 기술하고 있다는 점이다. 이는 시스템 개발부터 폐기까지 안전성을 확보해야 됨을 의미하고 있다. 기존 메타모델은 설계 활동을 중심으로 정의가 되어 있고, 수명주기 관점에 대한 부분이 제시되어 있지 않았다. 그래서 안전 표준 메타모델에 phase와, 각 설계 활동의 Task를 추가했다.

3. 안전 표준 메타모델을 적용한 모델기반 철도 설계 프로세스

3.1 안전 표준 메타모델을 적용한 모델기반 철도 설계 프로세스

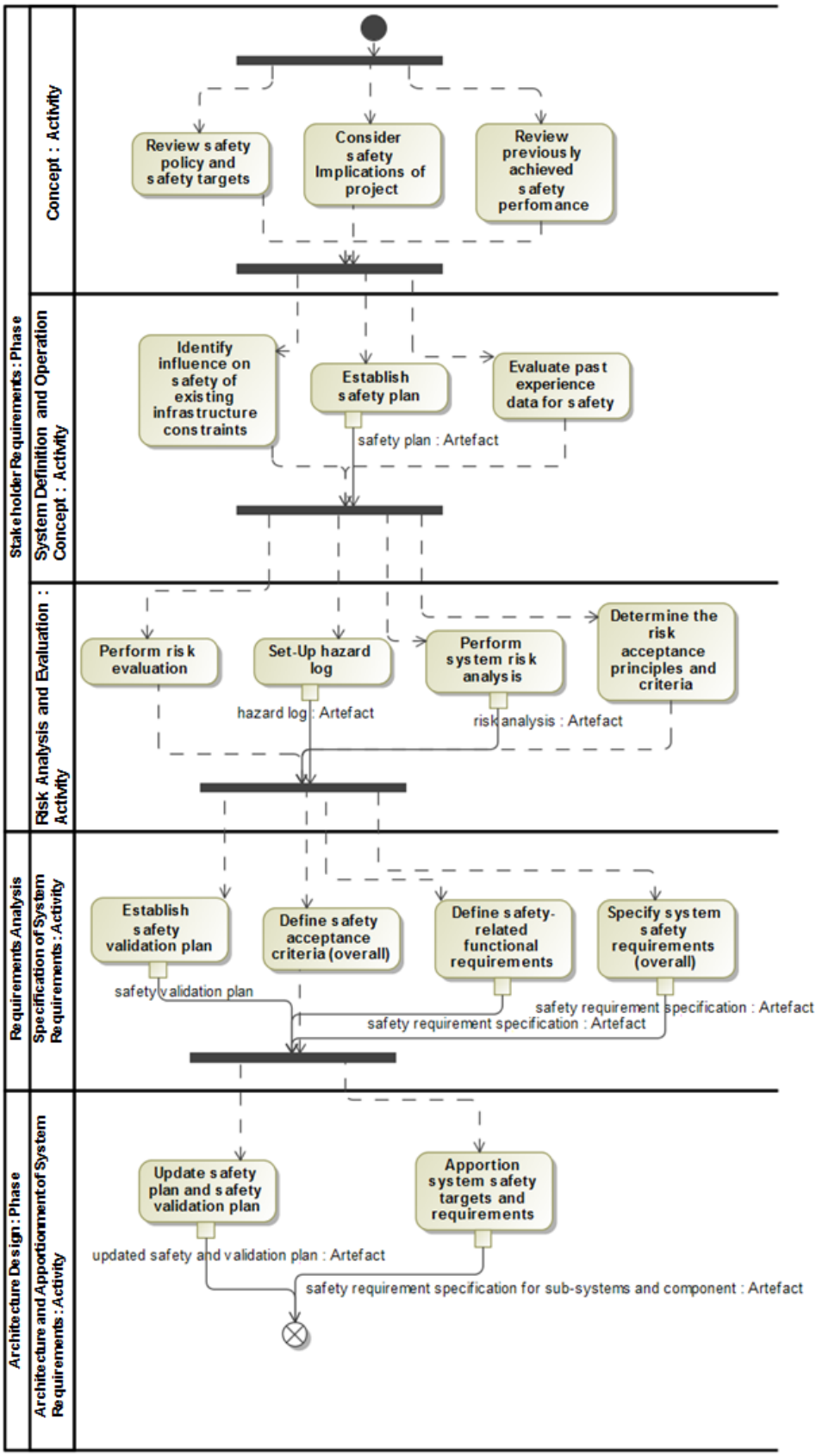

Fig. 2 Rail System Safety Life-Cycle

EN 50126에서는 시스템 수명주기 각 단계별에서 해야 하는 RAM과 Safety 활동을 명시하고 있고, RAMS 사이의 상호작용 관점에서도 기술하고 있다. SysML 모델링 언어를 기반으로앞에서 제시한 안전 표준 메타모델을 활용하여 철도 설계 프로세스를 모델로 나타낸다.

