Journal of the Korean Institute of Industrial Engineers
Vol. 42, No. 2, pp. 151-164, April 2016.
ISSN 1225-0988 | EISSN 2234-6457
http://dx.doi.org/10.7232/JKIIE.2016.42.2.151

<Application Research>

시뮬레이션을 이용한 통합전력시스템의 위험도 분석

이지영[1] · 한영진[2] · 윤원영[1†] · 빈재구[3]

[1]부산대학교 산업공학과 / [2]효성 신뢰성기술팀 / [3]국방과학연구소 6본부 2부

Simulation-Based Risk Analysis of Integrated Power System

Ji Young Lee[1] · Young Jin Han[2] · Won Young Yun[1] · Jae Goo Bin[3]

[1]Department of Industrial Engineering, Pusan National University
[2]Reliability Engineering Team, Hyosung Corporation
[3]6-2, Agency for Defense Development

In this paper, we deal with a risk analysis for an IPS (Integrated power system) and propose a simulation model combining the fault tree and event tree in order to estimate the system availability and risk level, together. Firstly, the basic information such as operational scenarios, physical structure, safety systems is explained in order to make the fault tree and event tree of the IPS. Next, we propose a discrete-event simulation model using a next-event time advance technique to advance the simulation time. Also the state transition and activity diagrams are explained to represent the relationship between the objects. By numerical examples, the redundancy allocation is considered in order to decrease the risk level of the IPS.

Keywords: Risk Analysis, Fault Tree Analysis, Event Tree Analysis, Redundancy Allocation, Simulation

1. 서 론

최근 개발되는 해군 함정은 육군의 전차나 공군의 전투기와 달리 수백 개의 무기체계가 유기적으로 연동되면서 임무를 수행하는 복합무기체계로 선체, 추진설비 등과 같은 많은 하위 시스템들이 임무 수행을 위해 독립적 또는 상호보완적으로 작동한다. 따라서 임무의 성공률을 높이기 위해서는 시스템의 고장을 유발하는 주요 하위 시스템들의 고장 발생을 줄이고, 신속한 복구를 통해 임무 기간 동안 함정의 가용도(Availability) 높게 유지하는 것이 중요하다. 함정의 주요 하위 시스템들 중에서 통합전력시스템(Integrated power system)은 다른 하위 시스템의 작동에 필요한 전력을 공급하는 시스템으로, 시스템의 고장이 임무 실패뿐만 아니라 인명 피해를 유발할 수 있다. 특히, 수중 임무를 수행하는 도중에 전력이 공급 되지 않는다면 함정이 수면위로 부상을 하지 못하게 되며 최종적으로 인명 피해를 동반하는 안전사고(Safety accident)가 발생한다. 이와 같이, 통합전력시스템은 함정의 임무 실패와 더불어 승조원의 생명에도 큰 영향을 미치는 주요 시스템이다. 따라서 설계와 개발 단계에서부터 통합전력시스템의 위험 분석(Risk analysis)을 수행하고, 이를 바탕으로 요구되는 목표 위험 수준을 달성하는 안전성 높은 통합전력시스템이 개발되어야 한다. 일반적으로 위험 수준은 안전사고의 발생 빈도와 이로 인해 발생한 피해 규모에 의해 결정되며, 이를 통해 단위 시간 동안 발생 가능한 안전사고의 피해 규모를 산출할 수 있다. 위험 평가를 위해서는 먼저 안전사고를 유발하는 위험 요인을 파악하고, 안전사고의 시작이 되는 사건과 이와 연관되어 있는 각 안전사고의 발생빈도와 피해를 분석한다. 이를 바탕으로 위험 등급을 결정하게 되고 허용범위 내로 존재하도록 안전성 활동을 수행하게 된다. 안전사고를 유발하는 위험 요인을 파악하는 기법으로는 고장나무분석(FTA, Fault tree analysis), 사상나무분석(ETA, Event tree analysis), 고장모드영향분석(FMEA, Failure mode and effect analysis), 위험과 운전분석(HAZOP, Hazard and operability

