Journal of the Korea Academia-Industrial cooperation Society
Vol. 18, No. 9 pp. 9-17, 2017

https://doi.org/10.5762/KAIS.2017.18.9.9
ISSN 1975-4701 / eISSN 2288-4688

자동차 기능안전 표준을 반영하는 개선된 FTA 및 위험원 분석 기법

정호전, 이재천*
아주대학교 시스템공학과

An Improved Method of FTA and Associated Risk Analysis Reflecting Automotive Functional Safety Standard

Ho-Jeon Jung, Jae-Chon Lee*
Dept. of Systems Engineering, Ajou University

요 약 자동차 및 철도 등 수송 시스템에서 무인화 운전으로의 진전으로 인해 시스템 운영 시 안전성의 확보는 필수불가결한 요소로 간주되어 왔다. 자동차 안전설계를 뒷받침하기 위해 제정된 기능안전 표준인 ISO 26262에서는 위험원 분석 및 평가 그리고 안전 설계를 수행할 때 시스템 설계 정보를 적절하게 반영함으로써 안전성이 확보되는 자동차 시스템을 구현하기 위한 절차가 제시되어 있다. 이에 따라 위험원 분석에 관해 많은 연구가 이루어졌는데, 주로 이미 운영되고 있는 유사 시스템 사례에 의존하여 설계 정보를 활용하였다. 먼저 물리 구성품 수준에서 설계정보를 추출하고, 이로부터 기능 들을 역추적 한 후에 위험원을 식별하는 방법이 연구되었다. 이러한 방법은 빠르고 쉽게 위험원의 식별이 가능하기는 하지만, 설계 요구사항이 변경되거나 새로운 시스템을 설계할 때에는 설계 정보를 제대로 반영할 수 없어 일부 위험원이 누락될 수 있는 가능성이 있다. 이러한 점을 해결하기 위해서 본 논문에서는 기능안전표준에서 제시하는 안전수명주기 모델의 위험원 분석 단계에서 효과적인 방법을 연구하였다. 구체적으로 시스템 개념 설계를 Top-Down 방식으로 수행하면서 확보한 설계 정보를 위험원 분석에 적절하게 활용하는 방법을 제안하였다. 먼저 시스템 개념 설계를 수행하고, 획득된 기능 설계 결과를 분석하였다. 그러고 나서 기능 분석 결과를 활용하는 기능기반 Fault Tree Analysis 방법을 제시하고 위험원 분석을 수행하였다. 또한 자동차 시스템에서의 안전 설계 사례 연구를 통하여 본 논문에서 제시하는 방법이 대상 시스템의 설계 정보가 체계적으로 반영되어 누락 가능성이 줄어든 위험원 분석이 가능함을 보여 주었다.

Abstract Ensuring the safety of automobiles and trains during system operation is regarded as indispensable due to the progress in unmanned operation. The automotive functional safety standard, ISO 26262, has been proposed to ensure the safe design of vehicles. This standard describes in detail the required risk analysis and evaluation procedure and safety measures, while appropriately reflecting the system design information. Therefore, much research has been done on the risk analysis procedure, wherein the design information is mostly extracted from physical components of similar systems already in operation, the information traced back to obtain constituent functions, and then methods of identifying risk sources are studied. This method allows the sources of risk to be identified quickly and easily, however if the design requirements are changed or systems are newly developed, others may be introduced which are not accounted for, thereby yielding mismatched design information. To resolve this problem, we propose a top-down analysis in order to utilize the system design information appropriately. Specifically, a conceptual system is designed to obtain the functions, which are then analyzed. Then, a function-based fault tree analysis is conducted, followed by a risk source analysis. In this paper, a case study of automotive safety is presented, revealing that the proposed method can analyze the risk sources with reduced possibility of omission by systematically reflecting the system design information.

Keywords : Functional Safety, Safety Design, Conceptual System Design, Hazard Analysis, Fault Tree Analysis (FTA), Function-Based FTA

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 August 9, 2017 Revised (1st August 29, 2017, 2nd September 5, 2017)
Accepted September 15, 2017 Published September 30, 2017

1. 서론

표준 IEC 61508로 대표되는 기능안전은 시스템 전수명주기적 관점 그리고 계층적 접근을 통하여 차별화되는 진전을 이루었다[1]. 자동차 기능안전 규격인 ISO26262의 특징은 Fig. 1에 도시되어 있는 바와 같이 안전수명주기를 정의하고 시스템의 설계 정보를 반영하여 위험원 분석 및 평가를 수행하고, 이를 기반으로 한 안전기능이 설계과정에서 구현되도록 하고 있다[2-3]. 이러한 과정을 통해 미리 설계과정에서 대상 시스템에 존재할 만한 위험원을 식별하고 이것의 발현확률을 낮추기 위한 안전기능을 시스템에 구현 할 수 있게 된다[4].

