SysML 기반 M&S 기법을 통한 시스템 고장 모델의 검증

On the Verification of Systems Failure Models Using SysML-Based M&S Methods

조정호*†, 이재천*

Jeong Ho Jo*†, Jae-Chon Lee*

Abstract There has been noticeable demand on safety assurance for the safety-critical systems such as rail systems as the underlying systems are getting more complex and using electronic/electrical components more frequently. As such, the functional safety standard and its variations have been developed and used in a variety of industrial domains. The standards are urging that hazard analysis be performed and the result incorporated in the systems design from the conceptual design phase. The objective of this study is to present a model-based approach to hazard analysis. Specifically, a system model including functional and physical models are developed first based on SysML. Those models are then used to construct systems failure models. Finally, to verify the model-based hazard analysis, simulation of the models developed are carried out. The verified results of hazard analysis would be useful in the design of corresponding safety systems.

Keywords **:** SysML, Failure Models, M&S, Model-Based Safety Analysis, Systems Engineering

초 록 오늘날의 철도시스템을 비롯한 안전중시시스템은 그 복잡성과 전장구성품의 비중이 증가함에 따라, 시스템의 안전성 확보에 대한 필요성도 함께 증가하고 있다. 이를 반영하여 안전중시시스템에 대한 다양한 산업별 안전표준에서는 개념설계 단계에서부터 체계적인 위험원 분석을 수행하여 설계에 반영할 것을 요구하고 있다. 본 논문에서는 철도시스템의 개념설계 단계에서 수행되는 위험원 분석의 결과를 검증하기 위해서 SysML을 활용하여 시스템 고장 모델을 생성하고, 시뮬레이션을 통하여 검증하는 방법을 연구하였다. 구체적으로 먼저 대상시스템의 기능/물리 아키텍처를 SysML 기반으로 모델링하였다. 그리고 나서 시스템 모델에 대한 위험원 분석을 모델 기반으로 수행할 수 있도록 위험원 분석 기법에서 공통적으로 다루는 고장 유형, 고장의 원인과 영향 등의 요소를 식별하여 시스템 모델에 추가하였다. 그 후 모델 기반 위험원 분석을 수행하고, 결과를 토대로 고장 모델을 정의하였다. 마지막으로 고장 모델이 반영된 시스템 모델을 시뮬레이션 함으로써 모델 기반 위험원 분석에 대한 검증을 수행하였다. 검증된 위험원 분석의 결과를 향후 효과적으로 안전 설계에 활용할 수 있다.

주요어 : 시스템 모델링 언어, 고장 모델, 모델링과 시뮬레이션, 모델 기반 위험원 분석, 시스템공학

1. 서 론

철도, 발전소 등의 국가기반시설은 과학기술이 발달함에 따라 국민의 편의성 증대를 위해 꾸준히 발전해 왔다. 그에 따라 현대의 시스템은 점차 대형화되고 복잡화되었으며, 시스템을 구성하는 부품 또한 기계 중심에서 전기/전자/소프트웨어 중심으로 바뀌게 되었다. 이러한 변화는 이용자의 편의성을 증대시키는 효과를 가져왔지만, 반대로 시스템의 고장으로 인

† 교신저자: 아주대학교 시스템공학과(rila4@ajou.ac.kr)

* 아주대학교 시스템공학과

한 안전사고의 위험성도 함께 증가시켰다. 따라서, 안전사고 발생시 국민의 생명과 재산 상에 큰 피해를 입히는 안전중시시스템의 경우, 시스템의 안전성 확보는 선택이 아닌 필수가 되었다. 이를 반영하여 다양한 산업 군에서는 안전표준을 제정하여 시스템 개발시 초기의 개념설계 단계부터 위험원 분석을 수행하여 그 결과를 시스템의 설계 변경에 활용할 것을 요구한다. 하지만 기존의 위험원 분석은 상세설계 단계부터 주로 수행되었기 때문에, 개념설계 단계에서 위험원 분석을 수행하기에는 시스템 설계가 완전하지 않다는 어려운 점이 있다. 또한 위험원 분석을 수행했더라도 결과를 시스템의 설계 변경에 반영하기 위해서는 먼저 그 분석이 정확하였는지 검증하는 과정이 필요한데, 개념설계 단계의 경우에는 위험원 분석의 검증 또한 어려운 점이 사실이다.