Fig.2에서는 SysML 거동 Diagram중에 하나인 Activity Diagram으로 철도 시스템 안전프로세스의 Concept 개발 단계를 나타낸 것이다. 시스템 생명주기 단계를 메타모델 요소인 Phase를 사용해서 정의하고 있고, 각 단계에서 수행해야 할 안전 활동은 메타모델 요소 중에 Activity를 사용해서 정의하고 있다. 각 단계에 활동을 통해 나온 산출물은 Activity Diagram의 Pin이라는 모델요소를 통해 나타냈고, 메타모델 요소 중에 Artefact를 사용했다.

Concept 단계에서는 안전 대상과 안전 정책에 대한 사전 검토와, 프로젝트의 안전 관련 사항을 고려하고, 이전에 달성된 안전 성능에 대해 미리 검토한다. System Definition and Operation Concept 단계에서는 기존 설비의 제약 조건이 안전에 미치는 영향에 대해 확인해보고, 안전성 계획을 수립하고, 안전에 대한 과거 정보를 평가해본다. 이 단계에서 모든 Safety Plan을 구축하고, 관련된 문서가 산출물로 나온다. Risk Analysis and Evaluation 단계에서는 Risk를 평가하고 Hazard 로그를 남기고, 시스템 Risk Analysis를 진행한 후에 받아 들일 수 있는 Risk 정도를 결정한다. Specification of System Requirement에서는 안전성 검증 계획을 수립하고 허용 가능한 안전 기준을 정의, 안전과 관련된 기능 요구사항을 정의하고 시스템 안전 요구사항을 정의한다. Architecture Apportionment of system requirements 단계에서는 안전성 검증 계획과 안전성 계획을 갱신하고 시스템 안전 목표와 요구사항을 시스템에 할당한다.

4. 결 론

본 연구에서는 안전 표준 메타모델의 필요성에 대해서 설명하고, 안전 표준 메타모델을 철도 시스템 특성에 맞게 확장시켰다. 그리고 안전 표준 메타모델을 활용하여 SysML을 기반으로 철도 시스템 안전 설계 프로세스에 적용해보았다.

철도 시스템 설계에서 안전 표준 메타모델을 사용함으로써 설계에서 필요한 안전관련 정보 및 자료를 일관적으로 관리하거나 구성하기가 효과적이다. 이뿐만 아니라 같은 안전 표준 메타모델을 사용했다면, 철도 안전에서 사용한 안전관련 정보 및 자료를 다른 표준에 적용하거나 또는 다른 안전 표준의 정보를 가져와서 사용하는 것이 매우 용이하다.

참고문헌

[1] Jose Luis de la Vara, Alejandra Ruiz, Katrina Attwood, Huáscar Espinoza, et al. (2016) Model-based specification of safety compliance needs for critical systems: A holistic generic metamodel, *Information and Software Technology*, 72, pp. 16-30

[2] EN (2012) Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)- Part1, EN Standard, EN 50126-1

[3] IEC (2010) Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC Standard, 61508.

[4] Jose Luis Vara and Rajwinder Kaur Panesar-Walawege, (2013) SafetyMet: A Metamodel for Safety Standards, *Model-Driven Engineering Languages and Systems: 16th International Conference*, pp. 69-86.

[5] Ibrahim Habli, Ireri Ibarra, Roger Rivett, and Tim Kelly, (2010) Model-based assurance for justifying automotive functional safety, *SAE International*.

[6] Alessio Ferrari, Alessandro Fantechi, Stefania Gnesi, and Gianluca Magnani, (2013) Model-Based Development and Formal Methods in the Railway Industry, *IEEE Softw.*, 30(3), pp. 28-34.