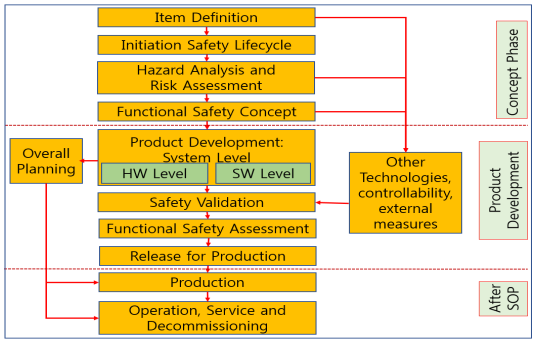

Fig. 1. ISO 26262 Safety Life Cycle[2]

안전수명주기에 따라 안전을 확보하는데 있어 Concept Phase에서 Hazard Analysis를 수행하는 것은 매우 중요하다. 대상시스템에 존재할 만한 위험원을 이 단계에서 빠짐없이 식별하여야 다음의 Functional Safety Concept 설계 단계에서 안전 기능을 도출해서 안전 설계 수행 및 구현을 할 수 있다. 따라서 시스템 설계 정보를 활용하여 대상 시스템에 존재하는 잠재 위험원을 사전에 분석하고 이에 대응하는 안전설계에 관한 연구가 필요하다[5-8]. 기존의 연구 결과들의 공통점은 기능정보를 얻기 위해 구성품 수준의 정보를 기반으로 하여 bottom-up 방식의 분석을 수행했다는 것이다. Majdara 등[9]은 구성품정보로 부터 구성품들이 수행 할 기능을 역으로 식별하였다. Tumer 등[10]에서는 구성품 수준에서의 failure mode에 관한 정보로 부터 failure mode들이 어떤 기능과 연관이 있는지를 역으로 분석하여 기능을 식별하는 방법을 연구하였다.

이러한 방법 들은 빠르고 쉽게 기존 설계정보를 활용하여 위험원의 식별이 가능하다는 장점이 있다. 그러나 새로운 시스템을 설계할 때 시스템의 특성을 제대로 반영하지 못하여 위험원이 누락될 수 있는 위험이 존재한다. 또한 기존에는 기능수준에서 FTA를 수행할 때 Fig. 2와 같이 fault tree의 top event의 식별수준에서 기능정보가 활용되었다. 그리고 Fig. 2와 같이 event를 분해하는 것이 아닌 기존의 고장정보를 활용하여 하위 event tree를 만들어 top event와 연결하는 형태로 fault tree를 도출하였다. 따라서 기능수준에서 설계정보를 활용하여 event의 분해, 조합 등이 수행 되진 못했다.

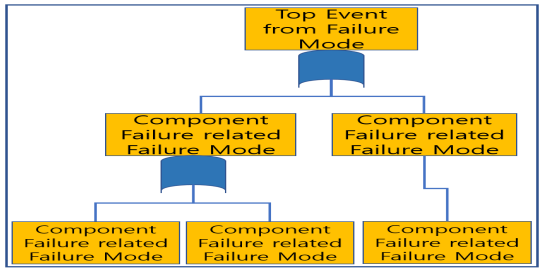

Fig. 2. Example of Traditional Function-Based Fault Tree

본 논문에서는 기존 연구에서의 문제점 들을 개선하기 위해 두 가지 의 연구목표를 설정하였다. 첫째, 시스템 개념설계 단계에서 확보되는 설계정보 중 기능분석결과에 기반을 두어 top event의 식별, event의 분해, 조합 등을 도출하여 기능기반 fault tree를 도출하는 것. 둘째, 기능기반 fault tree를 활용한 위험원 분석 수행 방법의 제시이다.

연구목표 달성을 통해 안전수명주기에서 top-down으로 수행되는 설계 절차에서 확보되는 설계정보를 기반으로 Hazard Analysis 단계를 수행 할 수 있다. 이렇게 위험원 분석을 수행하게 됨으로써 누락의 위험을 줄인 위험원 분석의 수행이 가능하다. 또한 이를 달성하기 위해 FTA기법을 기능수준에서의 설계정보를 기반으로 수행할 수 있게 된다. 기능기반 FTA의 수행을 통해 기능 수준에서 위험원, 원인, 영향을 식별할 수 있고 이것은 안전수명주기에서 다음단계인 Functional Safety Concept에서 어떤 safety function이 어디에 구현이 되어야 하는지를 결정하는 판단 근거로 활용될 것이다.

본 논문의 구성은 다음과 같다. 1절 서론에 이어 2절 및 3절에서는 본 논문에서 제시하는 기능기반 FTA의 수행방법을 제안하고 4절에서는 사례분석을 통해 유용성

을 검증한 결과를 제시하였다. 마지막으로 5절에서는 본 논문의 결과를 정리 및 요약 하였다.

