Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 8 pp. 363-368, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.8.363
ISSN 1975-4701 / eISSN 2288-4688

안전중시 시스템의 체계적인 설계를 위한 시스템 설계 및 안전 분석 활동 모델의 통합

김창원, 이재천*
아주대학교 시스템공학과

Model Integration of Systems Design and Safety Analysis Processes for Systematic Design of Safety-Critical Systems

Chang-Won Kim, Jae-Chon Lee*
Dept. of Systems Engineering, Ajou University

요 약 고장으로 인한 사고 등으로 막대한 피해를 초래할 수 있어 안전성이 중요시 되는 시스템을 안전중시 시스템이라고 한다. 시스템의 대형화, 복잡도 증가 및 무인화 운영 등으로 인해서 안전 위해 요소가 증가하고 있기 때문에 안전성 확보는 국방 및 다양한 산업분야에서 중요한 문제가 되었다. 이러한 이유로 미 국방부와 IEC 등 국제표준기구 등에서는 안전 관련 표준을 만들어서 안전성 확보의 강조 및 시스템 설계와 안전성 분석의 연계를 제시하고 있다. 또한 많은 연구들에서 안전성 분석 활동이 반영된 시스템 설계 프로세스, 방법론 및 도구가 개발되고 있다. 하지만 현재까지 제시된 시스템 설계와 안전성 분석의 통합 프로세스는 각 계층 수준에 존재하는 시스템 설계 정보를 어떻게 활용하는지 명확하게 제시하지 하지 못했다. 그 결과, 체계적인 방식으로 위험원을 식별하는데 어려움이 따르게 되었다. 이와 같은 문제점을 해결하기 위해서 본 연구에서는 각 계층 수준의 시스템 설계 정보를 기반으로 위험원을 식별하여 안전성을 향상 시키고, 여러 산업 분야에 적용 가능한 시스템 설계와 안전성 분석 활동의 통합 모델을 생성했다. 통합 모델이 체계적으로 안전성 분석을 수행할 수 있는 것을 보여주기 위해서 자동차 시스템을 대상으로 적용한 연구결과를 제시하였다.

Abstract In safety-critical systems (SCS), failure may result in accidents with serious damage to human beings and property. As systems become more complex and automated, the goal of acquiring safety has attracted increasing attention lately in the defense industry, as well as the rail, automotive, and aerospace industries, among others. As such, the Department of Defense and international organizations have established appropriate standards and guidelines for systems safety and design. To this end, there has been research on the processes, methods, and associated tools for safety design. However, those results do not seem to sufficiently utilize system architectural information. The purpose of this paper is to provide a more systematic approach to SCS design. To better identify potential hazards, design information at each level of system hierarchy is exploited. Based on the results, an integrated process model was developed by combining the processes of system design and safety analysis. As a case study, the resultant integrated process model was applied to the safety design of an automobile system, which shows useful results for safety evaluation.

Keywords : Functional Safety, Hazard Analysis, Integrated Process, Safety Analysis, Safety-Critical Systems, System Engineering Process, System Safety

1. 서론

안전중시 시스템은 안전사고가 발생했을 때, 인명손실과 재산상의 막대한 피해를 주는 시스템이다. 현대의 시스템은 대형화, 복잡화 되어가고 있기 때문에 안전중시 시스템의 사고 및 고장에 대한 위험이 증가하게 되었

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 15, 2016 Revised August 2, 2016
Accepted August 11, 2016 Published August 31, 2016

다. 따라서 이러한 시스템들의 안전성 문제를 해결하기 위한 안전 관련 표준들이 제정되었다.

미국 국방부에서는 무기체계의 안전성 평가를 위해서 제정한 시스템 안전 표준(MIL-STD-882E) 에서는 시스템 안전과 시스템 설계 활동 간의 연계의 중요성을 언급했다[1]. 기능 안전의 중요성이 부각되면서 표준인 IEC 61508이 제정되었고[2], 이를 기반으로 다양한 산업에 특화된 기능 안전 표준들이 등장했다. 대표적으로 자동차 분야에서는 자동차 설계에 기능 안전성을 반영하기 위한 국제 표준인 ISO 26262를 제정함으로써, 자동차 시스템 설계와 기능 안전의 연계성을 중요하게 다루었다[3].

