Journal of the Korean Society of Safety, Vol. 30, No. 5, pp. 114-122, October 2015
 http://dx.doi.org/10.14346/JKOSOS.2015.30.5.114

철도차량 제동장치의 위험도 평가

이성권 · 김종운* · 구정서†

서울과학기술대학교 철도차량시스템공학과 · *한국철도기술연구원

(2015. 8. 26. 접수 / 2015. 9. 21. 수정 / 2015. 10. 14. 채택)

Risk Assessment for Pneumatic Braking of EMU

Sung-Kwun Lee · Jong-un Kim* · Jeong-Seo Koo†

Rolling Stock System Engineering, Seoul National University of Science and Technology

*Korea Railroad Research Institute

(Received August 26, 2015 / Revised September 21, 2015 / Accepted October 14, 2015)

Abstract : FMEA and FTA have been widely applied to the safety studies for railway systems respectively. But it would be more effective to use these two methods at a same time because these are complementary. This article suggests a FMEA-FTA combined analysis technique to evaluate the risk for railway systems. A FMEA-FTA combined risk evaluation model and process are proposed and a case study is dealt with for PBU(Pneumatic Breaking Unit), a major subsystem of a railway vehicle.

Key Words : systems engineering, risk assessment, FMEA-FTA technique, pneumatic braking unit(PBU)

1. 서 론

위험도는 하나의 위험원이 실질적으로 일어날 가능성과 심각도의 조합으로 정의되는 척도로서 위험도 평가는 철도 시스템의 RAMS(Relaibility, Availability, Maintainability, Safety) 관리의 핵심 분야 중 하나이다. 일반적으로 위험도는 Fig. 1과 같이 원인, 위험원, 영향이 상호 관련되어 있으며, 이를 정량적이고 정성적으로 정의하기 위한 4가지 요소로 ① 잠재적인 위험원 발생의 근본원인 ② 하나의 위험원 ③ 위험원의 영향 ④ 위험원 영향의 발생확률 요소들이 있다[1,2].

철도시스템의 설계 및 개발 프로젝트는 매우 복잡한 엔지니어링 환경을 가지고 있어서 위험도 평가를 위한 하나의 통합된 엔지니어링 프로세스의 적용이 필요하다.철도시스템의 위험도 분석에 적용될 수 있는 대표적인 방법으로는 고장모드 및 영향분석(Failure mode and effect analysis: FMEA), 고장트리 분석(Fault tree analysis: FTA), 사건트리 분석(Event Tree Analysis: ETA) 등이 있다. FMEA는 대형이고 복잡한 시스템 프로젝트에 설계단계에서부터 핵심적으로 적용되며, FTA는 시스템엔지니어링(System engineering: SE) 의 모든 단계에서 적용될 수 있어 개념설계 단계에서부터 문제점을 효과적으로 개선할 수 있는 분석 기술이다. ETA는 잠재적인 고장 이벤트 결과의 시나리오에 대한 고장사건의 시퀀스(Sequence)를 평가하는 기술로서 위험평가 거의 대부분 형태에 적용할 수 있고, 사고를 효과적으로 모델화 하는데 사용될 수 있다. 이 고장 시나리오는 FMEA에 의해 표현될 수 있고 또한 확률은 FTA에 의해서 평가가 가능하다.

Park 등[5] 및 Cha[9]는 철도시스템의 고장 및 안전성 분석에 FMEA를 적용하였고, Kim[10]은 FTA를 사용하여 안전성을 분석하였다. 위 연구와 같이 FMEA 및 FTA는 개별적으로 적용될 수 있지만 FMEA는 기본적으로 'Bottom-Up' 접근법이고 FTA는 'Top-Down' 접근법이기 때문에 이 두 가지를 상호 보완적으로 사용한다면 더 큰 효과를 기대할 수 있다.

따라서 본 연구에서는 SE 단계에서 유용한 위험도 평가 기술로서 FMEA-FTA 분석적 결합 모델을 제시하고, 이를 철도차량 제동장치에 적용한 사례연구를 수행한다.

† Corresponding Author : Jeong-Seo Koo, Tel : +82-02-970-6878, E-mail : koojs@seoultech.ac.kr
Department of Rolling Stock System, Seoul National University of Science & Technology, 232, Gongreung-ro, Nowon-gu, Seou l01811, Korea

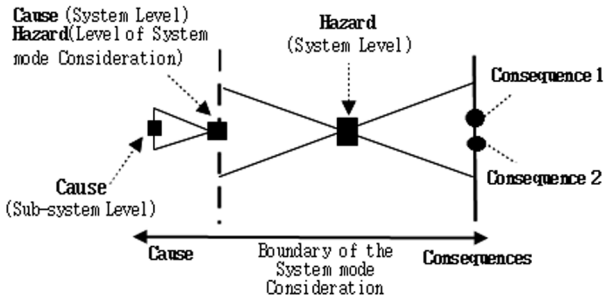

Fig. 1. The definition of risk concepts.

2. FMEA-FTA 기반의 위험도 평가 모델

Fig. 2는 FMEA-FTA 기술을 결합한 위험도 평가 모델로서 FMEA 기술은 모든 시스템 구성요소의 질적인 고장분석으로 고장결과에 대한 고장원인의 사나리오 개발을 위해 사용되고 연역적 접근을 적용한다. 반면 FTA는 고장원인에 대한 논리적 분석을 통하여 고장결과에 대한 양적 분석 및 효과적인 귀납적 접근을 적용한다[3,4].