2. 시스템 설계 정보를 활용한 개선된 기능 기반 Fault Tree 생성 방법

2.1 운영시나리오 모델을 활용한 Top Event 결정 방법

본 논문에서는 운영시나리오 모델을 생성하고 이를 기반으로 top event를 결정하는 방법을 도출하였다. 운영시나리오는 대상시스템의 최상위의 기능모델이라 할 수 있기 때문에 설계초기에 도출된다. Fig. 3은 SysML의 activity diagram을 활용하여 생성한 운영시나리오 모델의 예시를 나타내고 있다[11]. 생성한 운용시나리오 모델로 부터 대상시스템의 최상위 수준의 기능들을 식별하고 기능들의 순서, 상호관계 등에 대한 정보를 얻을 수 있다. 이 정보들은 fault tree의 top event를 결정하는데 활용된다.

Top event는 앞서 생성된 기능에 대한 정보를 바탕으로 분석한 기능오류로 정의 할 수 있다. 이때 기능의 오류는 다음과 같이 다섯 가지 유형을 기반으로 식별된다. 이것은 미 국방부와 유럽 철도 분야에서 제시하는 functional failure case들을 분석하여 정의한 것이다[3]. “1. Fails to operate, 2. Operates early/late, 3. Operates out of sequence, 4. Unable to stop operation, 5. Degraded function or Malfunction.” Fig. 3과 같이 확보되는 운영시나리오 모델에서 식별된 기능과 기능간의 상호관계, 위의 정의된 5가지의 기능오류 유형을 기반으로 각 기능들의 오류를 분석하여 top event를 결정하게 된다.

2.2 기능분석 결과를 활용한 기능기반 Fault Tree의 생성 방법

개념설계에서 기능분석을 수행함으로써 도출되는 대표적인 산출물은 기능트리와 기능의 거동모델이라 할 수 있다. 기능트리는 운영시나리오 모델에서 정의 되었던 최상위 수준의 기능들을 분해하여 어떠한 기능들의 조합을 통해 최상위 수준의 기능이 수행 될 수 있는지를 파악할 수 있도록 상하위 기능들 간의 추적성을 제공한다. 기능트리를 활용하여 하위 기능들의 오류의 조합으로 상위 수준의 기능의 오류가 발생한다는 것을 파악 할 수 있다. 따라서 이것을 근거로 fault tree의 event를 분해해