안전관련 표준들에서 제시하는 것처럼 시스템 설계 정보를 활용하여 안전성 분석을 수행하고, 안전성 분석의 결과를 시스템 설계에 반영하는 것은 필수적이다[1-3]. 하지만 안전중시 시스템 개발을 지원하기 위한 프레임워크나 가이드는 부족하다[4-5]. 또한 시스템 개념 설계가 완료된 후에 수행되는 안전성 분석의 결과는 많은 비용과 시간이 소요된다[6-7]. 따라서 두 활동 사이의 단순한 연계가 아닌 동시공학적인 요소가 반영된 통합이 필요하다.

위와 같은 문제점을 해결하기 위해서 본 논문에서는 기존의 시스템 설계와 안전성 분석 활동의 통합 모델 보다 체계적인 방식으로 안전중시 시스템 개발을 지원할 수 있는 통합 모델을 생성하여 안전중시 시스템 개발에 적용시켰다.

이어지는 2절에서 시스템 설계와 안전성 분석의 통합에 관한 기존의 연구들을 분석한다. 2절의 분석결과를 기반으로 3절에서는 시스템 설계와 안전성 분석의 통합 모델을 생성한다. 마지막으로 4절 사례연구에서는 생성한 통합 모델을 기반으로 자동차 시스템의 안전성 분석을 수행한다.

2. 선행연구 분석

2.1 시스템 설계와 안전성 분석 활동의 통합 모델 분석

안전중시 시스템 개발에서 시스템 설계와 안전성 분석 활동을 통합시키고, 시스템 설계 변경으로 발생하는 비용과 시간을 줄이기 위한 연구들이 수행되었다. 우선, 통합에 관한 연구에서는 시스템 공학과 안전 공학 프로세스를 통합하기 위해서 명확한 통합 절차, 두 프로세스의 상호작용(interaction) 및 각 단계에서 생성해야 하는 산출물 식별이 제시됐다[5]. 하지만 이 연구는 각 활동들 사이의 상호작용을 양방향이 아닌 단방향으로 제시했다.

기본적인 자동차 설계 프로세스에 안전성 분석 프로세스를 추가한 연구는 어떤 방식으로 통합이 이루어지는지 구체적으로 제시하지 못했다[6]. 따라서 [5-6]의 통합 프로세스는 안전중시 시스템 개발의 가이드나 프레임워크로서 역할을 제대로 수행하기 어렵다.

SysML의 Activity diagram을 활용하여 통합되는 두 활동에 대한 정의, 각 활동의 산출물 및 산출물의 교환을 제시한 연구들이 수행됐다[8-9].

하지만 [8]에서는 각 활동들 사이의 순서관계가 불명확하고, Dependability 분석을 시스템 공학 활동과 통합시켰기 때문에 상대적으로 안전성 분석과 그 결과물에 대해서 낮은 비중으로 다루고 있다. 즉, 안전 조치나 안전 요구사항이 시스템 설계에 어떻게 반영되는지를 제시하지 못했다.

[9]에서는 각 활동들에 대한 정의 및 각 활동 사이의 순서관계를 명확하게 제시했다. 하지만 제시된 안전성 분석 활동이 FTA(Fault Tree Analysis)와 FMEA(Failure Mode and Effects Analysis)에 국한되어 있다. 위의 두 기법은 서브시스템과 컴포넌트 수준의 안전성 분석을 수행하는데 적합하기 때문에 시스템 수준의 위험원을 식별할 가능성이 낮다. 이 경우, 뒤늦은 설계 변경으로 많은 시간과 비용이 소요될 수 있다.

2.2 문제정의 및 연구 목표

시스템 설계와 안전성 분석 활동의 통합에 대한 연구들은 다음의 사항들을 모두 고려하지 못했다.

1) 시스템 설계와 안전성 분석 활동 및 각 활동 사이의 순서관계 정의
2) 각 활동들 사이의 산출물 교환
3) 각 계층(시스템, 서브시스템, 컴포넌트) 수준에서의 통합

따라서 본 논문에서는 각 활동들과 활동들 사이의 데이터 교환을 표현하기 적합한 SysML의 Activity diagram을 통해서 위의 세 가지 요소를 모두 반영 통합 모델을 제시할 것이다[10]. Fig. 1은 통합 모델 생성 절차를 정리한 것이다.