이 논문은 부산대학교 기본연구지원사업(2년)에 의하여 연구되었음.
† 연락저자 : 윤원영 교수, 46241 부산광역시 금정구 부산대학로 63번길 2 부산대학교 산업공학과, Tel : 051-510-2421, Fax : 051-512-7603, E-mail : wonyun@pusan.ac.kr
2015년 10월 20일 접수; 2015년 12월 26일 수정본 접수; 2016년 1월 24일 게재 확정.

study) 등이 있다. 그 중에서 고장나무분석과 사상나무분석이 보다 높은 안전성이 요구되는 국방과 철도 같은 산업 분야에서 많이 활용되고 있는데, 이는 사건들의 인과관계와 발생 빈도를 통해 최상위사건의 발생확률을 산출할 수 있기 때문이다. 먼저, 고장나무분석은 시스템의 고장인 정상사건(Top event)과 원인들의 관계를 하향식(Top-down)으로 표시하는 분석 방법으로, Ku *et al.*(2008)은 전기 철도에 직접 전력을 공급하는 전차선의 고장 요인 및 신뢰도 산출에 대한 연구를 다루었다. Choi *et al.*(2009)은 열차 방호시스템인 ATP 시스템의 위험원 식별 및 평가를 위해 고장나무분석을 수행하였으며, Seo and Lee(2011)는 전기 모터와 센서 등과 같은 전자 시스템으로 구성된 전기 자동차의 고장 특성과 원인들의 관계 분석을 위해 고장나무분석 기법을 활용하였다. 또한, Byun *et al.*(2012)은 전기 자동차의 조향시스템(Steering system)을 대상으로 고장나무분석을 통해 시스템의 신뢰도를 분석하였으며, Seong *et al.*(2012)은 고장나무분석을 통해 수소 충전소의 안전성 평가 및 개선사항을 도출하였다. 반면, 사상나무는 사고의 발생으로부터 결과로 진행되는 과정을 단계적으로 추론하고 결과를 분석하는 기법으로 Jeon and Kim(2008)은 해군의 초계함(Patrol combat corvette) 내 승조원 침실 화재로부터 전개 가능한 시나리오를 사상나무로 표현하고 각 안전사고의 발생 빈도를 예측하였다. Kwak *et al.*(2008)은 일반철도와 도시철도 운행 시 터널 구간에서 발생하는 화재 사고의 시나리오를 사상나무로 표현하였으며, Choi *et al.*(2008)은 철도 사고로 인한 안전사고의 피해 규모를 감소시키기 위해 사상나무분석으로 위험요인을 규명하고 인명 피해를 분석하였다.

기존 연구들은 고장나무분석과 사상나무분석 중 하나를 시스템의 위험 요인 분석 및 안전사고의 발생빈도 계산에 사용하였다. 그러나 일반적으로 시스템의 안전사고를 유발하는 것은 고장나무분석을 통해 파악된 임무 실패를 유발하는 필수기능의 고장이므로, 이들의 발생 빈도는 연관되어 있는 안전사고의 발생빈도에 영향을 주며 고장나무를 통해 구할 수 있다. 반면, 안전사고의 피해규모는 사고를 제어하기 위해 순차적으로 작동하는 안전시스템(Safety system)의 고장 발생에 영향을 받으며, 이는 시나리오 모델링에 적합한 사상나무분석을 통해 산출 할 수 있다. 따라서 시스템의 보다 정확한 위험 평가를 위해서는 고장나무분석을 사상나무 분석과 연동한 위험 평가 모델을 세우는 것이 중요하다. Park *et al.*(2009)은 철도운행으로 인한 사상사고의 위험 평가를 위해 위험요인을 고장나무로 분석하고, 안전사고의 확대 과정을 사상나무로 표현하였다. Kim *et al.*(2009)은 철도의 건널목 사고의 위험 수준을 평가하기 위해 열차 운행속도로 70km/h 이상으로 운행할 확률을 고장나무분석을 통해 산출하고, 해당 운행속도를 기준으로 발생 가능한 사고 진전 시나리오를 사상나무로 전개하였다. 그리고 Kim *et al.*(2011)은 고장나무분석을 통해 화재 발생 시나리오의 발생 확률을 산출하였으며, 화재 발생으로 전개 가능한 시나리오를 사상나무로 표현한 후 화재/피난 시뮬레이션으로 피해규모(사망자수)를 분석하였다. Kim *et al.*(2012)은 LNG 플랜트에서 인화성 물질의 누출로 인한 사고 발생빈도를 고장나무를 통해 계산하고, 화재나 폭발 사고로 이어지는 과정을 사상나무를 통해 분석하였다. 이와 같이 안전사고의 발생빈도와 각 안전사고의 피해규모가 분석이 되면, 위험 등급을 결정하기 위해 위험도 매트릭스(Risk matrix)가 많이 활용되고 있다.