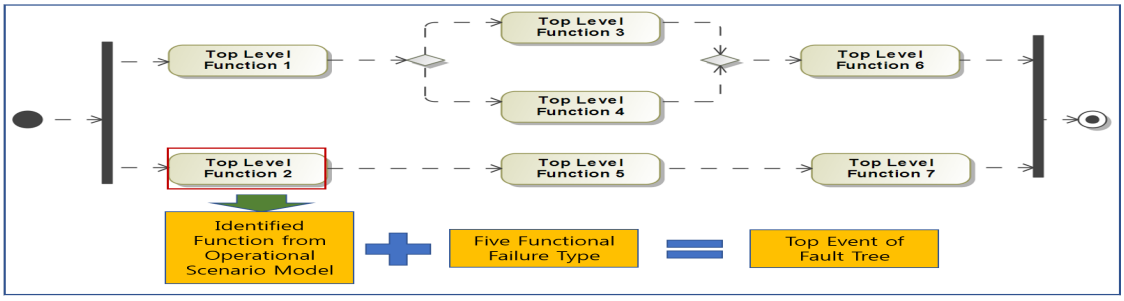

Fig. 3. Concept of Identifying Top Event in Fault Tree

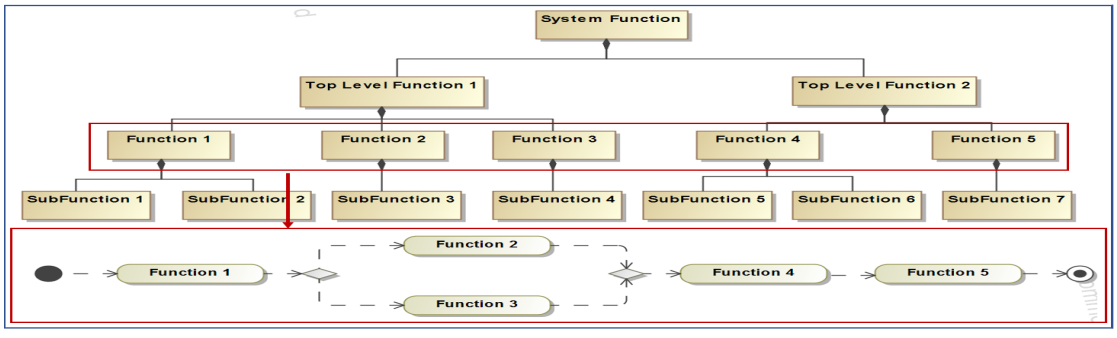

Fig. 4. Example of Function Tree and Associated Functional Behavior Model

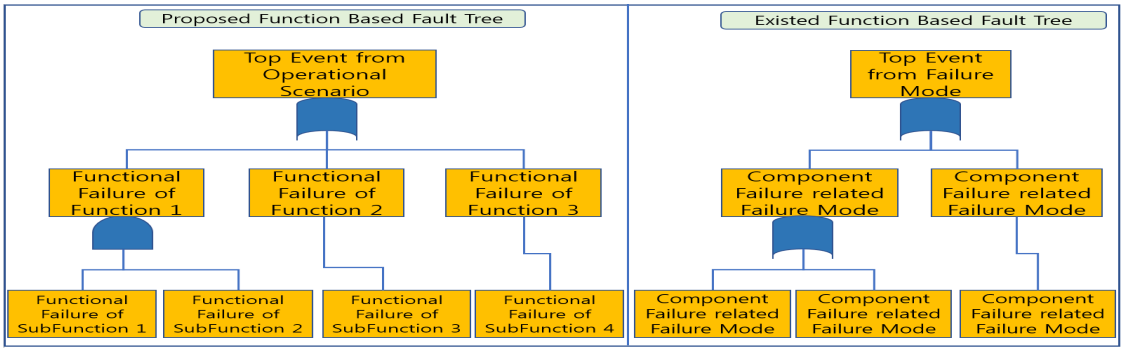

Fig. 5. Comparison of Fault Tree Methods between Proposed and Existing Cases

나갈 수 있다. 거동 모델은 기능들 간의 상호관계, 즉 기능간의 인터페이스를 식별하는데 활용 할 수 있다. 인터페이스 정보는 event를 분해하는 또 다른 정보로 활용할 수 있다. Fault tree에서 상하 event는 and. or gate로 조합이 이뤄지게 된다. 동일 수준의 기능들 간의 인터페이스 분석을 통해 and, or gate 중 어떤 gate가 적절한지 식별할 수 있게 된다. 위의 개념을 바탕으로 Fig. 4는 System Function에 대해 Top Level Function부터 SubFunction 까지 식별한 기능트리와 Function Level의 기능에 대한 거동모델을 도출한 예이다.

Fig. 4와 같이 event를 분해 및 조합하는 절차는 다음과 같다.

첫째. 기능트리를 통해 최상위 수준의 기능이 분해된 기능들을 식별한다. 그 후 식별된 기능들 각각의 오류를 식별한다. 식별된 각각의 오류들은 top Event아래의 intermediate event가 된다.

둘째. 앞 단계에서 식별한 intermediate event들 간의 조합을 또 다른 산출물인 거동 모델을 통해 식별한다. 즉 개별 기능의 오류는 or gate로, 여러 기능들의 조합은 거동모델을 기반으로 병렬연결 되는 기능이 동시에 수행되는 것인지, 어느 하나가 수행되는 것인지를 식별하여 전자의 경우 or gate, 후자의 형태는 and gate로 조합을 하게 된다.

위의 두 단계에 따라 점차 event를 식별하고 분해해 가며 기능트리의 가장 하위의 기능에 관련된 event를 식별할 때까지 반복적으로 수행한다.

Fig. 5는 앞서 제시한 방법과 기존의 연구에서의 방법에 따라 도출한 fault tree를 나열한 것이다. 좌측의 본 연구에서 제시한 방법에 따른 기능 기반 fault tree는 식별된 모든 event와 event의 조합이 온전히 설계초기 기능분석 결과를 활용하여 도출한 결과이다. 즉 설계과정에서 식별된 모든 기능들에 대한 오류를 분석하여 fault tree에 반영이 되어 있다. 우측의 기존 연구에서의 fault tree는 기존의 고장정보에서 failure mode로부터 역으로 failure mode와 관련된 기능을 식별하여 top event로 결정하였다. 그리고 하위 event들은 기존의 고장정보를 가져와 top event와 관련이 있다고 판단되는 것들을 연결시키는 수준에서 fault tree가 도출되었다. 따라서 설계과정에서 식별된 기능들 중 top event에 반영이 안 된 기능들이 존재할 확률이 있다. 또한 event들의 조합이 어떻게 결정되었는지에 대한 근거도 미약하다. 이에 반해 본 연구에서 제시한 fault tree는 거동모델에 근거한 기능간의 인터페이스를 이용하여 event의 조합의 근거를 제시하였다. 즉 좌측 fault tree의 and gate는 subfunction1,2가 병렬연결로 이뤄져있음을 거동모델을 통해 분석하였고 이를 근거로 event의 조합이 이뤄진 것이다.

3. 개선된 기능기반 Fault Tree를 활용한 위험원 분석 수행 방법

3.1 기능 기반 Fault Tree를 활용한 위험원의 식별 방법

2절에서 제시한 방법에 따라 도출된 기능기반 fault tree를 활용하여 위험원 분석을 수행하는 방법을 아래에서 제시한다. 위험원은 Fig. 6과 같이 크게 hazardous element, initiating mechanism, target/threat, 3가지 구성요소로 이뤄져 있다. 그리고 각 요소들은 Fig. 6과 같이 앞서 도출한 설계정보 및 fault tree를 통해 도출 할 수 있다. Hazardous element는 위험원이 존재하는 요소들