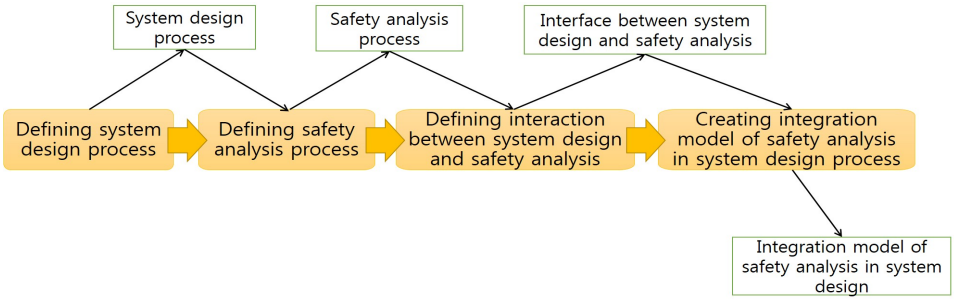

Fig. 1. Identified relationship between the two processes of safety analysis and system design.

3. 시스템 설계와 안전성 분석 활동의 통합 모델 개선

3.1 시스템 설계 및 안전성 분석 활동 정의

시스템의 설계는 사용자, 고객 등의 니즈를 기반으로 시스템 아키텍처를 생성하는 활동이다. 시스템 설계 동안에 요구사항, 기능 아키텍처 및 물리 아키텍처 정의가 각 계층 수준에서 반복적으로 수행된다.

먼저, 시스템 수준의 설계 활동은 니즈와 운영개념을 기반으로 이해당사자 및 시스템 요구사항을 도출함으로써 시작된다. 시스템 요구사항을 기반으로 대상시스템의 기능 아키텍처를 생성하고, 기능 아키텍처를 기반으로 시스템의 물리 아키텍처를 생성한다.

다음으로 서브시스템 수준의 설계 활동은 시스템 수준의 기능 아키텍처와 물리 아키텍처를 기반으로 서브시스템에 대한 요구사항 분석, 기능 아키텍처 생성 및 물리 아키텍처 생성과 같은 순서로 진행된다. 컴포넌트 수준에서의 설계도 위와 같은 방식으로 수행된다.

시스템의 안전성 분석 활동은 시스템 설계 정보를 기반으로 수행된다. 대표적인 기법으로 PHL(Preliminary Hazard List) 분석, PHA(Preliminary Hazard Analysis), SSHA(Subsystem Hazard Analysis)가 있다.

먼저, PHL 분석은 시스템의 니즈 및 운영개념과 더불어 위험원 체크리스트(hazards checklist)를 기반으로 수행되어 PHL을 생성한다.

다음으로 PHA는 시스템 수준의 기능 아키텍처와 물리 아키텍처 및 PHL, 위험원 체크리스트를 기반으로 시스템 수준에 존재하는 대부분의 위험원을 식별한다. 이 식별된 위험원에 의해서 발생 가능한 사고의 리스크를 평가하고, 리스크 평가 결과를 기반으로 안전 조치를 생성한다.

마지막으로 SSHA는 서브시스템의 기능 아키텍처와 물리 아키텍처 및 PHA의 산출물을 기반으로 PHA보다 상세하고, 자세하게 안전성 분석을 수행한다. SSHA의 산출물은 PHA에서 식별되지 않은 위험원 및 새로운 위험원이고, 이를 기반으로 리스크 및 안전 조치가 생성된다.

3.2 시스템 설계와 안전성 분석 활동 사이의 데이터 교환 식별

시스템 설계와 안전성 분석의 통합은 각 활동들 간의 데이터가 교환됨으로써 이루어진다. 따라서 각 활동들이 서로의 어떤 데이터를 필요로 하는지 식별해야 한다.

우선, 시스템 설계 활동은 안전성 분석의 최종 결과물인 안전 조치를 설계에 반영하여 요구사항 및 아키텍처를 수정 및 보완한다.

안전성 분석은 각각의 활동에서 필요로 하는 시스템 설계정보에 차이가 있다. Table. 1은 안전성 분석 기법에서 필요로 하는 시스템 설계 정보를 식별한 것이다.

Table 1. System design information required for safety analysis.

