Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 8 pp. 77-83, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.8.77
ISSN 1975-4701 / eISSN 2288-4688

SysML 기반 시스템 고장 모델과 시스템 아키텍처의 통합 모델에 대한 검증 기법

조정호, 이재천*
아주대학교 시스템공학과

A Verification Method for the Integrated Model Combining SysML-Based System Failure Model and System Architecture

Jeong-Ho Jo, Jae-Chon Lee*
Dept. of Systems Engineering, Ajou University

요 약 오늘날 다양한 산업분야에서는 시스템 안전을 확보하기 위한 표준들이 제정되었다. 해당 표준들에서는 시스템 개발 초기 단계인 개념설계 단계부터 위험원 분석 활동을 수행하고, 분석 결과를 안전을 확보하기 위한 시스템 설계 활동에 반영할 것을 제시하고 있다. 따라서 운영 목표에 부응하는 시스템의 설계와 시스템에 내재하는 위험원 분석은 밀접한 관계가 있다. 그럼에도 불구하고 기존에는 설계 결과의 검증에서 시스템 개념설계와 위험원 분석 결과를 분리하여 수행하였다. 본 논문에서는 분리 수행에 따른 문제를 개선하기 위하여 시스템 고장 모델과 시스템 아키텍처의 통합 모델에 대한 검증 방법을 연구하였다. 구체적으로, 먼저 대상시스템의 아키텍처를 시스템 모델링 언어인 SysML로 모델링 하였다. 그리고 나서 시스템 아키텍처 정보를 기반으로 위험원 분석을 수행하고, 이를 토대로 SysML 고장 모델을 생성하였다. 그 후에 시스템 고장 모델을 시스템 아키텍처에 통합하고, 이를 기반으로 고장에 대비한 안전 설계를 추가하였다. 최종적으로 시스템 운영 중 일부 고장에도 안전 설계 결과가 안전 목표를 만족하는지 검증하기 위한 시뮬레이션을 수행하였다.

Abstract International standards for systems safety have been established in various areas of industry. Such standards recommend that safety design activities be carried out early on in the beginning of systems development. Hazard analysis should be done in close interaction with the conceptual design of the system. This paper focuses on how to verify whether the safety goals are met while considering system design issues. The architecture of the underlying system was first modeled using SysML, a systems modeling language, and then hazard analysis was performed based on architectural information to obtain a system failure model. Thereafter, an integrated model was developed by combining the SysML failure model and the architectural model, and then safety designs were added to prevent system failure. Finally, a simulation of the developed model was performed to see if a system functions even when some components are failing.

Keywords : Functional Safety, Hazard Analysis, Model-Based Safety Analysis, SysML, Systems Engineering

1. 서론

현대의 시스템은 기술이 발전함에 따라 시스템의 효율성과 사용자의 편의성을 증진시키기 위해 지속적으로 발전되어 왔다. 이로 인해 하나의 시스템이 다수의 기능을 수행하도록 시스템이 변화되었고, 자연스레 시스템을 구성하는 부품 또한 기계 중심에서 전기/전자/소프트웨어 중심으로 바뀌게 되었다. 이와 같은 변화는 효율성과

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 July 14, 2016 Revised August 2, 2016
Accepted August 11, 2016 Published August 31, 2016

편의성 측면에서는 많은 이점을 가져왔지만, 반대로 시스템의 복잡성은 증가하게 되면서 안전성에 대한 우려를 가져오게 되었다. 특히, 안전사고 발생 시에 국민의 생명과 재산상에 큰 피해를 입히는 안전중시시스템의 경우, 안전성 문제는 반드시 해결해야 할 과제가 되었다. 이러한 문제를 고려하여 국방, 항공, 철도, 자동차 등의 다양한 산업 군에서는 안전표준을 발행하여 시스템 개발 시 안전성을 확보하기 위한 지침을 제시하였다. 안전표준들은 조금씩의 차이는 있지만, 공통적으로 시스템 개발 초기인 개념설계 단계부터 위험원 분석을 수행하여 결과를 안전 설계에 활용할 것을 제시하고 있다.