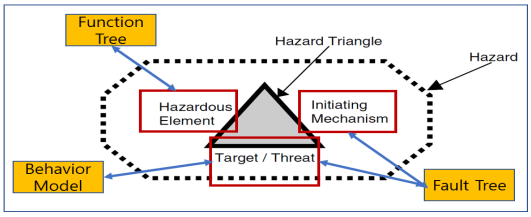

Fig. 6. Relationship among Three Elements of Hazard Analysis including Function Tree, Fault Tree, and Behavior Model

을 식별하는 것이다. 기능 수준에서의 위험원 분석은 대상 시스템의 기능에 관한 위험원을 식별하는 것이므로 기능트리를 통해 식별한 기능들이 hazardous element가 된다. Initiating Mechanism은 위험원을 발현시키는 event로써 fault tree에서 식별되는 event들이 initiating mechanism에 해당된다. Target/Threat는 위험원이 발현되었을 때 예측되는 피해의 대상과 피해의 정도를 기술하는 것이다. 기능 수준에서의 위험원 분석은 상세한 피해의 정도를 식별하는 것은 힘들며, 위험원이 발현되었을 때의 피해의 대상과 피해의 발생확률을 가능한 한 식별하여 기술하여야 한다. 기능 기반 fault tree와 거동모델을 활용하면 하나의 기능에 대한 위험원이 발현되었을 때 다른 어떤 기능에 영향을 미치는 지를 식별할 수 있다. 위와 같은 방법으로 기능기반 fault tree와 기능분석 결과를 활용하면 위험원의 3요소를 모두 도출 할 수 있다.

3.2 기능 기반 FTA 수행을 통한 Cause & Effect 분석 방법

위험원의 원인을 분석하는 것은 원인을 점차 상세히 분석하여 결과적으로 cause tree를 도출해내는 것이라 할 수 있다. Fault tree에서는 top event아래로 top event의 원인이 되는 event들을 계속 식별해 나가게 된다. 따라서 top event의 원인이 되는 가능한 한 모든 cause를 식별해 낼 수 있다. 본 연구에서는 거동 모델을 기반으로 다양한 event의 조합을 식별할 수 있으며, top event에 대해 식별 가능한 cause tree를 Fig. 7과 같이 도출할 수 있다.

기능수준에서 위험원의 영향은 개별 기능의 위험원이 발현되었을 때 다른 어느 기능에 영향을 미칠 것인가를 식별하는 것이다. 따라서 도출한 거동모델을 활용하여 각 수준에서의 기능간의 인터페이스 매트릭스를 도출할 수 있다. Fig. 8은 최상위 수준의 기능을 분해한 기능들에 대한 거동모델을 기반으로 도출한 기능 인터페이스 매트릭스이다. Fig. 8을 보면 Function 1의 오류는 Function 2와 3에 영향을 미치고 Function 2,3은 Function 4, Function 4는 Function 5에 영향을 미친다는 것을 파악할 수 있다.

이와 같이 fault tree와 기능분석결과를 활용하여 위험원의 원인과 영향을 분석 할 수 있다.