위험도 평가는 SE 설계 단계에서 모든 잠재적인 위험원을 확인하고, 이와 관련된 위험도를 평가하는 프로세스를 가져야 한다. 이 위험도 평가 프로세스는 적합한 위험도 축소 및 제거 등 위험에 대한 대책을 제시하기 위하여 필요한 정보나 논리를 제공한다. 따라서 FMEA-FTA의 결합을 통한 철도시스템의 위험도 평가 프로세스를 제시하고자 한다. Fig. 3과 같이 FMEA-FTA 분석 기술은 유지보수 요구사항과 유지보수 관리에 대한 필요성을 확인하는 것으로 시작된다. 또한 관련된 규정, 제품의 결정론적 수명, 고장모드뿐만 아니라 가능한 결과에 의한 고장영향을 참고로 결정할 수도 있다. 그러나 철도 시스템과 같은 대형의 복잡한 구조의 위험도 평가는 전문가의 엔지니어링 판단에 의해 수행될 수도 있다. 이러한 전문가의 판단은 충분하지 못한 데이터로 인해 양적인 위험도 평가가 불가능한 경우 또한 적용할 수 있다[5].

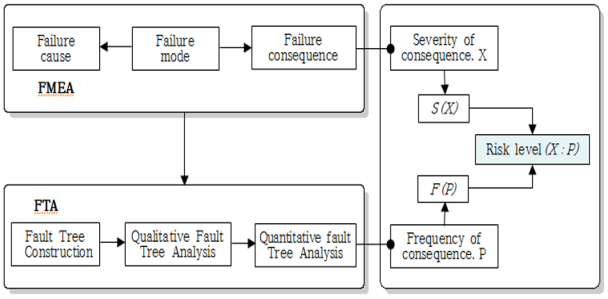

Fig. 2. FMEA– FTA based risk assessment model.

2.1 요구사항 정의

Fig. 3에서 첫째 위험도 요구사항 정의 단계는 타당성 조사를 통하여 철도 SE 프로젝트에서 유지보수 성능 관리의 필요성 및 포함 여부를 확인하여 설계해결방법 및 인수성능 조건을 정의한다. 시스템 경계, 운영적인 상황, 환경 및 수명주기 프로세스를 기반으로 정의하고 시스템을 구성하는 모든 수준단계 즉 시스템, 서브시스템, 부품 단계에서 정의되고 확인되어야 한다. 다음은 요구사항 단계에서 확인되고 정의되어야 하는 사항으로 ① 표준규격, 규제 등 ② 운영적인 시나리오와 시스템 효용성 척도 ③ 시스템 경계조건, 운영환경, 시스템 수명주기 프로세스 ④ 기능적인 요구사항, 결정론적이고 확률적인 유지보수 요구사항 ⑤ 유지보수성 인수조건이 있다.

2.2 위험도 파라미터와 매트릭스 결정

위험도 파라미터와 매트릭스 결정 단계는 먼저 데이터/정보 수집 및 분석에서 위험도 평가 파라미터 및 평가 매트릭스의 범위와 분류를 확립하기 위하여 데이터 및 정보를 분석하며, 유사한 시스템의 사고나 장애로부터 정보를 얻고 그 시스템의 과거사고 및 장애로부터 가능한 모든 위험요소를 정확하게 이해하기 위함이다. 예로서 통계적 데이터나 정보, 휴먼 경험 및 엔지

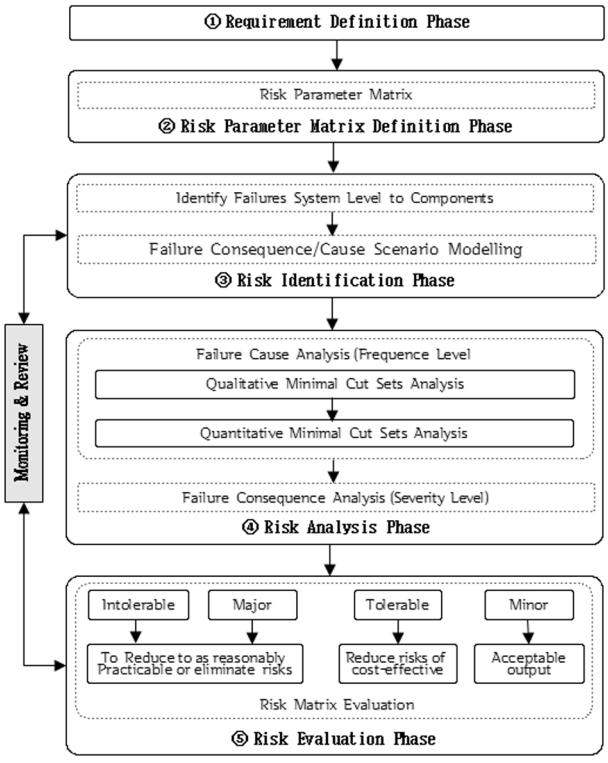

Fig. 3. FMEA–FTA technique based risk assessment process.

니어링 지식에 의한 분석, 개념적 프레임워크 등을 들 수 있으며, 통계적 기술을 2개 혹은 그 이상을 결합하면 위험도 평가의 고유한 단점을 극복할 수 있고, 환경적 특성에 대해 보완적으로 평가를 할 수 있다.