이러한 점을 해소하고 개념설계 단계에서의 안전성을 확보하기 위한 접근방법 중 하나가 모델 기반 위험원 분석이다. 모델 기반 위험원 분석이란, 위험원 분석과 그 결과에 대한 검증, 그리고 이를 시스템의 설계 변경에 반영하는 일련의 과정을 모두 모델을 기반으로 수행하는 방법을 말한다. Papadopoulos 등 [1][2]은 시스템 아키텍처의 계층 수준에 따라 FHA와 FMEA, FTA의 기법을 적용하여 위험원 분석을 수행하였다. Simulink 등의 도구를 활용하여 시스템 아키텍처를 생성하였고, 이에 대해 Isograph 등의 도구를 활용하여 위험원 분석을 수행 하였다. 하지만 위험원 분석 전용 도구를 사용했다는 점에서 진정한 의미의 모델 기반 위험원 분석은 아니다. Sharvia와 Papadopoulos [3], Joshi 등 [4][5]은 시스템 아키텍처에 대한 위험원 분석의 결과를 검증하기 위해 분석 결과를 토대로 시스템 고장 모델을 생성하였다. 그리고 생성한 고장 모델을 Model Checking 도구인 NuSMV를 활용해 시뮬레이션 함으로써 위험원 분석을 검증하였다. Ariss 등 [6]과 Cressent 등[7]은 위험원 분석 기법을 모델 기반으로 수행하기 위해서 각각 sheet형태의 FTA와 FMEA를 SysML 모델 형태로 변환하는 방법을 제시하였다. 이는 위험원 분석을 Isograph 등의 전용 도구가 아닌 모델로 수행함으로써, 위험원 분석의 결과를 추후 시스템의 설계 변경에 효과적으로 활용하기 위함이다.

위험원 분석은 정확한 결과가 시스템의 설계 변경에 활용되어야 그 의미가 있으며, 이를 위해 모델 기반 위험원 분석 기법이 효과적으로 활용될 수 있다. 하지만 현재의 모델 기반 위험원 분석 기법은 두 가지 문제가 있다. 첫째, 대부분이 모델 기반으로 분석한 것이 아닌 위험원 분석 전용 도구를 사용한 후 결과만 모델로 표현하였다. 또한 Ariss 등 [6]과 Cressent 등[7]은 모델을 기반으로 위험원 분석을 수행하였지만, FTA, FMEA와 같이 제한된 기법에만 적용할 수 있다. 둘째, 현재의 모델 기반 위험원 분석은 결과를 검증하는 과정에서 시스템 고장 모델을 생성하여 이를 시뮬레이션 하는데, 대부분이 시스템 아키텍처는 배제한 채 시스템 고장 모델에 대한 시뮬레이션만을 수행한다. 이 경우, 고장이 시스템의 전체 성능 또는 안전에 미치는 영향을 검증하기가 어려운 점이 있다. 따라서 본 논문에서는 먼저 특정 위험원 분석 기법이 아닌 일반적인 위험원 분석 모델을 SysML로 정의하였다. 그리고 나서 위험원 분석의 결과로 시스템 고장 모델을 생성하여 시스템 아키텍처에 통합한 후, 시뮬레이션을 통해 고장이 시스템 전체에 미치는 영향을 검증하였다.

본 논문의 구성은 다음과 같다. 1장에서는 모델 기반 위험원 분석의 연구동향과 필요성에

대해 기술하였고, 2장에서는 SysML을 활용한 시스템 아키텍처, 위험원 분석 모델, 시스템 고장 모델의 생성 방법에 대해 기술하였다. 3장에서는 2장에서 생성한 모델들을 통합하여 SysML 기반의 시뮬레이션을 수행하였다. 4장에서는 본 논문의 결과를 요약 및 정리하였다.

2. SysML 기반 시스템 고장 모델의 생성

2.1 연구수행 절차

현재의 모델 기반 위험원 분석은 약간의 차이가 있지만 대부분 공통적인 절차로 수행되며, 본 논문의 연구수행 절차도 이를 따르고 있다. 다만 본 논문에서는 모든 과정을 SysML 기반으로 수행한다는 차이점이 있다. 본 논문의 구체적인 연구수행 절차는 먼저 대상시스템의 시스템 아키텍처를 SysML 기반으로 모델링 한다. 그 후 시스템 아키텍처에 대한 위험원 분석을 모델 기반으로 수행하기 위해, 위험원 분석 기법에서 공통적으로 다루는 정보를 식별하여 일반적인 위험원 분석 모델을 정의한다. 모델 기반 위험원 분석을 수행한 후, 분석 결과를 검증하고 시스템의 설계 변경에 활용하기 위해 시스템 고장 모델을 정의한다. 마지막으로 시스템 고장 모델이 반영된 시스템 아키텍처를 시뮬레이션 함으로써 모델 기반 위험원 분석에 대한 검증을 수행한다. 구체적인 연구수행 절차와 방법은 Fig.1 과 같다.