위험도 매트릭스는 위험 수준에 영향을 주는 안전사고의 발생 빈도와 심각도(Severity)를 매트릭스 형태로 배치하여 위험 등급을 결정하는 방식으로, 주로 대상 시스템의 위험 수준이 수용 가능한지 아니면 안전 대책을 통해 제어를 해야 하는지 파악하기 위해 활용되고 있다. Jo *et al.*(2006)은 발생빈도 6등급과 심각도 4등급으로 구성된 위험도 매트릭스를 이용한 열차제어시스템의 안전성 평가 연구를 소개하였으며, Kim(2013)은 위험도 매트릭스를 이용해서 모노레일 차량 시스템의 위험 수준을 평가하였으며, Song *et al.*(2013)은 화력 발전 설비의 위험 수준을 평가하기 위해 사고 발생과 파손 피해를 5등급으로 구성된 위험도 매트릭스를 제안하고 화력 발전 설비 내 위험한 설비를 평가하였다.

기존의 위험 평가 연구들을 정리하면, 고장나무분석을 통해 시스템의 고장을 유발하는 필수 기능 고장을 파악하고 각 기능의 고장 발생 빈도를 구하였다. 그리고 필수기능의 고장 중에서 안전사고를 유발하는 필수기능의 발생빈도를 바탕으로 안전사고의 발생빈도를 구하였다. 그 다음 사상나무로 파악된 안전시스템의 고장 발생 빈도를 바탕으로 각 안전사고의 피해 규모를 산출하고 최종적으로 위험도 매트릭스를 통해 위험 등급을 결정하였다. 위와 같은 접근 방법은 수리 불가능 시스템(Non-repairable system)의 위험 평가에는 적합하다. 그러나 함정과 같이 수리 가능한 시스템(Repairable system)의 위험 평가에는 보전을 통한 복구가 고려된 위험 평가 모델이 필요하다. 그 이유는 필수 기능과 안전기능의 고장 발생은 보전의 정도(Degree)에 따라 감소될 수 있으며, 고장이 난 안전 시스템의 복구시간 길이에 따라 안전사고를 제어 못할 수도 있다. 예를 들어, 안전사고의 발생빈도와 각 초기사건의 피해 규모 통계량은 초기사건이 발생하였을 경우 또는 이미 발생한 초기사건을 안전기능이 제어하고 있는 상태에서 관련 안전시스템의 고장이 발생한 경우에 업데이트가 된다. 초기사건을 유발하는 기능의 고장이 발생하였을 때 해당 초기사건을 제어할 수 있는 안전기능이 정상적으로 수행되고 있는지 순차적으로 확인하고, 만약 모든 안전기능이 초기사건을 제어할 수 없는 경우 현재 초기사건의 가장 큰 피해규모를 가진다. 반면, 하나의 안전기능이라도 정상적으로 수행하고 있는 경우에는 발생한 초기사건의 제어가 가능하기 때문에 해당 안전기능과 관련된 안전사고의 피해 규모가 현재 초기사건의 피해 규모가 된다. 만약 초기사건을 유발한 고장 난 기능이 복구되기 전에 해당 안전기능의 고장이 발생한다면, 발생한 초기사건을 더 이상 제어하지 못하기 때문에 초기사건은 다시 자신을 제어 가능한 다음 안전기능의 상태를 확인하고 작동 여부에 따라 피해 규모