다음은 위험도 파라미터의 확립에서 수집된 정보나 데이터의 분석을 통해 얻어진 결과는 위험도 평가를 위한 질적인 분류를 결정하기 위해 매트릭스를 사용할 수 있다. FMEA-FTA 결합을 기반으로 위험도 평가 모델은 2종류의 파라미터를 요구한다. 하나는 심각도 파라미터이고 다른 하나는 심각도에 대한 발생빈도 파라미터이다. 이는 철도의 시스템 수준과 서브시스템에 대한 고장영향 및 고장결과에 대한 위험수준을 결정하는데 사용된다. 또 하나는 위험도 수준을 결정하기 위해 4가지의 평가 매트릭스를 요구한다.

① 심각도 파라미터 결정은 전체 시스템에 대한 고장결과에 대해 가능한 정도를 설명하며, Table 1과 같이 철도 RAMS 규격의 분류를 사용하였다[7]. 철도시스템의 고장결과는 사람, 환경 또는 서비스의 3가지로 분류하였다.

② 발생빈도 파라미터 결정은 Table 2에서 심각도에 대한 발생빈도 분류는 일반적으로 6단계로 분류하였다. 이들에 대한 단계별 용어는 국제규격[7]에서 적용되는 방식에 따라 발생빈도에 대하여 연간 100~10^{-6}을 제시하였다. 따라서 철도시스템에서도 Table 2와 같이 세분화하여 결정하였다[6].

Table 1. Failure-severity parameters

Classification	Level	Results for human or environmental	Results of the service
Catastrophic	4	Fatalities and/or multiple severe injuries and/or major damage to the environment	
Critical	3	Single fatality and/or severe injury and/or significant damage to the environment	Loss of a major system.
Marginal	2	Minor injury and/or significant threat to the environment	Severe system(s) damage
Insignificant	1	Possible minor injury	Minor system damage

Table 2. Failure-frequency parameters

Classification	Level	Description	Frequency
Frequent	6	It is likely to occur frequently and will be continually experienced.	≥ 100
Probable	5	It will occur several times and can be expected to occur often.	$100 < \text{to} \leq 1$
Occasional	4	It is likely to occur several times and can be expected to occur several times.	$1 < \text{to} \leq 10^{-2}$
Remote	3	It is likely to occur at some time in the system life cycle and can reasonably be expected to occur.	$10^{-2} < \text{to} \leq 10^{-4}$
Impossible	2	It is unlikely to occur but is possible and can be assumed that it may exceptionally occur.	$10^{-4} < \text{to} \leq 10^{-6}$
Incredible	1	It extremely unlikely to occur and can be assumed that it may not occur.	$< 10^{-6}$

Table 3. Risk assessment parameters

Classification	Level	Risk reduce/control
Intolerable	4	Risk shall be eliminated.
Undesirable	3	Risk shall only be accepted when risk reduction is impracticable and with agreement.
Tolerable	2	Risk is acceptable with adequate control and agreement.
Negligible	1	Acceptable without any agreement.

③ 위험도 결정 파라미터에서는 일반적으로 Table 3과 같이 양적 또는 질적으로 분류한다. 철도시스템 RAMS 국제규격[7]은 위험도 평가를 4단계로 구분하여 사용하고 있으며, IEC 62278에서 ALARP이 질적인 단계를 제공하고 있다[7].

④ 위험도 평가 매트릭스 결정은 Table 4에서 철도시스템의 위험요소에 대한 위험도를 결정할 수 있는 평가 매트릭스로서 수평열은 고장결과의 심각도에 대한 파라미터를 나타내며, 수직열은 심각도에 대한 발생빈도의 파라미터이다. 각 열이 만나는 지점이 발생된 고장결과의 위험도가 된다. 예로서 심각도 'insignificant'와 발생빈도 'frequent'가 만나는 지점의 위험도는 'undesirable'이 된다. 이는 매우 높은 수준의 위험도를 보여주고 있고, 'negligible'은 매우 낮은 수준의 위험도를 의미한다[7].

2.3 위험도 확인

SE 단계에서 시스템 및 기능적 아키텍처가 정의되면 위험요소를 확인할 수 있으며 위험요소를 확인하기 위해 다른 시스템, 시스템, 서브시스템, 부품 단계에서

Table 4. Risk assessment matrix decision

Frequency level		Risk level			
Frequent	6	Undesirable	Intolerable	Intolerable	Intolerable
Probable	5	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	4	Tolerable	Undesirable	Undesirable	Intolerable
Remote	3	Negligible	Tolerable	Undesirable	Undesirable
Improbable	2	Negligible	Negligible	Tolerable	Tolerable
Incredible	1	Negligible	Negligible	Negligible	Negligible
		1	2	3	4
		Insignificant	Marginal	Critical	Catastrophic
		Severity levels of failure consequence			

의 모든 잠재적인 고장모드, 고장원인, 고장영향을 체계적으로 확인하는 프로세스로서 3가지 단계로 구성된다. 첫 단계는 운영적인 단계로서 주요한 위험요소를 확정하기 위해 수행한다. 다음은 기능적 정의단계에서는 위험을 비교・확인하기 위해 귀납적 접근 방법으로 수행한다. 마지막 단계인 물리적 설계구조 정의단계는 앞선 단계에서 확인된 위험요소에 대하여 개선을 위해 연역적 접근으로 평가를 수행하며, 이는 고장원인과 고장영향에 대한 시나리오 모델을 확인하는 과정으로 구성된다.