개념설계에 대한 위험원 분석을 체계적으로 수행하고 결과를 안전 설계에 효과적으로 활용하기 위해 제시되는 방법 중 하나가 모델 기반 접근방법이다. 이는 개념설계에 대해 수행하는 위험원 분석과 결과의 검증, 문서 산출 등에 모델을 활용하는 접근방법을 말한다. 기존에 문서 중심으로 수행되어온 위험원 분석에 비해서 보다 일관성 있고 체계적으로 시스템 설계와 위험원 분석을 함께 수행할 수 있고, 시뮬레이션을 통해 결과를 검증을 할 수 있으며, 자동으로 문서를 산출할 수 있다는 이점이 제시되었다.

이를 위해서는 우선적으로 시스템 설계와 위험원 분석 산출물을 모델 기반으로 연계하는 연구가 필요하였다. 따라서 개념설계가 진행됨에 따라 시스템 계층 수준별로 위험원 분석을 수행하고, 결과를 설계에 다시 반영하는 프로세스와 방법론이 제시되었다[1,2]. 이처럼 식별된 고장 정보를 시스템 아키텍처에 통합하게 되면, 도구의 연동을 통해 위험원 평가 및 문서 산출을 용이하게 할 수 있음을 강조하였다.

또한, 이와 같은 프로세스와 방법론을 적용한 위험원 분석을 검증하기 위해, 고장 모델을 생성하고 Model checking을 수행하는 방법이 제시되었다[3,4,5]. Model checking 도구로는 NuSMV를 사용하였는데, 시스템의 고장 모델에 오류가 있는 경우에는 산출된 반례를 기반으로 오류를 수정하고 다시 위험원 분석을 수행할 수 있음을 강조하였다.

개념설계의 위험원 분석 과정에서 모델을 활용한 연구들의 추세를 살펴보면, 앞서 언급한 것과 같이 마지막 검증 단계에서 고장 모델에 대해 Model checking을 수행한다. 하지만 위험원 분석을 실제적인 시스템 설계 관점에서 검증하기 위해서는, 고장 모델을 시스템 아키텍처에 통합한 모델에 대한 검증이 추가적으로 수행되어야 한다.

본 논문에서는 개념설계에 대해 수행한 위험원 분석을 시스템 설계와 함께 체계적으로 검증하기 위해, SysML[6,7]을 활용한 M&S 방법론을 연구하였다. 이를 위해 먼저 대상 시스템을 선정하고 시스템 아키텍처를 정의하였다. 그리고 위험원 분석을 수행하여 고장 모델을 정의하고, 이를 시스템 아키텍처에 통합하여 시뮬레이션을 수행하였다. 시뮬레이션을 통해 시스템의 하위 컴포넌트에 고장이 발생하여도 시스템이 시스템 요구사항을 만족하는지 검증하였다.

본 논문의 구성은 다음과 같다. 1장에서는 위험원 분석에서 모델 기반 접근방법의 필요성과 연구동향에 대해 기술하였고, 2장에서는 선행연구에 대한 문제정의와 연구목표, 범위와 방법을 기술하였다. 3장에서는 SysML을 활용한 시스템 고장 모델의 생성 방법을 기술하였고, 4장에서는 시스템 고장 모델을 시스템 아키텍처에 통합하여 시뮬레이션을 통해 검증하는 방법을 제시하였다. 5장에서는 제시한 방법론을 적용하여 수행한 자동차 브레이크 시스템의 Case study를 기술하였다. 마지막으로 6장에서는 본 논문의 연구수행 결과와 공헌을 정리하였다.

2. 시스템 고장 모델 검증의 필요성

2.1 모델 기반 위험원 분석의 절차

기존의 모델 기반 위험원 분석을 종합해 보면 그 절차는 다음과 같이 4단계로 구분할 수 있다. 첫째, 시스템 아키텍처의 생성이다. 위험원 분석을 수행할 대상으로 시스템 아키텍처가 정의되어 있어야 한다. 둘째, 위험원 분석의 수행이다. 시스템의 고장 유형과 영향을 식별 및 평가하기 위해서 시스템 아키텍처에 대해 위험원 분석을 수행하고, 결과를 모델에 반영한다. 셋째, 고장 모델의 생성이다. 위험원 분석 결과를 검증하고 안전 설계에 활용하기 위해서 분석 결과를 기반으로 시스템 고장 모델을 생성한다. 넷째, Model checking을 통한 고장 모델의 검증이다. 생성한 시스템 고장 모델에 오류가 있는지 검증하기 위해서 도구를 통한 Model checking을 수행한다[3,4,5].