를 업데이트 하게 된다. 뿐만 아니라, 다양한 임무를 수행하는 함정은 각 임무에 따라 필요한 필수기능이 다를 수도 있으며, 이는 통합전력시스템의 운용 특성에도 영향을 준다. 이와 같은 복잡한 운용 형태와 보전도를 반영해서 안전사고의 발생빈도와 심각도를 분석하기 위해서는 시뮬레이션을 활용하는 것이 적합하다. Han *et al.*(2013)은 함정을 구성하는 정밀화된 구성품 및 복잡한 지원체계를 가진 함정의 RAM 성능을 보다 정확하게 분석하기 위해 유사장비의 실제 운용 데이터와 함정의 운용 조건을 바탕으로 시뮬레이션을 설계하였다. 이에 본 연구에서는 보다 정확하게 함정의 통합전력시스템 위험 평가를 위해 고장나무와 사상나무가 연동해서 안전사고의 발생빈도와 심각도를 산출할 수 있는 시뮬레이션 모델을 제안한다. 시뮬레이션은 객체지향설계(Object-oriented design)기법을 적용한 이산사건 시뮬레이션(Discrete-event simulation)으로 객체간의 관계를 Class diagram, Activity diagram, State diagram으로 통해 표현한다. 본 논문은 다음과 같이 구성된다. 제 2장에서는 고장나무기법과 사상나무기법을 연동한 위험 분석 절차에 대해 설명하고, 제 3장에서는 고장나무와 사상나무가 연동하여 통합전력시스템의 위험도를 평가할 수 있는 시뮬레이션 모형을 제안한다. 그 다음, 제 4장에서는 제안한 시뮬레이션을 이용한 예제 실험 결과를 보여준다. 마지막으로 Section 5에서 본 연구의 결론에 대해 설명한다.

2. 통합전력시스템의 위험도 분석 절차

본 연구에서는 통합전력시스템의 고장 요인과 이로부터 발생 가능한 안전사고의 유형을 분석하고 위험 수준을 정량적으로 평가하기 위해 <Figure 1>과 같은 절차를 제시한다. 위험 수준은 안전사고의 발생 빈도와 사고의 심각도를 바탕으로 산정되며, 발생 빈도는 임무 수행에 필요한 기능들 중에서 안전사고와 관련 있는 기능의 고장 발생과 보전시간 그리고 피해규모는 안전시스템의 고장 발생과 복구 시간에 영향을 받는다. 필수기능과 안전시스템의 고장 발생 빈도는 보전의 정도에 따라 감소가 가능하기 때문에 고장 및 예방 보전에 대한 정보를 분석해야 한다. 그리고 복구 시간은 보전을 수행할 때 이루어지는 절차와 보전 요청에 따른 신속한 처리와 보전자원(수리부속, 정비장비, 정비원)의 가용성에도 영향을 받는다. 따라서 위험 평가를 위해서는 먼저 통합전력시스템의 운용 시나리오, 물리적 구조, 고장 및 예방 보전, 보전절차, 보전지원성에 대한 분석이 필요하다. 그 다음 통합전력시스템의 전력 공급 기능 고장을 정상사건(Top event)으로 정의하고 이를 발생시키는 필수기능의 고장을 분석해서 고장나무를 작성한다. 고장나무에서 기본사건(Basic event)은 하드웨어적으로 고장이 발생하는 중요 부품의 고장모드(Failure mode)로 정의한다. 그리고 고장나무에서 안전사고를 유발하는 필수기능의 고장을 사상나무의 초기사건(Initial event)으로, 안전사고를 제어하기 위한 안전시스템의 기능을 중간사건(Intermediate event)으로 설정해서 통합전력시스템의 안전사고 제어를 위한 시나리오를 사상나무로 표현한다. 고장나무와 사상나무가 작성 되면 고장나무의 기본사건인 중요부품의 고장모드와 안전 시스템의 신뢰도와 보전 정보를 바탕으로 통합전력 시스템의 위험 수준을 산출한다.

2.1 통합전력시스템의 기본 정보 분석

통합전력시스템의 운용 형태를 분석하기 위해서는 먼저 최상위 시스템인 함정의 운용 시나리오를 파악해야 한다. 함정의 운용 시나리오는 다양한 특성을 가진 임무들의 조합으로 구성되어 있지만, 대부분의 임무에서 통합전력시스템은 항상 전력을 공급하기 위해 작동한다. 그러나 함정의 수상 임무와 수중 임무에 전력을 생산하는 방식이 다르며 이에 따라 필요한 하위기능이 달라질 수 있다. 따라서 함정의 임무들을 수상과 수중을 기준으로 분류하고 이들의 조합이 통합전력시스템의 운용 시나리오가 된다. 전력 공급 기능을 수행하기 위해 필요한