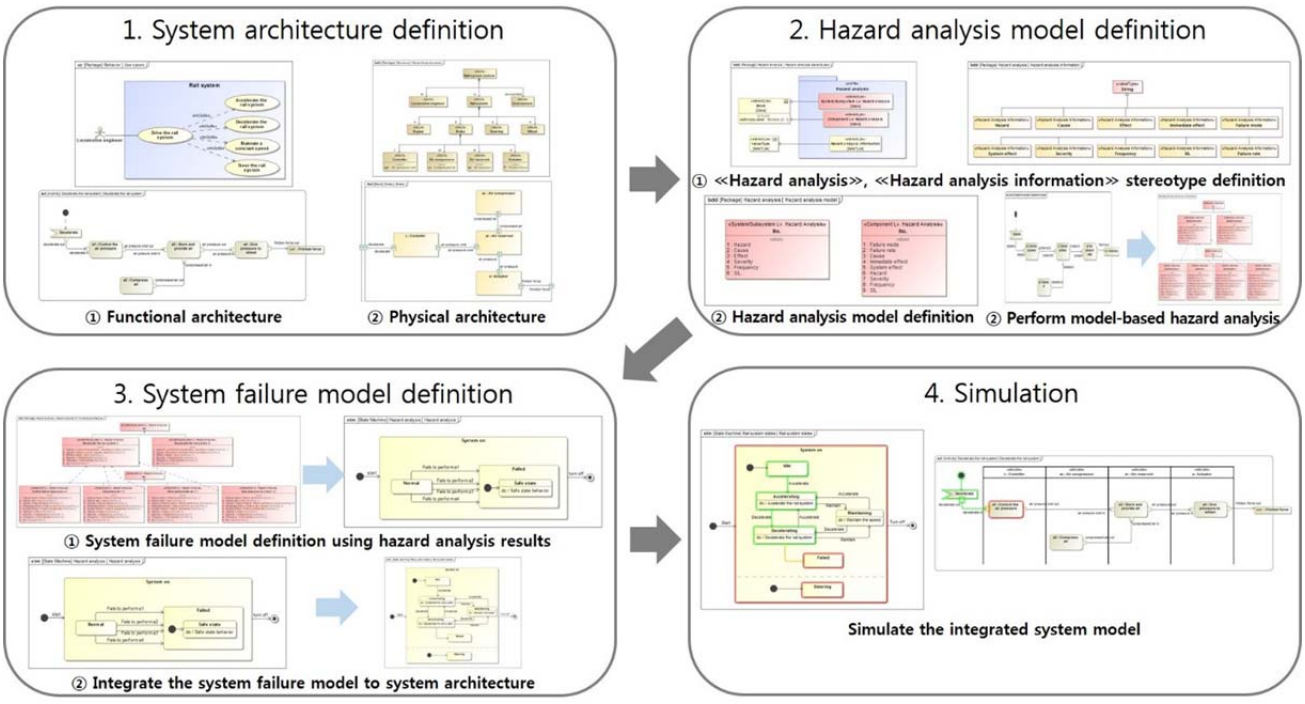

Fig. 1 The verification process of systems failure models using SysML-based M&S methods

2.2 시스템 아키텍처 모델링

본 논문에서는 모델 기반 위험원 분석을 수행하기 위해 철도의 공기 브레이크 시스템을 대상 시스템으로 선정하였다. 철도 공기 브레이크 시스템의 시스템 아키텍처를 정의하기 위해, 먼저 대상 시스템의 최상위 기능인 “Decelerate the rail system”을 식별 및 정의하였다. 그리고 이 기능을 달성하기 위한 구체적인 하위 기능인 “Control the air pressure”, “Compress air”, “Store and provide air”, “Give pressure to wheel”을 정의한 후, Block definition diagram을 통해 기능의 계층 구조를 표현하였다. 그리고 Activity diagram을 통해 하위 기능 사이의 제어 흐름과 정보의 입출력을 정의하여 인터페이스를 표현하였다. 기능의 목록과 흐름을 정의한 다음에는 각 기능을 수행할 물리 구성품을 Block definition diagram에 정의한 후, 계층 구조로 표현하였다. 그리고 앞서 정의한 기능들을 해당 Block에 할당하고, 물리 구성품 사이의 인터페이스는 Internal block diagram으로 정의하였다. 대상시스템의 기능/물리 아키텍처를 생성한 결과는 Fig.2와 같다.