2.2 M&S 기법을 통한 시스템 고장 모델 검증의 필요성

앞서 모델을 활용한 위험원 분석 기법은 결과를 고장 모델을 통해 검증할 수 있으며, 대부분의 연구에서 NuSMV 도구를 통해 Model checking을 수행한다고 언급했다[3,4,5]. 하지만 이 경우에는 고장이 시스템 설계에 미치는 영향을 검증하기가 어렵다. 따라서 기존의 검증 기법과 더불어 고장 모델을 통합한 시스템 아키텍처를 시뮬레이션 함으로써, 하위 컴포넌트에 고장이 발생하여도 시스템이 시스템 요구사항을 만족하는지 검증할 필요가 있다.

따라서 본 논문에서는 시스템 아키텍처의 위험원 분석으로 산출한 고장 모델을 시스템 설계와 함께 체계적으로 검증하기 위해, SysML을 활용한 M&S 방법론을 제안하고자 한다.

2.3 연구수행 방법 및 절차

본 논문의 연구수행 절차는 2.1에 기술한 기존 절차를 전반적으로 따른다. 다만 모든 절차를 SysML 기반으로 수행하였고, 고장 모델을 시스템 아키텍처에 통합하여 시뮬레이션을 통해 검증한 것이 차이점이다. Fig. 1은 본 논문의 M&S 절차를 나타낸다.

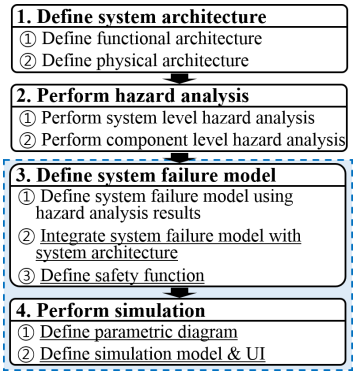


Fig. 1. M&S process proposed in the paper to verify safety design

3. SysML 기반 시스템 고장 모델의 생성

3.1 시스템 아키텍처의 생성

시스템 아키텍처는 기능 아키텍처와 물리 아키텍처로 구성된다. 본 논문에서는 향후 정의할 고장 모델과의 통합을 고려하여, 기능 아키텍처를 SysML의 State machine diagram(이하 stm)과 Activity diagram(이하 act)으로 정의할 것을 제시한다. 먼저 stm으로 시스템 수준의 기능(상태)를 정의한 후에, 이 기능(상태)을 수행하기 위해 필요한 하위 기능들을 act로 정의하여 stm과 연동한다. 그리고 Block definition diagram(이하 bdd)을 통해 기능들을 직접적으로 수행할 물리 구성품과 속성, 계층구조, 시스템의 성능/제약과 관련된 수식을 Block과 Constraint block 등으로 정의한다.

3.2 위험원 분석을 통한 시스템 고장 모델의 생성

대상 시스템(시스템 아키텍처)에 대해 시스템 수준에서 컴포넌트 수준까지 위험원 분석을 수행하면, 고장 유형과 원인, 영향 등을 식별할 수 있다. 식별된 고장의 인과관계는 고장 모델의 생성에 활용되며, 고장 모델을 통해 위험원 분석을 검증할 수 있다.

고장 모델은 stm으로 정의할 수 있다[4,5]. stm은 대상의 상태전이를 나타내는 다이어그램으로, 크게 State와 Transition으로 구성된다. 따라서 고장 유형은 State, 고장 원인은 Transition의 Trigger(Event)로 정의하여 고장 모델을 생성할 수 있다. Fig. 2는 stm을 활용한 일반적인 고장 모델을 나타낸다.

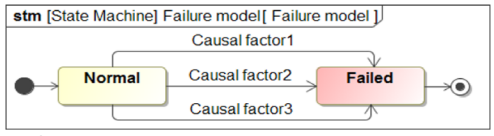


Fig. 2. A generic failure model.