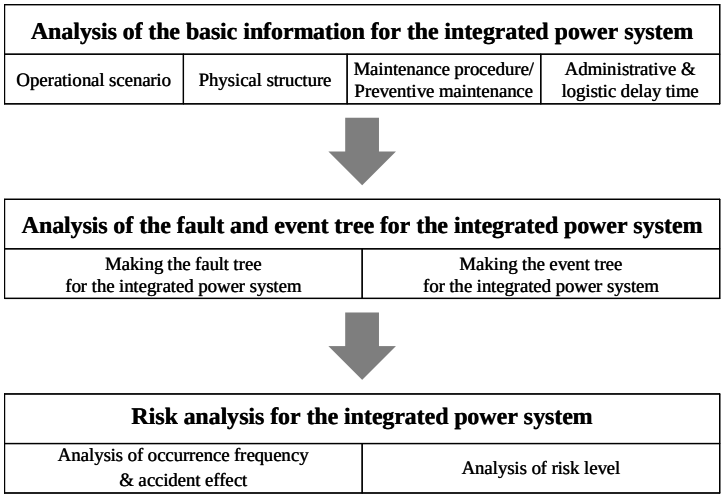

Figure 1. Procedure for Risk Analysis of an Integrated Power System

하위 기능은 크게 전력을 생산하는 '전력 생산 기능', 생산된 전력을 요구하는 전력으로 변환하는 '전력 변환 기능'과 전력 에너지를 전달하는 '전력 배전 기능'으로 정의할 수 있다. 특히 전력 생산 기능이 전력 공급 기능에 중요한 역할을 수행하며 통합전력시스템의 대부분 구성품들이 이를 위해 작동한다. 이에, 본 연구에서는 전력 생산 기능을 중점으로 <Figure 2>와 같이 하위 기능을 분석하고 AND와 OR Gate를 이용해서 전개하였다. 예를 들어, 통합전력시스템은 수상과 수중, 두 가지의 임무로 조합된 운용 시나리오를 수행하며, 각 임무를 달성하기 위해 수상 임무는 전력 생산 기능, 수중 임무는 전력 생산 기능, 전력 변환 기능과 전력 배전 기능 모두 성공적으로 수행되어야 한다.

그리고 통합전력시스템이 수행하는 각 임무에 필요한 기능들의 특성에 따라 작동이 요구되는 구성품이 다를 수 있기 때문에 물리적 구조를 바탕으로 각 필수 기능에 필요한 구성품을 파악해야 한다. 물리적 구조 분석은 설계도면 및 보고서를 기반으로 수행되어야 하며, <Figure 3>은 통합전력시스템의 전력 생산부의 물리적 구조를 예로 보여준다. 최종적으로 최하위 기능을 수행하기 위해 필요한 최하위 구성품의 관계를 <Table 1>과 같은 Matrix로 표현할 수 있다.

2.2 통합전력시스템의 고장나무분석

분석된 통합전력시스템의 운용 시나리오와 임무, 각 임무마다 필요한 기능들과 중요 구성품들을 바탕으로 <Figure 4>와 같이 통합전력시스템의 고장나무를 작성한다. 고장나무는 정상사건, 중간사건과 기본사건으로 구성되어 있으며, 상위 사건과 하위 사건들의 발생 관계는 AND와 OR Gate를 사용해 표현할 수 있다. 통합전력시스템의 고장나무에서 정상사건은 전력 공급 기능의 고장이 되며, 정상사건의 발생에 직접적인 영향을 주는 필수 기능의 고장인 전력 생산 기능 고장, 전력 변환 기능 고장, 전력 배전 기능이 중간사건으로 정의된다. 그리고 하나의 중간사건이라도 발생하면 전력 공급 기능의 고장이 발생하므로 OR Gate로 연결한다. <Figure 4>에서 전력 생산 기능의 고장 사건은 하위 기능 A와 B의 고장 사건이 모두 발생하므로 AND Gate로 연결하고, 하위 기능 A-1 또는 A-2의 고장 사건이 발생하면 상위 기능 A의 고장 사건이 발생하므로 OR Gate로 연결한다. 고장나무에서 최하위기능의 고장을 유발하는 최하위 구성품들의 고장모드가 고장나무의 기본사건이 되므로, 중간사건과 정상사건의 발생확률과 복구시간은 기본사건의 고장시간과 수리시간 정보를 통해 산출 된다.