따라서 철도시스템의 위험요소를 정확히 확인하기 위하여 FMEA 분석 기술과 같이 사용될 수 있으며, 시스템 초기에서 시작하여 부품 수준까지 확장하여 시스템 수준까지 반복적으로 수행한다. 이 단계는 고장결과와 고장원인에 대한 시나리오 모델을 시스템 설계의 논리적인 구조를 확립하기 위하여 개발하여야 한다. 첫째 고장결과에 대한 시나리오 개발은 고장 이벤트에 환경 등에 대한 영향을 평가하기 위한 것이고, 고장결과는 하나의 고장영향, 일련의 고장영향, 실험적인 연구의 판단 등으로부터 전체적인 결과의 심각도를 결정하기 위하여 모델링하여야 한다. 둘째 고장원인에 대한 시나리오 개발에서 위험확인은 시스템 고장에 이르는 가능한 모든 원인을 확인하기 위하여 구조화된 방법이 되어야 하며, 가능한 발생요소들을 넓은 범주로 분류되도록 조직화하여야 한다. 그러나 모든 가능한 원인이 실질적인 고장에 이르는 것은 아니다. 단지 수집된 정보나 데이터 또는 실험적인 데이터에 의해 결정되기 때문으로 이 시나리오는 논리적 구조를 사용하여 모델링할 수 있으며 모델링은 고장트리 구조를 사용하여 수행할 수 있고, 하나의 탑 이벤트로부터 시작하는 반복적인 프로세스가 된다. 탑 이벤트의 결정은 하나의 고장트리는 고장 이벤트가 일어날 수 있는 시스템 상황에 대하여 심벌을 사용하여 표현하고, 다음은 심벌의 결정에는 OR 또는 AND 게이트에 의해 표현되는 논리적 심벌과 이벤트 심벌이 있다.

2.4 위험도 분석

위험도 분석은 앞 단계에서 FMEA에 의해 결정된 고장결과와 그 원인의 관계에 대한 시나리오를 양적으로 평가하는 프로세스로서 FTA 분석을 통해 수행된다. 각 고장결과에 대한 심각도와 이 심각도에 대한 발생빈도의 평가 수준은 Table 4에서 제안한 위험도 평가 매트릭스에 적용한다. 첫째 고장원인 시나리오에 대한 질적인 분석은 하나의 고장트리는 탑 이벤트를 일으킬 수 있는 것들의 고장결합에 대한 정보를 제공하고, 또한 탑 이벤트에 이르는 하나의 메카니즘을 제시해 준다. 그러므로 고장트리의 절단집합(Cut set)은 높은 확률을 갖는 절단집합과 관련된 안전을 확인하는 것으로 시스템 설계에 중요하거나 단점으로 연결된 것들을 확인할 수 있도록 한다. 절단집합 분석은 최소로 결정・확인하기 위하여 수행되고, 이는 일반적으로 부울대수 규칙(Boolean algebra rule)을 적용하여 결정하며 최소 절단집합(Minimal cut sets; MCSs)을 결정하는데 있어 매우 중요하다. Fig. 4는 부울대수 규칙의 고장트리 예이다[4].

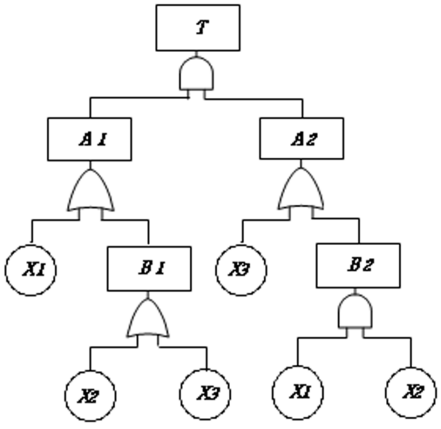

Fig. 4. Fault-tree equivalent of Boolean algebra rule.

Fig. 4는 다음과 같이 표현할 수 있다.

$$T = A_1 \cdot A_2 \quad (1)$$

$$A_1 = X_1 + B_1 \quad (2)$$

$$B_1 = X_2 + X_3 \quad (3)$$

$$A_2 = X_3 + B_2 \quad (4)$$

$$B_2 = X_1 \cdot X_2 \quad (5)$$

귀납적 대체방법(The top-down substitution method)에 대한 식(1)은 흡수법칙(Absorption law)으로 정리하면

$$T = (X_1 \cdot X_3) + (B_1 \cdot X_3) + (B_2 \cdot X_1) + (B_1 \cdot B_2) \quad (6)$$

또한, 멱등법칙(Idempotent law)을 적용하면

$$T = X_3 + B_2 \cdot X_1 + B_2 \cdot X_2 \quad (7)$$

식(7)의 B2는 2회에 걸쳐 흡수법칙을 적용하면

$$T = X_3 + (X_1 \cdot X_2) \cdot X_1 + (X_1 \cdot X_2) \cdot X_2 = X_1 \cdot X_2 \quad (8)$$

식(8)은 $T = X_3 + (X_1 \cdot X_2) + (X_1 \cdot X_2)$ (9)

결과적으로 MCSs에 의해 표현하면

$T = X_3 + X_1 \cdot X_2$ (10)

탑 이벤트 MCSs는 하나의 싱글 이벤트(X_3)와 하나의 더블 이벤트($X_1 \cdot X_2$)로 구성되어 있고 식(10)은 Fig. 5로 나타낼 수 있다[4].

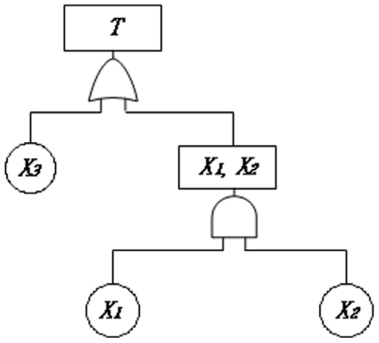

Fig. 5. Simply expresses the fault-tree [Fig.4].