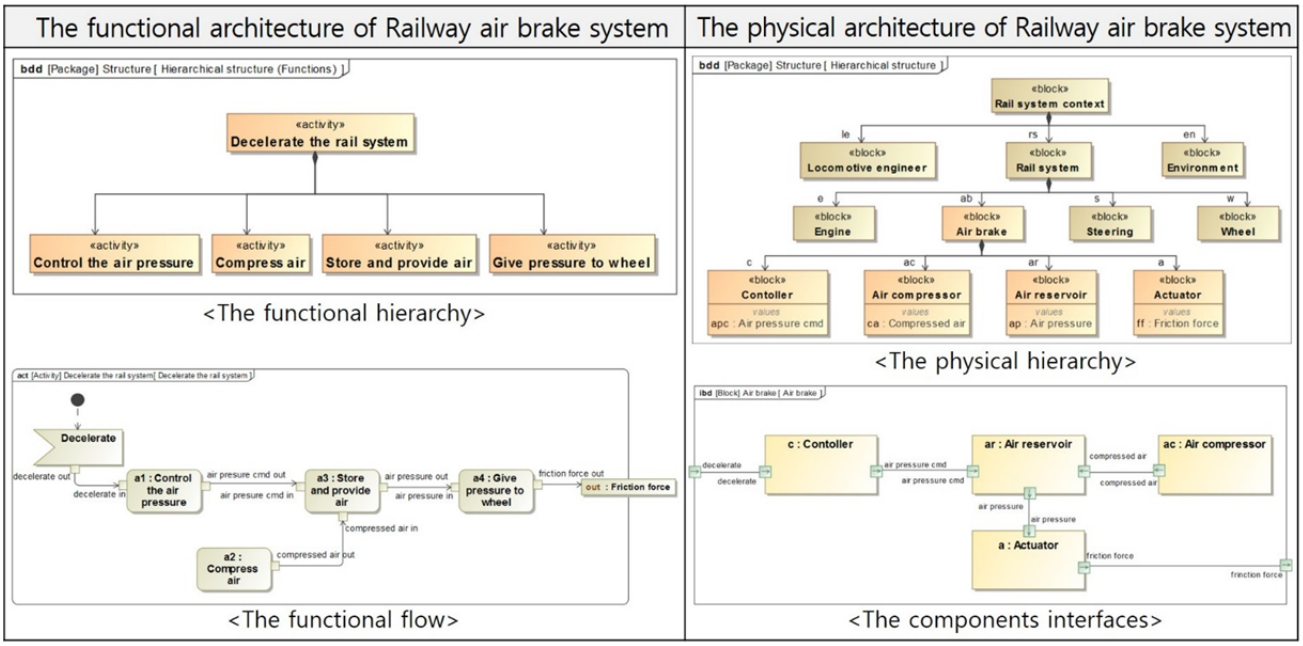

Fig. 2 The system architecture of Railway air brake system

2.3 모델 기반 위험원 분석을 위한 필수 요소 식별 및 모델링

위험원 분석 기법에는 다양한 종류가 있다. 이 기법들은 위험원 분석을 수행하는 수명주기상의 단계, 분석 대상(기능 또는 구성품), 분석 대상의 계층 수준에 따라서 선택적으로 활용된다[14]. 이렇듯 다양한 위험원 분석 기법들을 모두 모델 기반으로 수행하려면 각각에 맞는 위험원 분석 모델을 생성해야 한다는 점에서 한계가 있다. 예를 들어 Ariss 등 [6]과 Cressent 등 [7]은 각각 FTA와 FMEA를 모델 기반으로 수행하는 방법을 제시하였지만, 다른 기법을 모델 기반으로 수행하려면 새로운 위험원 분석 모델을 재정의해야 한다. 그러므로

각 계층 수준별로 적용되는 위험원 분석 기법들을 나누고, 분류별 기법들에서 공통적으로 다루는 정보를 식별하여 일반적인 위험원 분석 모델을 만든다면 다양한 분석을 이 모델을 통해 수행할 수 있다. 이를 위해 먼저 계층 수준별로 적용되는 위험원 분석 기법들을 분류하고, 각 분류별 기법들에서 공통적으로 다루는 정보를 식별하였다.

이 정보를 모델로 표현하기 위해서 SysML을 활용하여 Block의 stereotype인 ≪System/Subsystem Lv. Hazard Analysis≫, ≪Component Lv. Hazard Analysis≫를 정의하고, Value의 stereotype인 ≪Hazard Analysis Information≫을 Fig.3의 왼쪽과 같이 정의하였다. 그리고 앞서 식별한 공통의 정보들을 ≪Hazard Analysis Information≫ stereotype으로 정의하고, 정의한 ≪Hazard Analysis Information≫을 ≪System/Subsystem Lv. Hazard Analysis≫, ≪Component Lv. Hazard Analysis≫ stereotype의 속성값으로 Fig.3.의 오른쪽과 같이 반영하여 두 계층의 위험원 분석 모델을 정의하였다. 생성된 두 개의 모델은 일반적인 모델로 이를 Generalization path로 상세화하여 구체적인 위험원 분석을 수행할 수 있다. Fig.4는 ≪System/Subsystem Lv. Hazard Analysis≫ stereotype을 활용하여 시스템 수준의 기능인 “Decelerate the rail system”에 대한 위험원 분석을 수행한 결과이다.