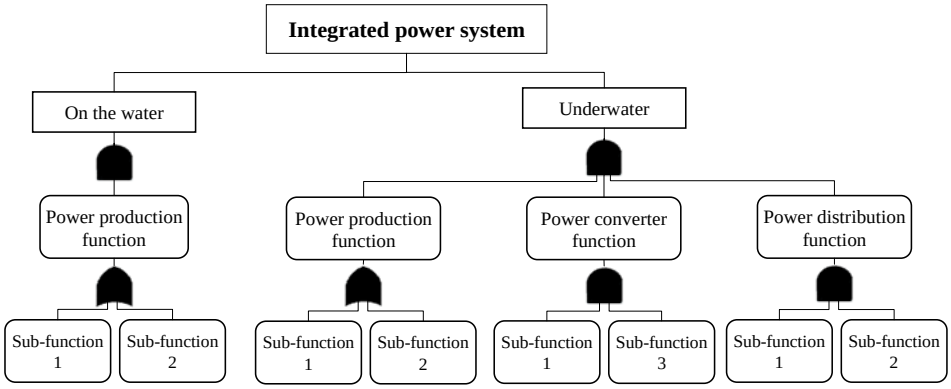

Figure 2. Example of Mapping between Missions and Functions

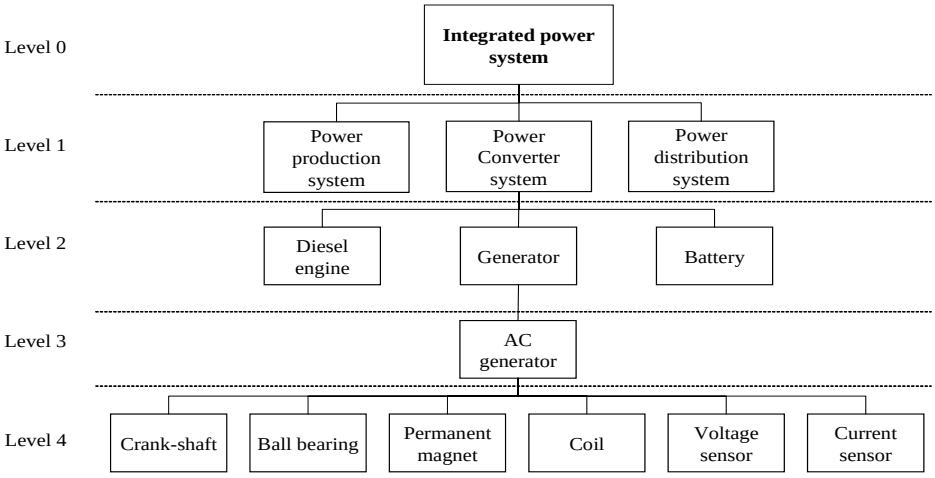

Figure 3. Example of the Physical Structure for the Integrated Power System

Table 1. Example of Mapping between the Essential Functions and Components

	Cooling 1	Temperature sensor 1	Cooling water rotation	Cooling water storage	Pressure measure	Air intake	Temperature sensor 2	Gas emission	Gas rotation	Rev count measure	Power energy transmission	Fuel storage	Fuel rotation	Fuel rotation pressure control	Fuel spray	Fuel spray control	Fuel filter	A magnetic field production	Exiting current production 1	Voltage measure 3	Current measure 3	Rectification	Cooling 1	Automatic voltage control	Voltage measure 1	Current measure 1	Current control	Voltage measure 2	Current measure 2	Frequency measure	Temperature measure	Voltage measure 4	Current measure 4	Voltage measure 5	Current measure 5
Cooling fan 1	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Cooling pump	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Cooling water storage tank	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Cooling fan 2	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×
Temperature sensor	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×
Water temperature sensor	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Fan belt	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Fly wheel	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Intake manifold pressure sensor	×	×	×	×	○	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Intake manifold temperature sensor	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Air filter	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Manifold	×	×	×	×	×	○	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Valve	×	×	×	×	×	○	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Fuel	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Fuel pressure sensor	×	×	×	×	×	×	×	×	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Pressure pump	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Solenoid valve	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Nozzle	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Filter	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Voltage sensor 1	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	○	×	×	○	×	×	×	×	×	×	×	×
Current sensor 1	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	○	×	×	○	×	×	×	×	×	×	×
Voltage sensor 2	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	○	×	×
Current sensor 2	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	○	×
Ball bearing	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Permanent magnet	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Coil	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Diode	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×
MCU	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×
ECU	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	○	×	×	×	×	×	×	×	×
Frequency measurement sensor	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×
Crank-shaft	×	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Crank-shaft position sensor	×	×	×	×	×	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×