4. 시뮬레이션 기법을 통한 시스템 고장 모델의 검증

4.1 시스템 고장 모델과 시스템 아키텍처의 통합

3장에서 생성한 두 모델을 통합하는 모델링 기법과 절차는 2단계로 제시할 수 있다. 첫째, 기능 아키텍처로 정의한 시스템 수준의 stm에 고장 모델로 정의한 stm을 통합한다. 구체적으로, 기능 아키텍처로 정의했던 stm의 States 중에서 고장 모델과 직접적으로 관련 있는 State의 Sub-state로 고장 모델을 통합시킨다. 둘째, 통합된 모델에 안전 상태를 추가하고[5], 세부적인 안전 기능을

act로 모델링하여 안전 상태와 연동한다. 구체적으로, 안전 상태인 Degraded state를 Normal state와 Failed state 사이에 추가하여 컴포넌트의 고장이 시스템의 고장으로 이어지지 않도록 stm을 모델링한다. 그리고 안전 기능을 수행하는 세부 기능과 거동을 act로 모델링한 후, Degraded State와 연동함으로써 두 모델의 통합과 안전 설계를 달성할 수 있다. Fig. 3은 고장 모델과 시스템 아키텍처의 통합 절차 및 방법을 나타낸다.

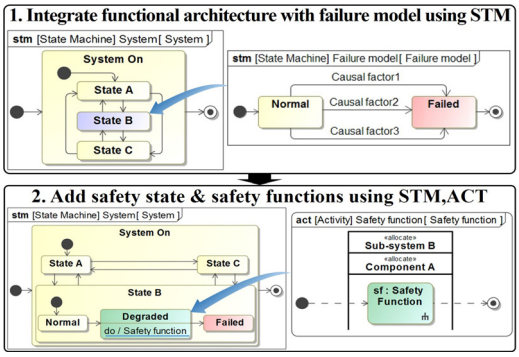


Fig. 3. The process model for the integration of failure model and architecture and the addition of safety measure.

4.2 시뮬레이션을 통한 통합 모델의 검증

통합된 시스템 아키텍처를 SysML 기반으로 시뮬레이션 하기 위해서는 Parametric diagram(이하 par)을 정의해야 한다. par를 통해 앞서 bdd에서 정의한 Constraint block의 성능을 대상 시스템이 만족하는지 정량적으로 검증 할 수 있다. Constraint blocks의 수식을 구성하는 파라미터는 Blocks의 관련된 속성(Value)과 par를 통해 연결할 수 있으며, 시뮬레이션을 수행하게 되면 Blocks가 가진 속성 값이 수식의 파라미터에 입력 값으로 들어가게 되어 목표하는 성능을 정량적으로 평가할 수 있다.

par를 정의한 후에는 추가적으로 시뮬레이션에 필요한 모델 요소 및 UI를 정의한 후, 시뮬레이션을 수행한다. 그리고 시뮬레이션이 수행되는 중에 앞서 식별한 고장 상황을 UI를 통해서 부여한다.