둘째 고장원인 시나리오에 대한 양적인 분석에 대한 모델은 고장확률에 의해서 수량화할 수 있으며, 기본적인 개념은 FTA 분석 기술의 논리적 게이트에 의해 적용될 수 있으며 OR와 AND 게이트로 설명할 수 있다. 다음은 고장률에 의한 수량화로서

OR 게이트는 식(11)에 의해서 평가될 수 있다[8].

$$R_s(t) = \prod_{i=1}^{n} R_i(t) \quad (11)$$

Rs : 직렬 시스템의 신뢰성

R_i : $_i$번째의 신뢰성, n : 부품의 수량

AND 게이트 식(14)는

$$R_p(t) = 1 - \prod_{i=1}^{n} [1 - R_i(t)] \quad (12)$$

R_P : 병렬 시스템의 신뢰성

R_i : $_i$번째의 신뢰성, n : 부품의 수량

2.5 위험도 평가

위험도 평가는 위험도 평가 매트릭스에 의해 심각도와 발생빈도의 결합에 대한 위험도 수준을 평가하기 위해 수행된다. 이 평가된 결과는 주로 시스템 제품을 설계하거나 유지보수 정책, 유지보수 정비 지원이나 운영방법을 개발하는 SE를 지원하는데 사용된다. 만약 그 위험이 높은 수준의 위험대책을 요구한다면 발생빈도나 가능한 고장결과를 축소하기 위하여 통제되어야 하며 평가된 위험수준이 받아들일 수 있는 수준일 경우 특별한 대책이 필요 없지만 분석결과를 보증하기 위하여 정확히 기록 해 두어야 한다.

3. 적용사례(공압제동장치)

3.1 개 요

철도차량 시스템 측면에서 주요한 서브시스템의 하나인 공압제동장치(Pneumatic braking unit; PBU)에 FMEA-FTA를 기반으로 위험도 평가와 이 평가결과를 기반으로 한 유지보수 정책의 결정에 대한 사례이다. 이는 FMEA-FTA를 기반으로 PBU의 고장모드, 고장원인, 고장영향을 조사하고, 신뢰성을 평가하여 유지보수 정책을 결정하기 위함이다.

3.2 철도차량의 공압제동장치(PBU)

철도차량의 제동장치는 기계제동, 전기제동, 공압(공기)제동 기능이 차량의 형식에 따라 단독 혹은 복합적으로 작용한다. 하지만 PBU는 모든 제동에 대하여 기본적 백업 또는 비상기능을 수행한다. PBU의 목적은 1)속도를 신호 또는 운전자의 요구에 의해 감속, 2) 가능한 더 낮은 운행속도에 도달, 3) 정위치 정차, 4) 차량이나 궤도의 비상상황에 대비한 정차 등으로 PBU는 안전장치의 하나로서 매우 복잡한 프로세스를 갖는다.

다음 Fig. 6은 PBU의 구조로서 부품별 기능으로 AF (Air Filter; 공기휠터)는 주공기통에 포함된 불순물을 필터링하는 역할, BCU(Brake control unit; 제동제어유니트)는 공기제동의 제어공기량을 조절하는 역할, ADV(Automatic drain valve; 자동배수변)는 제어공기에

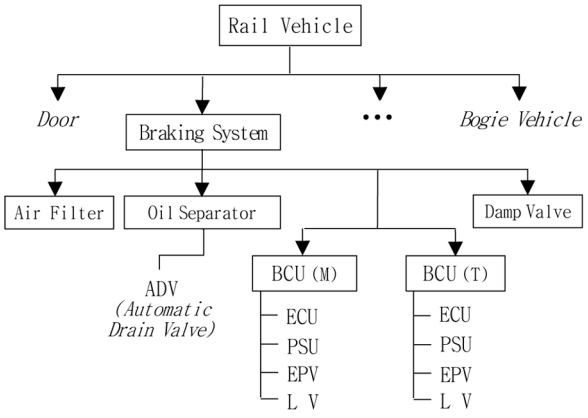

Fig. 6. The structure of PBU.

포함된 수분이나 오일을 분리하는 작용, DV(Dump valve; 덤프밸브)는 차량 차륜(Wheel)이 활주(Skid) 및 미끄러짐 등을 동시에 제어하기 위한 장치로서 승객의 안전을 위해 제동거리를 항상 일정하게 유지하는 역할을 한다[8,11].

3.3 PBU의 위험도 평가

고장저장장치에 수집된 데이터는 PBU의 신뢰성 위험평가를 위하여 현장조사를 통하여 검토하였으며, Table 5는 현장에서 수집된 운영 및 고장데이터이다. 한편 위험도 평가 매트릭스 정의에서 PBU의 위험도 평가를 위해 3가지 요소로 ① 심각도 및 발생빈도 척도의 결정, ② 위험도를 제어하기 위한 위험도 척도, ③ 위험도를 결정하기 위한 평가 매트릭스를 결정한다. Table 1에서 Table 4를 기준으로 평가한 고장결과에 대한 분석(Failure consequence analysis; FCA)은 PBU 구성품의 고장모드에 대해 심각도 결정을 위해 수행되었고 Table 5는 PBU의 심각도 결정을 위하여 수행된 고장결과의 분석 내용이다[1,8].

발생빈도 분석에서 Fig. 7의 고장트리는 중요한 분석 요건으로서 위험도 평가 수행을 위해 양적 및 질적 분석이 요구되고, Table 5는 FMEA 분석 결과에 의한 기본적인 사건을 나타내고 있다. 따라서 서브시스템의 고장모드는 차량 시스템 수준에서 '상용 만제동 에러'(Full service braking error)를 일으킬 수 있는 탑 이벤트(Top event)의 고장을 발생시키는 고장원인을 보여주며, Table 5는 고장모드에 대한 고장원인 시나리오 모델을 설명하고 있다[9].