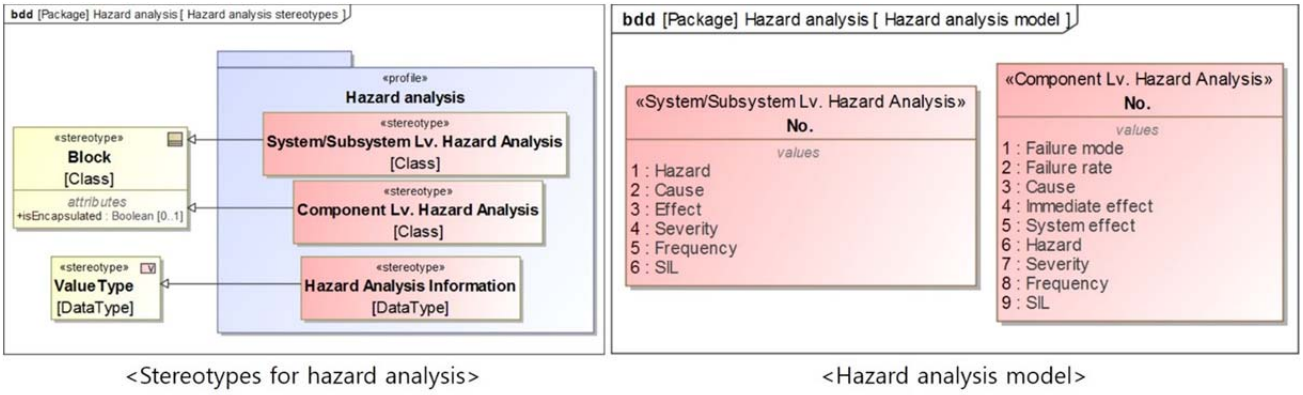

Fig. 3 The hazard analysis models

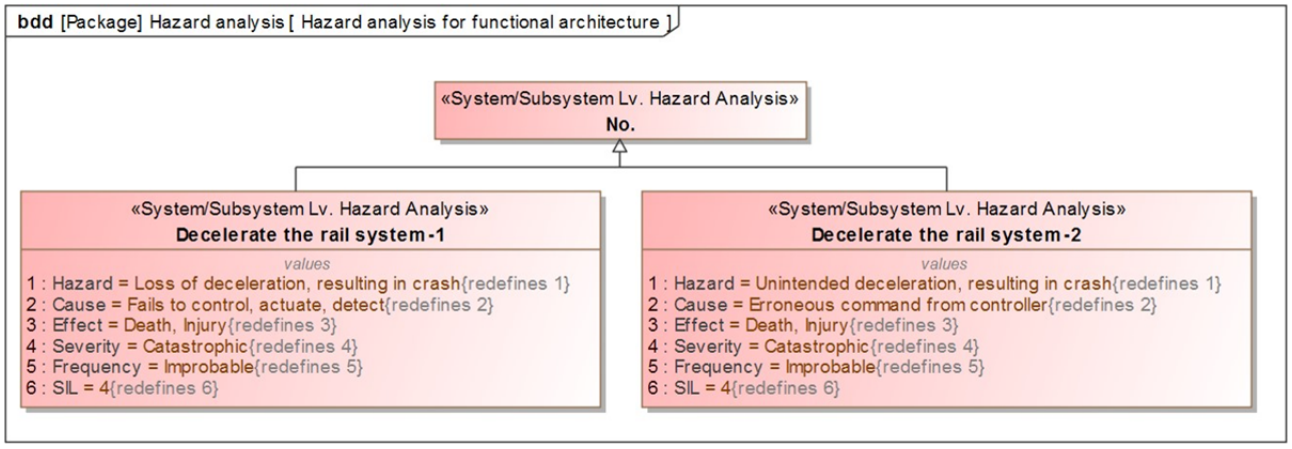

Fig. 4 The results of system/subsystem level hazard analysis using the hazard analysis models

2.4 모델 기반 위험원 분석의 결과를 활용한 시스템 고장 모델의 생성

≪Component Lv. Hazard Analysis≫ stereotype을 활용하여 컴포넌트 수준의 위험원 분석도 수행하게 되면, 앞서 수행한 시스템 수준의 위험원 분석 결과와 비교하여 고장 유형과 고장 원인에 대한 인과관계를 식별할 수 있다. 이를 Fig.5와 같이 dependency path를 통해 표현하면 효과적으로 고장의 인과관계를 식별할 수 있다. 이제 모델 기반 위험원 분석의 결과를 검증하고 효과적으로 시스템의 설계 변경에 활용하기 위해서 시스템 고장 모델을 생성해야 한다. 그 방법으로 SysML diagram에서 state machine diagram을 활용한다. 고장 유형을 state node로, 고장 원인을 transition path의 event로 변환하는 방법을 통해 시스템 고장 모델을 state machine diagram으로 정의할 수 있다[2][3].