	F1	F2	F3	F4	F5
F1		↑	↑		
F2				↑	
F3				↑	
F4					↑
F5					

Fig. 8. Function Interface Matrix

3.1, 3.2절을 통해 안전수명주기의 hazard analysis 단계에서 기능기반 FTA를 활용하여 기능수준에서 위험원,

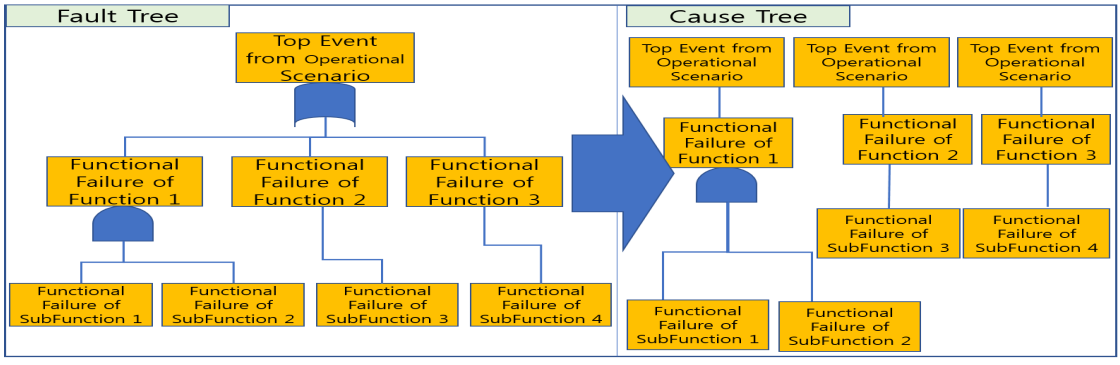

Fig. 7. Identification of Cause Tree from Fault Tree

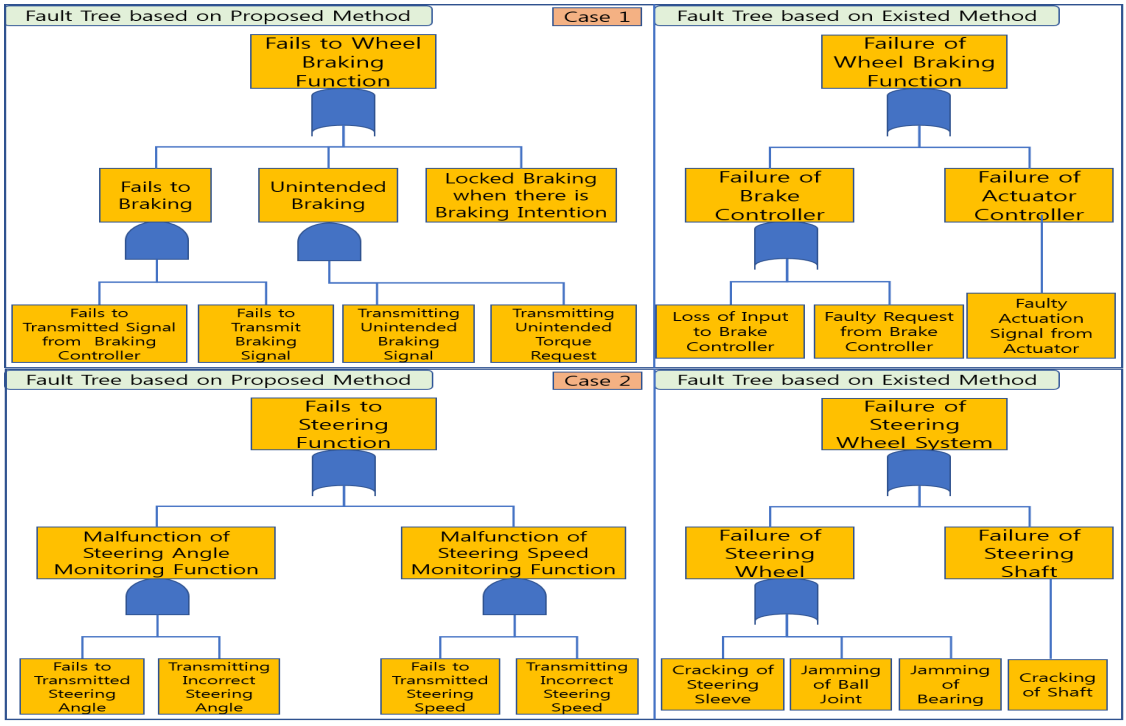

Fig. 9. Fault Trees Derived from Proposed Method and Existing Method

원인, 영향을 식별할 수 있음을 확인 하였다. 이 결과를 활용하여 안전수명주기에서 hazard analysis 다음단계인 functional safety concept 결정 단계에서 safety function을 도출 할 수 있다. 기존 방법과 같이 구성품 수준에서 위험원의 기술, 영향과 원인분석이 이뤄지게 되면 safety function이 어느 기능의 오류와 관련하여 필요한지, 다른 어떤 기능의 영향을 안 미치도록 구현되어야 하는 지등을 결정하는데 어려움이 있다. 그러나 본 논문에서 제시한 기능기반 FTA를 통해 위험원, 원인, 영향이 모두 기능수준에서 명확히 정의가 되어, 다음 절차인 functional safety concept 결정 단계에서 safety function이 어떤 기능의 오류에 대응하기 위한 것인지, 원인이 되는 다른 기능의 오류를 어떻게 차단할 것인지, 다른 기능에 영향을 어떻게 안 미치게 할지 등을 기능수준에서 명확히 정의할 수 있게 된다. 이렇게 되면 차후 상세설계단계에서 safety function을 구현함으로써 설계단계에서 안전을 확보할 수 있게 된다.

4. 사례를 통한 기존 방법과의 결과 비교

4절에서는 자동차의 안전에 큰 영향을 미치는 braking과 steering system에 대해 본 논문에서 제안한 방법과 기존 연구에서의 방법을 통해 FTA를 수행 한 결과를 비교하여 본 논문에서 제안한 방법의 유용성을 검증하였다.

Fig. 9는 본 논문에서 제안한 방법과 기존의 방법을 활용하여 fault tree를 도출한 결과이다. Case1은 braking, Case2는 steering에 대해 분석을 수행한 결과이다. Case1에서 기존의 방법을 통한 fault tree는 brake controller와 actuator controller에 대한 고장정보를 확보한 상태에서 두 구성품의 고장이 어떤 기능과 연관이 있는지를 역으로 식별하였다. 그 결과 두 구성품의 고장은 wheel braking function의 오류와 연관이 있다고 식별하였다. Top event는 wheel braking function의 오류로 놓고 그 아래는 두 구성품의 고장정보에 기반을 둔 event를 도출하여 top event와 연결하는 형태로 fault tree가 도출되었다.