Safety analysis technique	Input from system design
PHL	Needs Concept of Operations
PHA	Needs Concept of Operations System functional architecture System physical architecture
SSHA	Subsystem functional architecture Subsystem physical architecture

3.3 시스템 설계와 안전성 분석 활동의 통합을 위해 SysML 기반 모델 생성

지금까지 통합 모델의 활동 및 데이터 교환을 정의했다. 통합 모델은 각 활동, 활동 사이의 순서 및 데이터 교환을 표현하기 적합한 SysML의 Activity diagram으로 생성됐다.

위의 내용을 기반으로 통합 모델을 생성하기 위해서 먼저, 시스템 설계와 안전성 분석 활동은 모서리가 둥근 형태의 사각형인 Action으로 표현했다. 다음으로 각 활동을 수행하여 생성된 산출물은 직사각형으로 표현된 Data store로 나타냈다. 세 번째로 각 계층 수준의 설계 정보를 활용하여 시스템 설계와 안전성 분석 활동이 수행됨을 명확하게 표현하기 위해서 시스템 수준과 서브시스템 수준에서 수행되는 시스템 설계와 안전성 분석 활동을 Swimlanes 으로 구분했다. 네 번째로 시스템 설계 활동과 안전성 분석 활동 사이의 순서는 점선 화살표를 사용했고, 산출물의 흐름은 실선 화살표를 사용했다. Fig. 2는 논문에서 제시한 통합 모델로서 아래와 같은 순서로 진행된다.

1단계: 니즈, 운영개념 및 위험원 체크리스트를 기반으로 시스템 요구사항과 PHL 분석을 수행한다.

2단계: 시스템 요구사항이 정의되고, 이를 기반으로 시스템 기능 및 물리 아키텍처를 생성한다.

3단계: 2단계가 진행되는 동안에 PHL 분석이 완료되어 PHL을 도출한다.

4단계: 2단계와 3단계에서 도출한 기능 아키텍처, 물리 아키텍처, PHL 및 위험원 체크리스트를 기반으로 PHA를 수행하여 허용 가능하지 않은 리스크가 존재하면, 이를 감소시키기 위해서 시스템 안전 조치(System safety measures)를 정의하여 시스템 설계 활동에 반영한다.

5단계: 다시 1단계부터 4단계를 반복적으로 수행한다. 4단계를 수행하는 동안에 시스템의 리스크가 허용 가능하다면, 서브시스템 설계로 진행된다.

6단계: 서브시스템 설계와 서브시스템 수준에서의 안전성 분석 활동도 1단계부터 5단계를 반복적으로 수행한다. 서브시스템의 설계와 안전성 분석 활동이 종료되면, 컴포넌트의 설계와 안전성 분석 활동으로 진행된다.

4. 통합 모델을 활용한 자동차 시스템의 안전성 분석

본 논문에서 제시한 통합 모델을 다양한 산업 분야에 적용하기 위해서는 해당 분야에 적합하도록 통합 모델을 수정 및 변경해야 한다. 자동차 분야에는 ISO 26262라