앞서 “Decelerate the rail system”의 위험원인 “Loss of deceleration”의 원인은 하위 기능(a1~a4)의 고장과 관련 있음이 컴포넌트 수준의 위험원 분석을 통해 식별되었다. 따라서 “Loss of deceleration”을 state node로 정의하고, 하위 기능(a1~a4)의 고장을 Normal state와 Failed state를 연결하는 transition path의 event로 할당하였다. Fig.6은 시스템 고장 모델의 생성 결과이다.

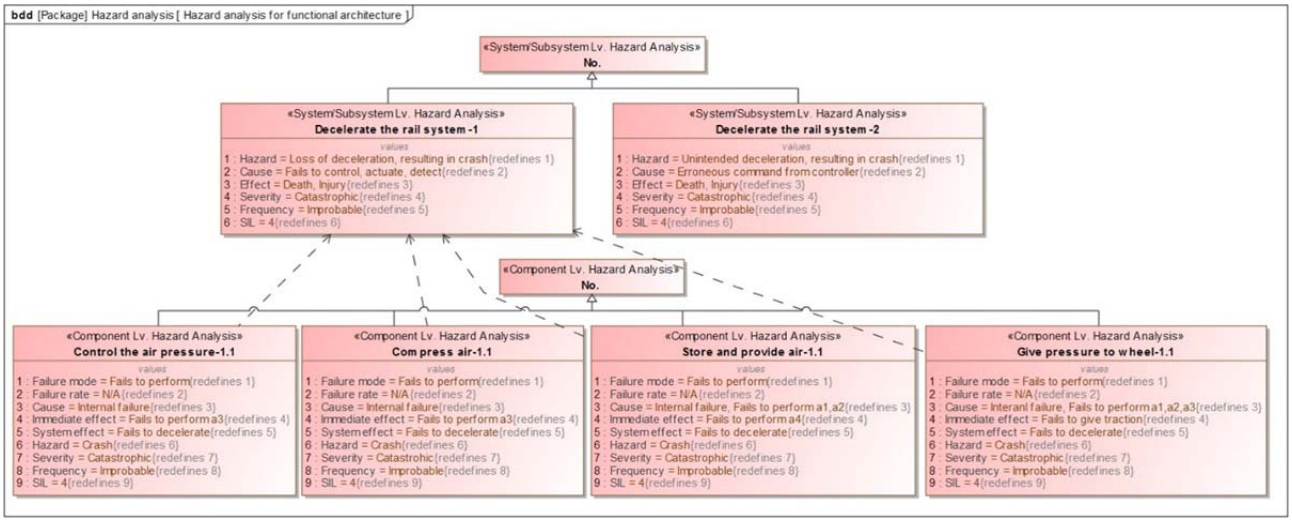

Fig. 5 The definition of relationships between failure and causal factors

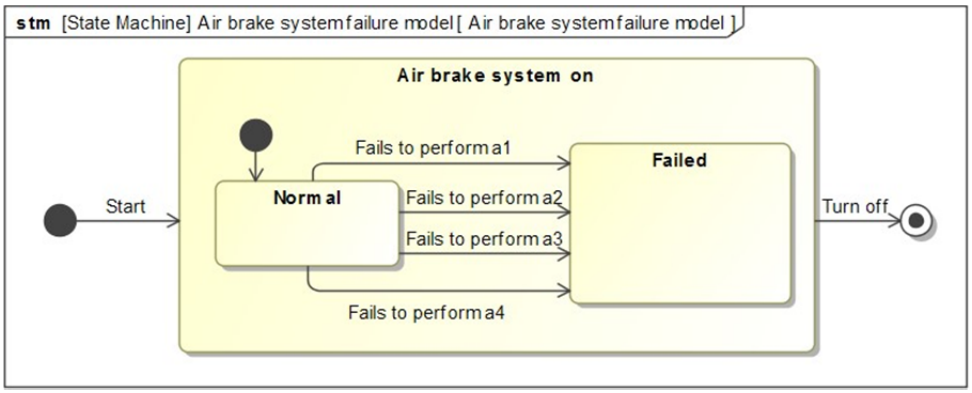

Fig. 6 The systems failure model of Railway air brake system

3. SysML 기반 시스템 고장 모델의 시뮬레이션 수행

3.1 시스템 아키텍처와 시스템 고장 모델의 통합

생성한 시스템 고장 모델만으로도 Model Checking 도구인 NuSMV를 통해 시뮬레이션을 수행할 수 있지만[3][5][8], 이 경우에는 고장이 시스템 전체의 기능과 성능에 어떠한 영향을 미치는지 검증하기가 어렵다. 시스템이 정상적인 기능을 수행하는 과정에서 고장이 발생했을 때, 시스템의 전체 성능에 미치는 영향, 그리고 저하된 성능이 최소한의 안전/성능 요구사항을 만족하는지 검증하기 위해서는 기존의 시스템 아키텍처에 시스템 고장 모델을 통합시켜 시스템 전체에 대한 시뮬레이션을 수행해야 한다.