5. Case study: 자동차 브레이크 시스템

5.1 시스템 아키텍처 및 고장 모델의 생성

본 논문에서는 자동차 브레이크 시스템을 대상으로

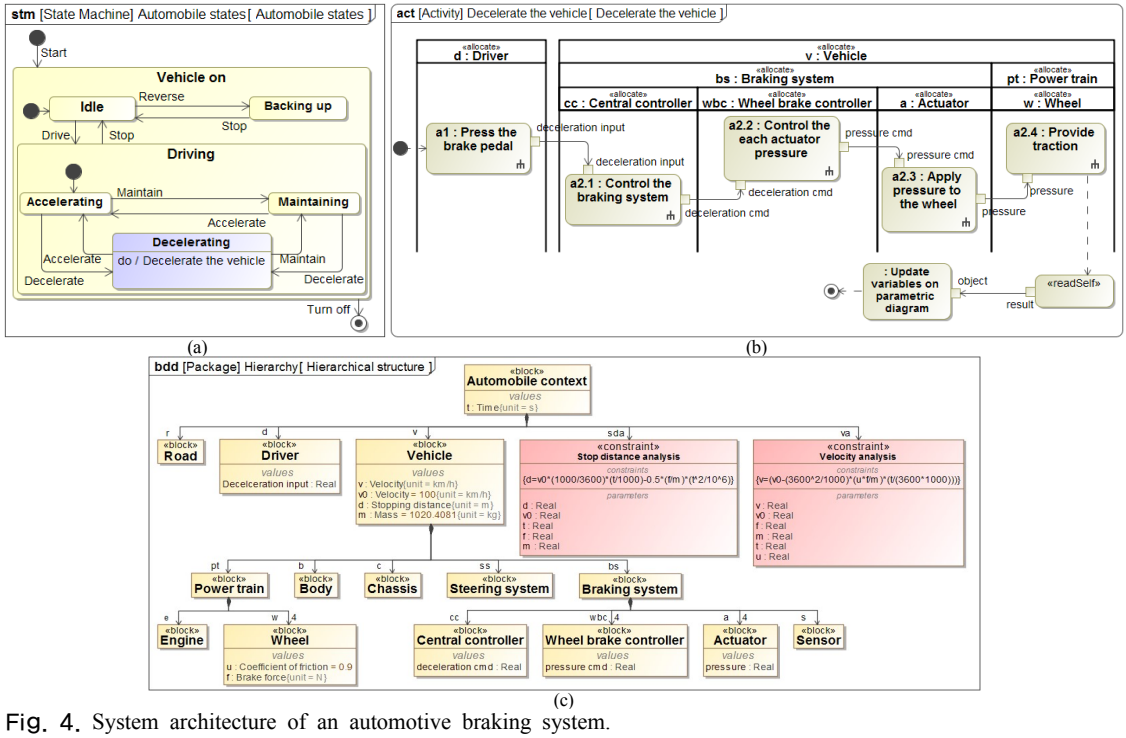


Fig. 4. System architecture of an automotive braking system.
(a) A functional architecture – stm. (b) A functional architecture – act. (c) A physical architecture – bdd.

Case study를 수행하였고, 시스템에 대한 정보는 참고문헌을 활용하였다[5,6,7,8]. 먼저, 차량 수준의 기능 아키텍처를 stm으로 정의하고, 브레이크의 최상위 기능(상태)으로 “Decelerating"을 식별하였다. 이 기능(상태)을 달성하기 위한 하위 기능들을 식별한 후, 하위 기능의 흐름과 인터페이스를 act로 정의하였다. 기능 아키텍처를 정의한 후에는, 각 기능을 수행할 물리 컴포넌트와 계층 구조, 성능 수식을 bdd로 정의하였다. Fig. 4는 자동차 브레이크 시스템의 시스템 아키텍처를 나타낸다.

자동차 브레이크의 시스템 아키텍처를 정의한 후에는 시스템 수준에서 컴포넌트 수준까지 위험원 분석을 수행하고, 그 결과를 기반으로 고장 모델을 정의하였다. 구체적으로, 시스템 수준의 고장 유형을 식별하여 Failed state로 정의한 후, 이 고장의 원인으로 컴포넌트 수준의 3개 고장 유형을 식별하여 Transition의 Trigger(event)로 정의하였다. Fig. 5는 자동차 브레이크 시스템의 고장 모델을 나타낸다.

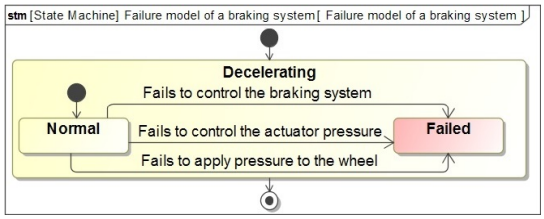


Fig. 5. A failure model of the automotive braking system.

5.2 시스템 아키텍처와 고장 모델의 통합

다음으로 고장 모델을 앞서 정의한 시스템 아키텍처와 통합한 후, 안전설계를 추가하였다. 즉, Fig. 5를 Fig. 4(a)의 Decelerating state에 Sub-state로 통합한 후, Normal state와 Failed state 사이에 Degraded state를 추가 정의하였다. 그리고 나서 Degraded state의 세부적인 안전 기능을 act로 정의한 후, stm의 Degraded state와 연동하였다. Fig. 6(a)는 Fig. 5와 Fig. 4(a)를 통합한 결과이며, Fig. 6(b)는 Degraded state의 세부 안전 기능을 나타낸다.