Table 5. Failure consequence analysis

Subsystem failure mode		Component failure mode		Failure consequence: System	Basic events	Failure sever-ity
F-1	AF	Air filter leakage		function eduction	X_1	2
F-2		Automatic drain valve fail		function reduction	X_2	2
F-3	LV	LV pressure change		function reduction	X_3	2
F-4		LV short		function reduction	X_4	2
F-5	PSU	PSU sensing err		function reduction	X_5	2
F-6		PSU short		function reduction	X_6	2
F-7	ECU	ECU In/output fail		function loss	X_7	3
F-8		Communication err		function loss	X_8	3
F-9		Power supply err		function loss	X_9	3
F-2	EPV	Automatic drain valve fail		function reduction	X_2	2
F-10						
F-8		Pressure sensing error		function reduction	X_{10}	2
F-11		Communication error		function loss	X_8	3
F-12		EPV function error	$_{EPV}$ leakage	function loss	X_{11}	2
			Dreg in $_{EPV}$	function loss	X_{12}	3

Fig. 7에서 탑 이벤트는 5개 실패 이벤트(A1, A2, A3, A4, A5)중에서 임의의 서브시스템이 실패할 때마다 차량 전체 제동장치에 동작오류(T)가 발생할 수 있으며, 탑 이벤트(T)가 낮은 오류 이벤트는 OR 게이트(G1)에 연결되고, AF 기능오류(A1)는 2개 실패원인(X1, X2)이 있으나, 1개 실패원인(X1 또는 X2)에 의해 운영되지 않을 수 있으며 OR 게이트(G2)에 접속되어 있다. LV 감지오류(A2)는 2개 실패원인(X3, X4) 에 의해 초래되고 X3 및 X4가 동시에 발생할 때 작동하지 않으며, AND 게이트(G3) 에 연결되며, PSU 감지오류(A3)는 2개 실패원인(X5, X6)이 동시 발생시 작동이 되지 않으며. AND 게이트(G4)이다. ECU 기능오류(A4)는 3개 실패원인(X7, X8 또는 X9)이 발생하고 이 모든 실패원인(X7, X8 또는 X9)이 발생할 경우에 작동하지 않으며 OR 게이트(G5)가 있다. EPV 기능오류(A5)는 3개 실패원인(X2, X8, X10)과 중간 이벤트(A6)가 있으며, 4개 실패원인(X2, X8, X10, A6)이 동시에 발생할 때 작동하지 않으며, (A5)는 OR게이트(G 6)와 연결되어 있다. Fig.8에서 EPV 함수오류 중간 이벤트(A6)는 2개 실패원인(X11, X12)이 발생하기 때문에(A6)은 AND 게이트(G7)에 연결되어 있다.

질적인 고장트리 분석(Qualitative fault tree analysis; QFTA)은 부울대수 규칙을 적용하여 MCSs를 결정하는 반복적인 절차에 의해 수행된다. Fig. 7의 분석은 식(15)에서 식(22)로 나타낼 수 있다.

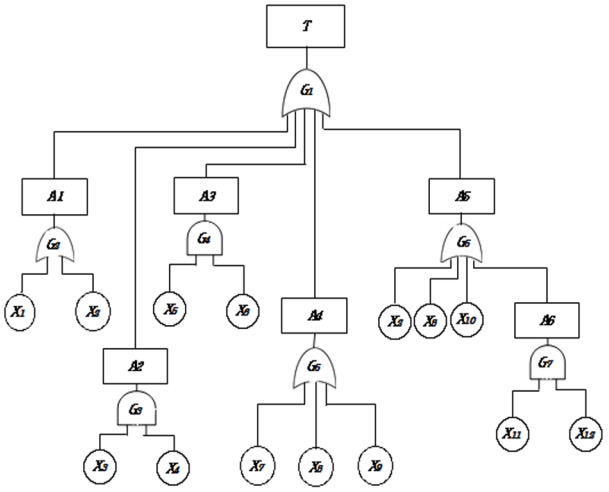

Fig. 7. Failure-tree of PBU.

$$T = A_1 + A_2 + A_3 + A_4 + A_5 \quad (15)$$

$$A_1 = X_1 + X_2 \quad (16)$$

$$A_2 = X_3 \cdot X_4 \quad (17)$$

$$A_3 = X_5 \cdot X_6 \quad (18)$$

$$A_4 = X_7 + X_8 + X_9 \quad (19)$$

$$A_5 = X_2 + X_8 + X_{10} + A_6 \quad (20)$$

$$A_6 = X_{11} \cdot X_{12} \quad (21)$$

$$\begin{aligned} T &= (X_1 + X_2) + (X_3 \cdot X_4) + (X_5 \cdot X_6) \\ &\quad + (X_7 + X_8 + X_9) + (X_2 + X_8 + X_{10}) + A_6 \\ &= X_1 + X_2 + (X_3 \cdot X_4) + (X_5 \cdot X_6) \\ &\quad + (X_7 + X_8 + X_9) + X_{10} + (X_{11} \cdot X_{12}) \end{aligned} \quad (22)$$

Fig. 8를 활용하여 시스템 및 부품의 고장률을 산출하기 위하여 식(23)에서 (28)과 같은 수학적 모델을 마련하였다.