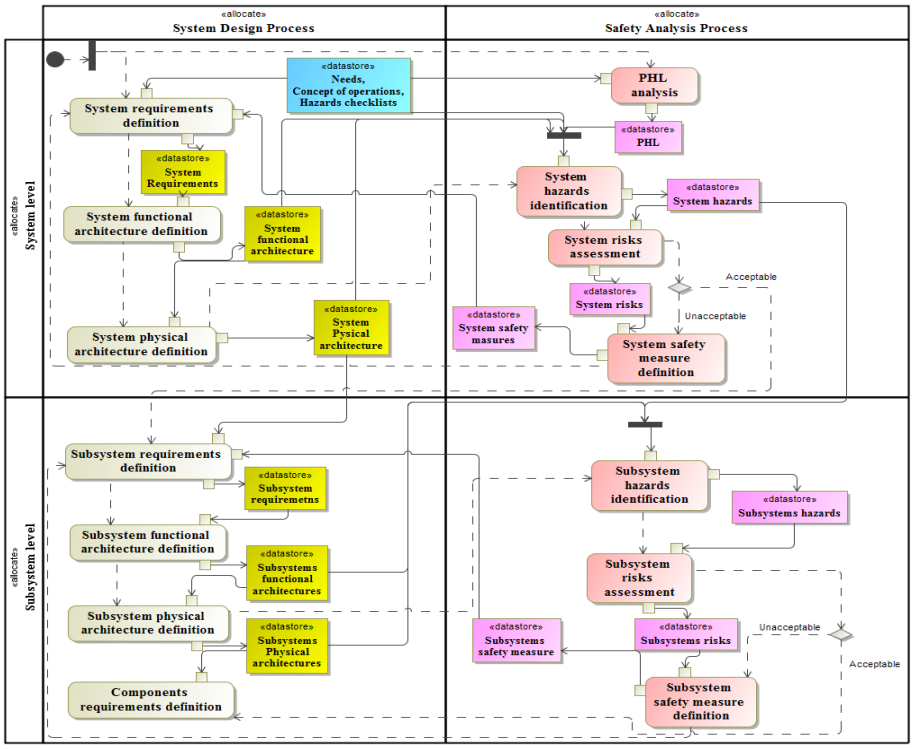

Fig. 2. Integrated process model for system design and safety analysis processes.

는 표준이 존재하고, 이 표준에 부합하도록 통합 모델을 수정할 필요가 있다.

먼저, 시스템 수준의 위험원 분석과 리스크 평가를 통해서 위험원, 위험 사건 및 위험 사건에 대한 ASIL을 도출한다. ASIL은 심각도(S), 노출도(E), 제어가능성(C)의 3요소를 가지며, 범위는 QM(Quality Management) 및 A에서 D까지 존재한다. ASIL은 높을수록 리스크가 큰 것을 의미한다. 다음으로 위험 사건을 제거하거나 경감시킬 수 있도록 안전 목표를 설정하고, 기능 안전 요구사항을 도출한다. 마지막으로 서브시스템 수준에서의 안전성 분석 활동은 기능 안전 요구사항을 기반으로 기술 안전 요구사항을 도출하는 활동이다. Fig. 3는 ISO 26262를 반영하여 자동차 설계에 적합하도록 수정한 통합 모델이다.

수정된 통합 모델을 기반으로 체계적으로 안전성 분석을 수행했다. 먼저, 위험원, 위험 사건 및 위험 사건으로 인한 ASIL 평가 결과를 도출했다. 다음으로 위험 사건에 대한 ASIL 평가 결과를 기반으로 안전 목표를 도출했다. 마지막으로 “Avoiding unexpected acceleration” 라는 안전 목표에 대해서 3개의 기능 안전 요구사항을 생성하고, 기능 안전 요구사항에 ASIL을 할당한 결과를 Table 2에 정리했다.

종합해보면 본 논문에서 제시한 통합 모델은 각 계층 수준의 시스템 설계 정보를 활용해서 안전성 분석을 수행하기 때문에 같은 수명주기 단계에서 두 활동이 수행된다. 이것은 시스템 설계 이후에 안전성 분석을 수행하는 방식보다 시스템 개발 시간을 단축시키며, 각 계층 수준에서 수행되어야 하는 활동들을 명확하게 분리시켜주

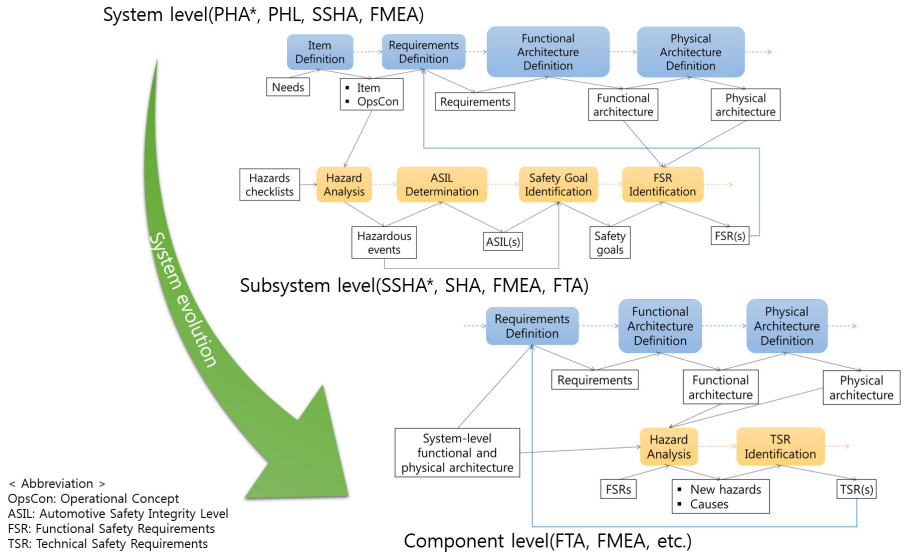

Fig. 3. Integrated process model for functional safety.