5.3 통합 모델의 검증 및 결과

마지막으로 Fig. 6(a)(b)와 Fig. 4(b)의 모델이 시스템 요구사항을 만족하는지 검증하기 위해, par를 정의하였다. 앞서 Fig. 4(c)에서 자동차의 제동 거리와 속도에 관한 수식과 파라미터를 두 개의 Constraint blocks로 정의하였다. 이 Constraint blocks의 각 파라미터를 Blocks의 관련된 속성(Value)과 연결하기 위해 par를 생성하였다. Fig. 7은 par를 나타낸다.

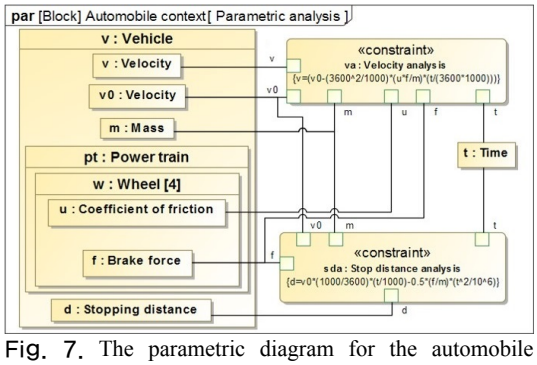
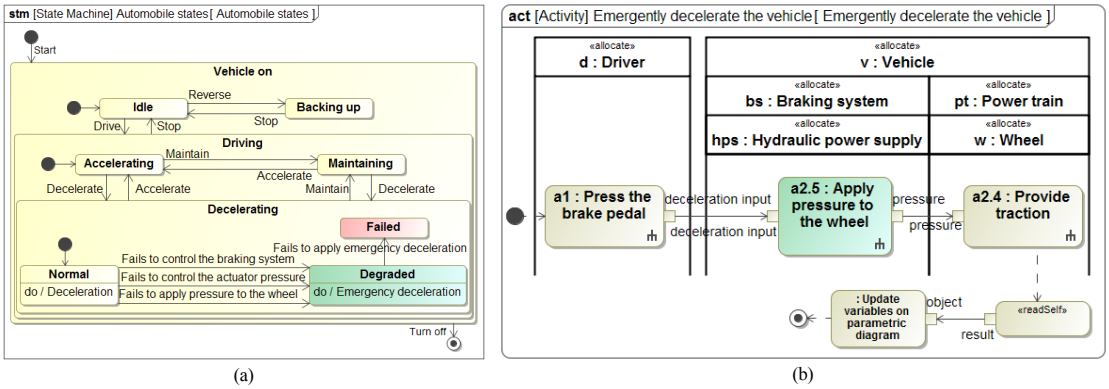


Fig. 7. The parametric diagram for the automobile system.



(a) (b)

Fig. 6. The system architecture integrated with the failure model.
(a) The integrated functional architecture – stm. (b) The added safety function in the "Degraded" state – act.

제동거리 요구사항은 “100km/h로 주행 시, 제동거리는 50m 이하여야 한다.”이며 시뮬레이션을 수행한 결과, 시스템의 일부 고장에도 제동거리는 38.9m로 요구사항을 만족한다는 결과가 Fig. 8.과 같이 산출되었다. 시뮬레이션 결과가 요구사항을 만족하지 못하는 경우에는 설계를 변경하여 다시 검증을 수행해야 한다. 실제 시스템의 경우에는 결함이 발생된 상태에서 고려해야할 변수가 상당히 많고 복잡하지만, 본 논문에서는 진단 시험간격과 결함 반응 시간[9,10]만을 결함과 관련된 변수로 반영하였다.