앞서 정의한 시스템 아키텍처와 시스템 고장 모델은 모두 철도의 공기 브레이크 시스템이 대상인데, 이것은 철도시스템의 서브시스템에 해당한다. 따라서 시스템 수준의 거동 모델 중 하나인 state machine diagram에서 composite state의 하위에 있는 sub-state "Decelerating"에 Fig.6의 시스템 고장 모델을 통합하여 다시 모델링 하였다. 통합된 모델의 결과는 Fig.7의 왼쪽과 같다.

3.2 시뮬레이션을 통한 시스템 고장 모델의 검증

SysML 기반의 시뮬레이션으로 시스템 고장 모델에 대해 검증할 수 있는 것은 크게 두 가지이다. 첫째는 시스템의 기능이 원래 목표에 따라 정상적으로 거동하는지 검증하는 거동 시뮬레이션이다. 둘째는 시스템이 정상 또는 고장 상태에서 최소한의 성능 또는 제약 요구사항을 만족하는지 검증하는 시뮬레이션이다. 후자의 경우에는 시스템의 성능 또는 제약과 관련된 수식을 parametric diagram의 constraint property node에 정의하고, 이를 구성하는 constraint parameter node를 Block의 value property와 연결하는 모델링이 추가적으로 필요하다. 본 논문에서는 전자인 시스템의 거동과 관련된 시뮬레이션을 수행하였고, 시스템이 정상적으로 작동하는 중에 컴포넌트 수준에서 고장이 발생하게 되면 시스템 전체의 거동에 어떠한 영향을 미치는지 시뮬레이션 하였다. 시뮬레이션을 수행한 후에는 고장 상태에서의 안전성 확보를 위해 Watch dog event와 safe state를 Fig.7의 왼쪽과 같이 추가하였다.