Table 2. Results of safety analysis in an automotive system.

Hazards	Driving Situation	Hazardous Event	Safety Goal	S	E	C	ASIL	FSR (for avoiding unexpected acceleration)	ASIL
Unexpected deceleration	Parking	A car runs at high speed.	Avoiding unexpected deceleration	S1	E2	C3	QM	Power Subsystem shall receive an accurate wheel speed signal.	QM
Unexpected stop	Driving in urban	A car is suddenly stopped.	Avoiding unexpected stop	S1	E4	C2	A	Power Subsystem shall monitor accurate torque and speed.	B
Unexpected start	Parking	A car is not accelerated.	Avoiding unexpected start	S1	E4	C0	QM	Brake Subsystem shall control overspeed.	A
Unexpected acceleration	Driving in urban	A car accelerates too much.	Avoiding unexpected acceleration DOI: http://dx.doi.org/10.1016/j.jss.2004.06.027	S2	E4	C3	C	-	-

기 때문에 불필요하게 중복되는 일을 줄일 수 있다. 또한 기존의 통합 모델이 산출물 교환과 순서관계를 명시하는데 그쳤다면, 저자가 제시한 통합 모델은 각 계층 수준에서 사용하기 적합한 안전성 분석 기법을 제시하여, 통합 모델의 효과성을 높였다.

5. 결론

본 논문에서는 시스템 설계와 안전성 분석 활동의 통합 모델을 Activity diagram으로 생성했다.

ISO 26262를 기반으로 위의 통합모델을 수정 및 변경하여 자동차 분야에 적용시킴으로써 통합 모델의 사례 연구를 진행했다.

사례 연구 결과는 첫째, 본 논문에서 제시한 통합 모델이 자동차 산업에 적용 가능하며, 두 번째로, 체계적인 안전성 분석의 프레임워크로서 역할 수행이 가능하다는 것을 보여준다. 마지막으로 각 계층 수준의 설계정보를 활용한 안전성 분석 활동을 명확하게 제시하기 때문에 기존의 통합 모델들 보다 안전성을 향상시킬 수 있다.

References

[1] *Department of Defense Practice: System Safety*, Department of Defense Standard, MIL-STD-882E, 2012.

[2] *Functional safety of electrical/electronic/programmable electronic safety-related systems*, IEC Standard, 61508, 2010.

[3] *Road vehicles – Functional safety –*, ISO standard, 26262, 2011.

[4] K. Thramboulidis and S. Scholz, "Integrating the 3+1 SysML view model with safety engineering," in Proc. Emerging Technologies and Factory Automation (ETFA), Bilbao, Spain, Sep. 13, 2010.
DOI: http://dx.doi.org/10.1109/ETFA.2010.5641353

[5] H. Aboutaleb, M. Bouali, M. Adedjouma, and E. Suomalainen, "An integrated approach to implement system engineering and safety engineering processes: SASHA Project," in Proc. European congress on Embedded Real Time Software and Systems (ERTS 2012), Toulouse, France, Feb. 1, 2012.

[6] Yiannis Papadopoulos and Christian Grante, "Evolving car designs using model-based automated safety analysis and optimisation techniques," The 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

[7] E. Denney, G. Pai, C. Ippolito, and R. Lee, "An integrated safety and systems engineering methodology for small unmanned aircraft systems," in Proc. Infotech@Aerospace 2012, Garden Grove, CA, Jun. 21, 2012.

[8] R. Cressent, P. David, V. Idasiak, and F. Kratz, "Designing the database for a reliability aware Model-Based System Engineering process," Reliability Engineering and System Safety, vol. 111, pp. 171-182, Mar. 2013.
DOI: http://dx.doi.org/10.1016/j.ress.2012.10.014

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

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

김 창 원(Chang-Won Kim) **[정회원]**

- 2014년 2월 : 한밭대학교 산업경영공학과 (공학사)
- 2014년 3월 ~ 현재 : 아주대학교 시스템공학과 (석·박사통합과정)

<관심분야>
시스템공학 (SE), Model-based SE (MBSE), System Safety, Functional Safety, Modeling & Simulation

이 재 천(Jae-Chon Lee) **[정회원]**

- 1977년 2월 : 서울대학교 공과대학 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