제안한 방법을 통한 fault tree는 wheel braking function과 다섯 가지 functional failure type을 조합하여 도출된 기능오류들을 top event로 결정하였으며 예시에서는 fails to operate에 상응하는 fails to wheel braking function을 top event로 하였다. Wheel braking function은 분해하면 pedaling, braking, actuating, sensing등의 기능으로 분해되며 예시에서는 그 중 핵심 기능인 braking 기능에 대해 분석하였다. 이를 위해 braking 기능과 functional failure type을 조합하여 fails to operate, operates early/late, operates out of sequence 유형이 조합되어 event가 식별되었다. 그중 fails to braking event는 braking 기능의 하위 기능인 신호 송수신과 관련된 event 두 가지를 추가적으로 식별하였다. 이와 같이 제안한 방법을 통한 fault tree는 구성품 수준의 고장정보의 확보 없이 설계과정에서 도출된 기능분석 결과를 활용하여 도출이 되었다.

Case2에서 기존의 방법을 활용한 fault tree는 Case1과 마찬가지로 steering system의 물리적 구성품인 steering wheel과 shaft에 대한 failure를 기반으로 fault tree가 도출되었다. 하위 event도 wheel과 shaft에 대해 failure를 유발하는 원인들이 식별되어 연결되었다.

제안한 방법을 활용한 fault tree는 steering function의 fail을 top event로 하였다. 하위 event는 steering function을 분해하였을 때 핵심기능인 steering speed 및 angle을 측정하는 기능에 관한 기능오류들로 도출되었다. Steering 기능은 steering speed와 angle을 실제와 같이 측정하여 전달할 수 있어야 정확한 조향기능을 수행할 수 있다. 따라서 두 가지 기능은 잘못된 조향으로 인한 위험을 방지하기 위해 매우 중요한 기능이다. 두 가지 기능은 각각 fails to operate와 malfunction 두 가지에 상응하는 functional failure 들이 추가적으로 식별이 되었다.

위의 두 가지 케이스에서 기존의 방법은 top event만이 기능을, 하위 event들은 고장정보를 기반으로 도출된 것이라 이에 대응하는 안전설계는 물리 설계 단계까지 진행된 이후에 본격적으로 반영이 될 수 있다. 반면 제안한 방법에 따라 도출된 위험원 분석결과는 모두 기능 수준에서 정의 가능하다. 이를 통해 설계를 진행하면서 기능설계 단계부터 위험원을 분석하고 이에 대응하기 위한 안전기능의 식별과 설계에의 반영이 가능해진다.

Table 1은 두 가지 케이스에서 두 가지 방법으로 도출한 위험원 분석결과이다. Table 1에는 식별한 위험원

Table 1. Comparison of Hazard Analysis Results for Case1,2

	Hazard	HE	IM	T/T	Cause
[Case1] Proposed Method	Wheel braking function fails to braking when fails to transmitted signal from braking controller and affect to actuating	O	O	O	Signal Transmitting Function Failure
	Wheel braking function fails to braking when fails to transmitting braking signal and affect to actuating	O	O	O	Signal Transmitting Function Failure
	Wheel braking function unintended braking when transmitting unintended braking signal and affect to actuating	O	O	O	Signal Transmitting Function Failure
	Wheel braking function unintended braking when transmitting unintended torque request and affect to actuating	O	O	O	Signal Transmitting Function Failure
	Wheel braking function early locked braking before transmitting braking signal and affect to actuating	O	O	O	Malfunction of Braking
[Case1] Existing Method	Failure of Brake Controller		O		Loss of Input to Brake Controller
					Faulty Request from Brake Controller
	Failure of Actuator Controller		O		Faulty Actuation Signal from Actuator
[Case2] Proposed Method	Steering function fails to steering when fails to transmitted steering angle and affect to steering angle measurement	O	O	O	Information Transmitting Failure
	Steering function fails to steering when transmitted incorrect steering angle and affect to steering angle measurement	O	O	O	Malfunction of Measurement
	Steering function fails to steering when fails to transmitted steering speed and affect to steering speed measurement	O	O	O	Information Transmitting Failure
	Steering function fails to steering when transmiitted incorrect steering speed and affect to steering speed measurement	O	O	O	Malfunction of Measurement
[Case2] Existing Method	Failure of Steering Wheel		O		Cracking of Steering Sleeve
					Jamming of Ball Joint
					Jamming of Bearing
	Failure of Steering Shaft		O		Cracking of Shaft

을 기술하고, 기술된 위험원이 위험원의 3요소를 식별하였는지를 평가하였다. 또한 위험원에 대한 원인을 식별하여 기술하였다. 이것은 식별한 위험원과 원인이 기능수준에서 기술되어 설계초기에 안전설계를 수행 할 수 있는가를 평가하기 위해 포함되었다.

Case 1 및 2에서 제안한 방법을 통해 식별된 위험원을 보면 제안한 방법을 통해 위험원의 3요소를 모두 식별되어 기술되었음을 확인할 수 있다. 기존의 방법에 따라 도출한 위험원들은 고장정보가 그대로 활용되어 IM은 식별이 가능하나 HE와 T/T는 기능수준에서 명확히 식별할 수 없었다. 또한 기존방법으로 식별된 위험원의 원인은 모두 구성품 수준에서의 고장에 의한 것이었다. 이것은 기존방법으로는 기능수준에서 안전기능이 필요한 대상의 식별과 설계에의 반영이 힘들다는 것을 의미한다. 즉 기존방법의 결과로는 Fig. 1의 안전수명주기에 따른 안전설계를 수행하는 것이 힘들다는 것을 의미한다.