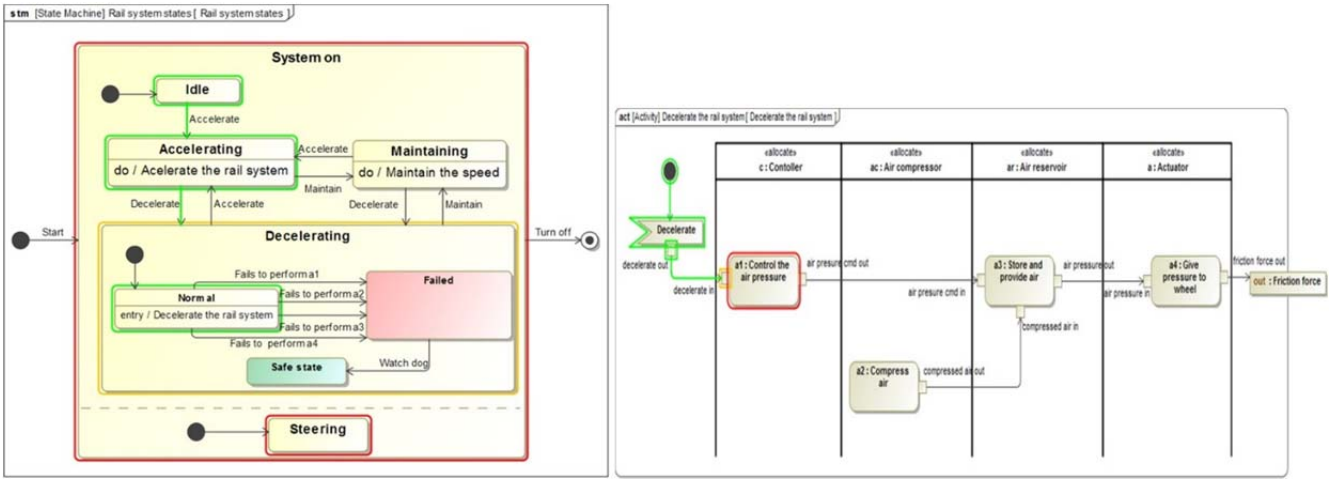

Fig. 7 The SysML-based simulation of the integrated system architecture

4. 결론

현대의 안전중시시스템은 개발 초기단계부터 체계적인 위험원 분석을 통해 위험원을 식별하고, 안전사고에 대한 리스크를 낮추기 위해 위험원 분석의 결과를 시스템의 설계 변경에 활용해야 한다. 위험원 분석의 결과를 효과적으로 설계 변경에 활용하기 위한 접근방법 중 하나가 모델 기반 위험원 분석이다. 이는 위험원 분석을 모델 기반으로 수행하면 분석의 결과를 시뮬레이션을 통해 검증할 수 있기 때문에 효과적이다. 이때, 위험원 분석의 결과를 검증하기 위해 생성하는 것이 시스템 고장 모델이며, 이를 시뮬레이션 함으로써 분석이 제대로 수행되었는지 확인하고 설계 변경에 활용할 수 있다.

본 논문에서는 시스템 고장 모델을 생성하고 시뮬레이션 하기 위해, 먼저 SysML을 기반으로 일반적인 위험원 분석 모델을 정의하여 시스템 아키텍처에 대한 위험원 분석을 수행하였다. 그리고 그 결과를 토대로 시스템 고장 모델을 state machine diagram으로 정의하였고, 이를 기존의 시스템 아키텍처에 통합한 후 고장이 시스템의 전체 기능에 미치는 영향을 거동 관점에서 시뮬레이션 하였다. 향후 거동 시뮬레이션을 진전시켜서, 시스템이 고장 상태에서도 최소한의 안전/성능 요구사항을 만족하는지 SysML 기반 시뮬레이션을 통해 검증하는 연구를 수행할 필요가 있다.

참고문헌

[1] Y. Papadopoulos, J. McDermid, R. Sasse, G. Heiner (2001) Analysis and synthesis of the behaviour of complex programmable electronic systems in conditions of failure, *Reliability Engineering and System Safety*, 71(3), pp. 229–247.

[2] Y. Papadopoulos, C. Grante (2015) Evolving car designs using model-based automated safety analysis and optimisation techniques, *Journal of Systems and Software*, 76(1), pp. 77–89.

[3] S. Sharvia, Y. Papadopoulos (2015) Integrating Model Checking with HiP-HOPS in Model-Based Safety Analysis, *Reliability Engineering and System Safety*, 135, pp. 64-80.

[4] A. Joshi, M. Whalen, M. Heimdahl (2006) Model-Based Safety Analysis Final Report, NASA, NASA/CR-2006-213953.

[5] A. Joshi (2009) Behavioral fault modeling and model composition for model-based safety analysis, Ph.D. dissertation, The University of Minnesota.

[6] O.E. Ariss, D. Xu, W.E. Wong (2011) Integrating safety analysis with functional modeling, *IEEE Transactions on Systems, Man and Cybernetics*, 41(4), pp. 610-624.

[7] R. Cressent, P. David, V. Idasiak, F. Kratz (2013) Designing the database for a reliability aware Model-Based System Engineering process, *Reliability Engineering and System Safety*, 111, pp. 171-182.

[8] F. Mhenni (2014) Safety analysis integration in a systems engineering approach for mechatronic systems design, Ph.D. dissertation, Ecole Centrale Paris.

[9] L. Rogovchenko-Buffoni, A. Tundis, M.Z. Hossain, M. Nyberg, et al. (2014) An integrated toolchain

for model based functional safety analysis, *Journal of Computational Science*, 5(3), pp. 408–414.

[10] S. Friedenthal, A. Moore, R. Steiner (2015) *A Practical Guide To SysML*, Elsevier, Waltham, MA.

[11] R.C. Sharma (2015) Braking Systems in Railway Vehicles, *International Journal of Engineering Research & Technology*, 4(1), pp. 206-211.

[12] Z. Yu, L. Zhao (2010) The Study on electric-pneumatic transfer control of the train brake system, *2010 IEEE International Conference on Intelligent Computing and Intelligent Systems*, Xiamen, China, pp. 388–392.

[13] X. Perpinya (2012) *Reliability and Safety in Railway*, InTech, Rijeka, Croatia, pp. 29-74.

[14] C.A. Ericson (2015) *Hazard Analysis Techniques for System Safety*, Wiley, Hoboken, NJ, 2015.