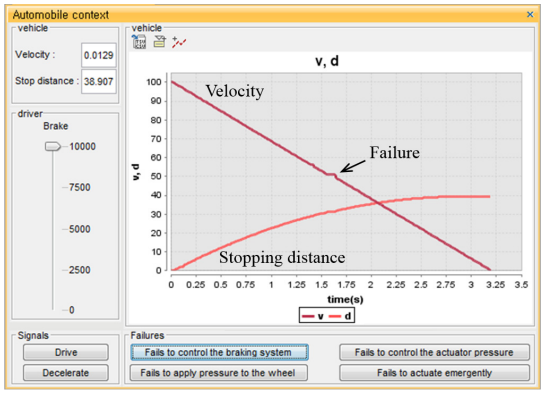


Fig. 8. Results of simulation of the integrated SysML model.

6. 결론

본 논문에서는 기존 모델 기반 위험원 분석의 검증 기법을 개선한 방법론을 제시하였다. 요약하자면, 먼저 대상시스템의 아키텍처와 시스템 고장 모델을 SysML 기반으로 모델링하였다. 그리고 나서 시스템 고장 모델과 시스템 아키텍처를 통합 모델링하고, 이를 기반으로 고장에 대비한 안전 설계를 추가하였다. 마지막으로 시스템 운영 중 일부 고장에도 안전 설계의 결과가 안전 목표를 만족하는지 시뮬레이션을 통해 검증하였다.

SysML을 활용하여 모델 기반 위험원 분석을 수행함으로써 시스템 설계와 위험원 분석을 일관성 있고 체계적으로 수행할 수 있었고, 시스템 고장 모델과 시스템 아키텍처의 통합을 통해 안전 설계를 효과적으로 수행할 수 있었다. 또한 통합 모델을 활용하여 시스템 및 안전 설계에 대한 SysML 기반 시뮬레이션을 수행함으로써, 기존의 모델 기반 위험원 분석에서 고장 모델에 대해서만 수행하였던 검증을 더욱 확장시킬 수 있었다. 향후 자동차나 철도시스템 같은 대형 복합시스템에서의 안전성 확보를 위한 연구개발에서 본 연구의 방법 및 결과의 활용이 기대된다.

References

[1] Y. Papadopoulos, J. McDermid, R. Sasse and G. Heiner, "Analysis and synthesis of the behaviour of complex programmable electronic systems in conditions of failure," Reliability Engineering and System Safety, vol. 71, no. 3, pp. 229-247, Mar. 2001.
DOI: http://dx.doi.org/10.1016/S0951-8320(00)00076-4

[2] Y. Papadopoulos and C. Grante, "Evolving car designs using model-based automated safety analysis and optimisation techniques," Journal of Systems and Software, vol. 76, no. 1, pp. 77-89, Apr. 2005.
DOI: http://dx.doi.org/10.1016/j.jss.2004.06.027

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

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

[5] S. Sharvia and Y. Papadopoulos, "Integrating Model Checking with HiP-HOPS in Model-Based Safety Analysis," Reliability Engineering and System Safety, vol. 135, pp. 64-80, Mar. 2015.
DOI: http://dx.doi.org/10.1016/j.ress.2014.10.025

[6] S. Friedenthal, A. Moore and R. Steiner, A Practical Guide To SysML, Elsevier, 2015.

[7] OMG Systems Modeling Language, Object Management Group, 2013.

[8] P. Sinha, "Architectural Design and Reliability Analysis of a Fail-Operational Brake-by-Wire System from ISO 26262 perspectives," Reliability Engineering and System Safety, vol. 96, no. 10, pp. 1349-1359, Oct. 2011.
DOI: http://dx.doi.org/10.1016/j.ress.2011.03.013

[9] J. Belz, T. Kramer and R. Münzenberger, "Timing is a Safety Issue! Functional Safety requires predictable reactions in real-time," Proc. of Embedded World Conference 2011, Mar. 1-3, 2011.

[10] P. Gradin and V. Ortman, "Development of a collision avoidance truck system from a functional safety perspective," M.S. thesis, Linköpings universitet, Oct. 2011.

조 정 호(Jeong-Ho Jo) **[준회원]**

- 2011년 2월 : 한국해양대학교 선박전자기계공학부 (공학사)
- 2015년 3월 ~ 현재 : 아주대학교 시스템공학과 (석사과정)

<관심분야>
시스템공학, 모델기반 시스템공학, 시스템 안전, M&S

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, Systems T&E, Modeling & Simulation