반면 본 논문에서 제안한 방법에 따른 결과는 위험원과 원인, 영향이 모두 기능수준에서 식별되고 정의되었다. 이를 활용하면 안전수명주기에 따라 설계를 진행하면서 기능수준에서부터 안전설계가 수행 가능해진다. 즉, wheel braking function과 steering function의 failure 유형, 원인, 다른 기능으로의 영향 등이 모두 기능 수준에서 식별이 되었다. 특히 원인이 주로 signal& information transmitting function과 관련이 있어 signal&information transmitting failure를 방지하기 위한 safety function이 필요함을 확인 할 수 있다. 이와 같이 본 논문의 방법을 활용하여 수행한 위험원 분석의 결과를 활용하면 안전기능의 정의가 체계적으로 이뤄지게 된다.

5. 결론

기능안전 규격에서 제시하는 위험원을 효과적으로 식별하기 위해 본 논문에서는 첫째, 대표적인 위험원 분석 기법인 FTA를 개념설계단계의 설계정보를 활용하여 수행하기 위한 방법을 제시하였다. 개념설계 정보인 기능분석 결과를 활용하여 기능기반 fault tree를 도출하는 방법과 이를 활용하여 위험원 분석을 수행하는 방법을 제시하였다. 이렇게 대상시스템에 대한 설계정보를 바탕으로 위험원 분석을 수행함으로써 대상 시스템의 설계특성이 반영된 위험원 분석이 수행되어 누락 없는 위험원 분석이 가능하게 된다. 둘째, FTA를 수행할 때 Top Event의 식별, Event의 분해, Cause의 식별등 FTA수행의 전반에 걸쳐 기능분석 정보를 활용하여 위험원 분석을 수행하는 방법을 제시하였다. 셋째, 제안한 방법을 통해 기능수준에서 위험원의 3요소를 명확히 도출하였다. 이때 도출한 정보는 안전수명주기의 다음단계인 functional safety concept 설계 단계에서의 안전기능의 식별 및 구현 대상 등이 명확히 도출되어 향후 설계에 안전기능이 체계적으로 반영이 될 수 있게 된다.

References

[1] Functional safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission Standard, IEC 61508, 2010.

[2] Road vehicles -- Functional safety --, International Organization for Standardization Standard, ISO 26262, 2011.

[3] Railway Applications - Communication Signalling and Processing Systems Software for Railway Control and Protection Systems, IEC Standard, IEC 62279, 2002.

[4] A. Scharl, K. Stottlar, R. Kady, "Functional hazard analysis methodology tutorial," in Proc. International System Safety Training Symposium, St.Louis, MO, Aug. 4-8, 2014, pp. 1-17.

[5] R. B. Stone, I. Tumer, M. Van Wie, "The function-failure design method," Journal of Mechanical Design, vol. 127, no. 3, pp. 397-407, Jul. 12, 2004. DOI: https://doi.org/10.1115/1.1862678

[6] M. H. Ordouei, A. Elkamel, G. Al-Sharrah, "New simple indices for risk assessment and hazards reduction at the conceptual design stage of a chemical process," Chemical Engineering Science, vol. 119, no. 8, pp. 218-229, Nov. 2014. DOI: https://doi.org/10.1016/j.ces.2014.07.063

[7] K. G. Lough, "The risk in early design method," Journal of Engineering Design, vol. 20, no. 2, pp. 155-173, Mar. 2009. DOI: https://doi.org/10.1080/09544820701684271

[8] Y. D. Shin, S. H. Sim, J. C. Lee, "Model-based integration of test and evaluation process and system safety process for development of safety-critical weapon systems," Systems Engineering, vol. 20, no. 3, pp. 257-279, May 31, 2017. DOI: https://doi.org/10.1002/sys.21392

[9] A. Majdara, T. Wakabayashi, "Component-based modeling of systems for automated fault tree generation," Research in Engineering Design, vol. 94, no. 6, pp. 1076-1086, Jun. 2009. DOI: https://doi.org/10.1016/j.ress.2008.12.003

[10] I. Tumer, R. B. Stone, "Mapping function to failure mode during component development," Research in Engineering Design, vol. 14, no. 1, pp. 25-33, Jan. 2003. DOI: https://doi.org/10.1007/s00163-002-0024-y

[11] System Modeling Language, Object Management Group Standard, 2015.

정 호 전(Ho-Jeon Jung) **[정회원]**

- 2010년 8월 : 경북대학교 전자공학과 (공학사)
- 2013년 2월 : 아주대학교 시스템공학과 (공학석사)
- 2013년 3월 ~ 현재 : 아주대학교 시스템공학과 (박사과정)

<관심분야>
시스템공학 (SE), 모델기반 시스템공학 (MBSE), 시스템 안전(System Safety), 기능안전(Functional Safety), 시스템 안전 관리체계, 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