$$F(A_1) = 1 - [1 - F(X_1)] \cdot [1 - F(X_2)] \quad (23)$$

$$F(A_2) = F(X_3) \cdot F(X_4) \quad (24)$$

$$F(A_3) = F(X_5) \cdot F(X_6) \quad (25)$$

$$\begin{aligned} F(A_4) = 1 - [1 - F(X_7)] &\cdot [1 - F(X_8) \\ &\cdot (1 - F(X_9)] \end{aligned} \quad (26)$$

$$F(A_5) = 1 - [1 - F(X_{10})] \cdot [1 - F(A_6)] \quad (27)$$

$$F(A_6) = F(X_{11}) \cdot F(X_{12}) \quad (28)$$

Fig. 7의 고장트리에 대한 MCSs는 Fig. 8과 같이 단순화할 수 있다. 탑 이벤트(상용 만제동 에러)는 9가지

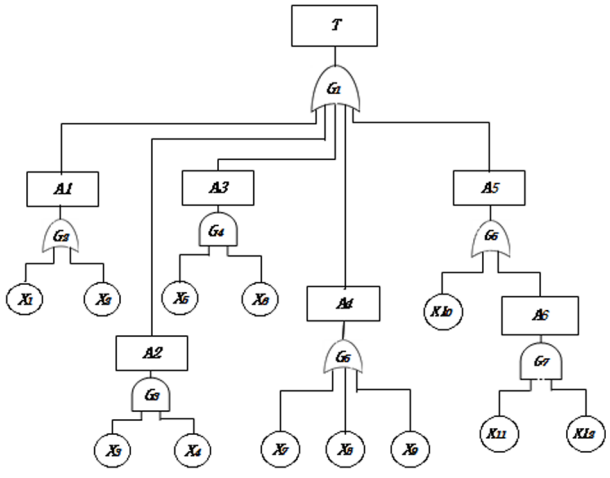

Fig. 8. Fault-tree simplified from [Fig. 8].

Table 6. Failure caused by the failure rate analysis

Sub-system failure mode	Component failure mode	Failure rate	Basic events
AF function loss (A1)	Air filter leakage	2.2×10^{-6}	X_1
	Automatic drain valve fail	1.8×10^{-6}	X_2
LV sensing error(A2)	LV pressure change	2.0×10^{-6}	X_3
	LV short	2.2×10^{-6}	X_4
PSU sensing error(A3)	PSU sensing error	3.0×10^{-6}	X_5
	PSU short	2.8×10^{-6}	X_6
ECU function error(A4)	ECU in/output fail	2.3×10^{-6}	X_7
	Communication error	4.6×10^{-6}	X_8
	Power supply error	2.3×10^{-6}	X_9
EPV function error(A5)	Automatic drain valve fail	1.8×10^{-6}	X_2
	Pressure sensing error	5.8×10^{-6}	X_{10}
	Communication error	4.6×10^{-6}	X_8
EPV operation error(A6)	Dregs in EPV	4.0×10^{-6}	X_{11}
	EPV leakage	5.4×10^{-6}	X_{12}

의 MCSs에 의해 표현할 수 있으며, 6개의 단독고장 을 갖고 3개의 이중고장을 갖는다.

양적인 고장트리 분석으로 부울대수 규칙에 의해 단순화된 식(28)은 고장률과 확률법칙에 의해 양적으로 표현할 수 있고, Table 6은 운영상황에서 수집된 기본적인 이벤트(수준의 고장모드)를 나타낸다[4,10].

Table 7은 MCSs에 대한 시스템 및 서브시스템의 양적인 분석결과로서 Fig. 8의 트리구조를 식(29) 와 같이 수학적 모델을 정의하여 고장률을 산출하였고, 시스템의 위험도를 평가한 결과를 설명하고 있다[7,9].

$$\begin{aligned} F(T) = 1 - [1 - F(A_1)] &\cdot [1 - F(A_2)] \\ &\cdot [1 - F(A_3)] \cdot [1 - F(A_4)] \\ &\cdot [1 - F(A_5)] \end{aligned} \quad (29)$$

위험평가는 FMEA-FTA에 의해 분석된 고장결과의 심각도와 발생빈도를 평가하는 단계로 이 결과에 의해 위험도 수준을 결정하는 것으로 Table 8은 PBU의 위험도 수준을 설명하고 있다.

Table 7. Risks in the system and subsystem level

Component	Tree expression	Failure rate	Frequency level	Severity level	Risk
PBU	**T**	**1.9×10^{-5}**	**2**	**3**	**2**
A F	A1	4.0×10^{-6}	3	2	2
L V	A2	4.4×10^{-12}	1	2	1
PSU	A3	8.4×10^{-12}	1	2	1
ECU	A4	9.2×10^{-6}	3	3	2
EPV	A5	5.8×10^{-6}	3	3	2

Table 8. The risk of PBU parts

Failure code	Failure rate	Frequency level	Severity level	Risk
F-1	2.2×10^{-6}	3	2	2
F-2	1.8×10^{-6}	3	2	2
F-3	2.0×10^{-6}	3	2	2
F-4	2.2×10^{-6}	3	2	2
F-5	3.0×10^{-6}	3	2	2
F-6	2.8×10^{-6}	3	2	2
F-7	2.3×10^{-6}	3	3	3
F-8	4.6×10^{-6}	3	3	3
F-9	2.3×10^{-6}	3	3	3
F-10	5.8×10^{-6}	3	2	2
F-11	4.0×10^{-6}	3	2	2
F-12	5.4×10^{-6}	3	3	3

3.4 분석결과

철도시스템의 위험도 정의에 의해서 FMEA와 FTA의 파라미터를 사용하여 고장에 대한 심각도는 FMEA 분석결과에 대하여 엔지니어링 판단에 의해 평가되었고, 심각도 수준에 대한 발생빈도는 부울대수 규칙 및 고장률을 사용하여 FTA에 의해 평가되었다.

FMEA-FTA 모델에 의해 수행된 PBU의 고장에 대한 위험도는 심각도와 발생빈도 수준의 결합에 의해서 제시되었고, 발생빈도는 위험도 레벨 3 수준(Remote level)으로 나타났으며, 심각도 수준은 레벨 2와 3수준으로 평가되었다. AF, LV, PSU의 심각도는 레벨 2 수준(Marginal level)으로 평가되었고 ECU와 EPV의 심각도는 레벨 3 수준(Critical level)으로 나타났으며 PBU의 전반적인 위험도 수준은 레벨 2 수준으로 나타났다.

PBU의 서브시스템 위험도 수준은 LV와 PSU의 발생빈도는 낮은 고장률로 레벨 1 , 심각도 레벨 2 , 위험도 레벨 1 수준으로 평가되었고 ECU와 EPV는 발생빈도, 심각도, 위험도가 레벨 3 수준이고, AF는 레벨 2 수준으로 평가되었다. 그러므로 PBU의 서브시스템 수준에서의 위험도는 레벨 2 수준으로 평가되었다. 그리고 시스템 수준에서의 심각도는 레벨 3, 발생빈도 레벨 2, 위험도 레벨 2 수준으로 허용할 수 있는 수준인 'Tolerable level'에서 설계가 가능한 것을 확인할 수 있었다. 한편 서브시스템 수준의 고장률은 $10^{-12} < \text{to} \leq 10^{-6}$ 이고, 이는 매트릭스에서 수명주기 단계에서 때때로 발생할 것 같으나 거의 발생되지 않을 것 같은 수준으로 나타났으며, 부품 수준에서는 10^{-6}의 범위로 조사되었으나 이는 수명주기 단계에서 때때로 고장을 일으키는 정도인 'Remote' level인 것으로 평가되었다.

4. 결 론

시스템엔지니어링은 철도시스템에 적용하기 위하여 극복해야 할 상대적인 새로운 엔지니어링 개념으로서 유지보수 관리에 따른 SE 관리 프로세스에 통합되어야 하며, 아울러 주요한 문제점 등을 효과적인 해결방안을 찾기 위해 실용적인 연구방법으로서 노하우나 경험의 범주를 확장할 수 있는 장점이 있을 뿐만 아니라 연구수행을 통해 얻어진 결과를 업데이트 하거나 개선할 수 있는 기회가 주어진다.

따라서 SE의 한 분야로서 철도차량에 장착된 PBU의 위험도를 평가하기 위한 방법으로 FMEA, FTA, ETA 등이 있으나, 본 연구에서는 FMEA- FTA 기반의 평가 모델을 적용하여 어떻게 위험도를 평가할 수 있는지? 또한 어떻게 결정하는가를 보여주었다. 이 FMEA-FTA 위험도 평가 모델은 시스템 설계분석에 효과적으로 적용할 수 있는 방법일 뿐만 아니라, 특히 높은 안전성과 관련된 철도시스템의 불확실한 수준을 평가하는 데 매우 효과적이라 할 수 있다. 그리고 시스템 설계단계에서 적용할 수 있는 데이터나 정보에 따라 양적 및 질적인 평가를 할 수 있다.

본 연구에서는 설계에 대한 성능조건의 정보가 없는 상태에서 제품설계 단계를 적용하였다. 이 연구의 평가 결과가 받아들일 수 있는 수준으로 평가되었으나 위험도 평가에 적합한 데이터와 정보는 RAMS 관리의 도입을 통해 효과적으로 수행할 수 있으므로 RAMS 유지보수 관리의 적극적인 도입이 요구된다.

감사의 글 : 이 연구는 서울과학기술대학교 교내연구비의 지원으로 수행되었습니다(2015).

References

1) IEC 31010. Risk Management-Risk Management Technology, European Norm, 2009.
2) Ericson, C. A. Hazard Analysis Tchniques for Sstem Sfety, Wiley-Interscience, 2005.
3) Andrews, J. Failure-Tree Analysis(FTA), Introduction. 2012 Reliability and maintainability conference, 2012.
4) EN 61025, Failure-Tree Analysis(FTA), European Norm, 2007.
5) G. S. Park, T. W. Kim, H. Y. Jung and . Park, "A Study on the Railway System FMECA Analysis Procedures and Techniques Developed", Korea Association of Auto Technicians Journal, Vol. 10, pp. 753-759, 2009.

6) IEC 62279, Railway Control and Protection Systems for the Software Application of the Rail, International Standard, 2000.
7) IEC 62278. Application of RAMS Specification and Verification of the Railway System, International Standard, 2009.
8) EN 60812, System Reliability Analysis Technology- failure Mode Effect and Analysis(FMEA) Process, European Norm, 2006.
9) J. H. Cha, “A Study on the Improvement of the Pneumatic Brake System with Scheduled Maintenance FMECA”, Seoul National University of Science and Technology, Master's thesis, pp. 68-77, 2010.
10) J. M. Kim, “FTA Study of Commercial Braking System for Ensuring the Safety of the Railway System”, Seoul National University of Science and Technology, Master's thesis, pp. 27-32, 2009.
11) Seoulmetro, Maintenance Manual, pp.1-6, 39-42, 49-52, 2010.