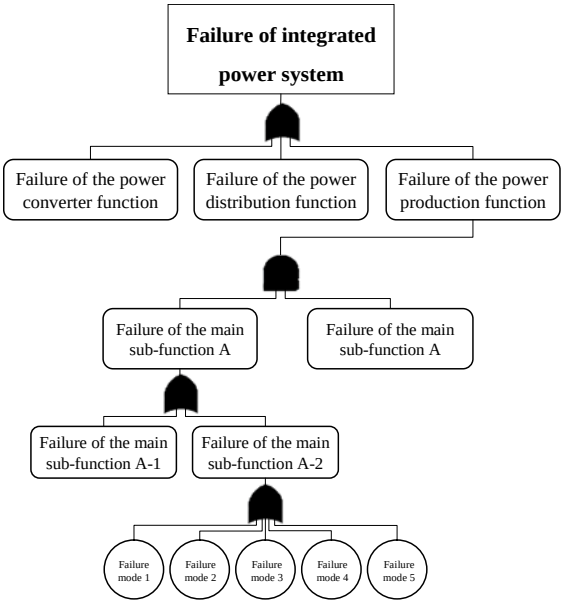

Figure 4. Example of the Fault Tree for the Integrated Power System

2.3 통합전력시스템의 사상나무분석

통합전력시스템의 고장나무를 작성한 다음에는 고장나무의 정상사건(전력공급기능의 고장) 또는 중간사건(필수기능의 고장)으로 인해 발생 가능한 안전사고와 피해규모를 최소화하기 위해 작동하는 안전시스템을 파악하기 위해 사상나무를 작성한다. 사상나무는 초기사건, 중간사건, 안전사고로 구성되어 있으며, 초기사건은 고장나무의 정상 또는 중간사건이 된다. 안전사고의 확산을 제어하고 피해규모를 최소화하기 위해 다양한 종류의 안전시스템이 순차적으로 작동하게 되며, 각 안전 시스템이 수행하는 안전기능이 중간사건이 된다. 통합전력시스템이 전력 공급을 수행하지 못할 때 함정의 부상을 목적으로 작동하는 안전 시스템은 <Table 2>와 같으며 작동순서는 초기사건에 따라 다를 수 있다.

안전사고는 초기사건으로 인해 발생 가능한 인명 피해 및 시스템의 손상 정도를 정량적인 수치와 사고결과의 범주를 설정하여 정의한다. <Table 3>은 통합전력시스템의 고장나무에서 필수기능의 고장 중 하나인 배터리 충전 기능의 고장이 사상나무의 초기사건 중 하나로 설정되고 사건이 발생하였을 때 진행되는 단계를 보여준다. 배터리 충전 기능의 고장이 발생하면, 먼저 주부력탱크기밀이 초기사건을 제어하기 위해 안전기능을 수행하며, 기능이 복구될 때까지 제어가 된다면 배터리 충전 기능의 고장으로 발생된 피해 규모는 0.1명이 되고, 함정의 손실 정도는 10%가 된다. 반면, 기능이 복구되기 전에 주부력탱크기밀의 고장이 발생하면 일반부상계통이 다시 안전기능을 수행하게 되며 제어의 성공이나 실패에 따라 피해 규모가 0.8명 또는 1.5명, 그리고 함정의 손실은 40% 또는 70%가 된다. 이와 같이 통합전력시스템의 고장나무를 통해 고장나무의 정상/중간 사건의 발생빈도를 산출할 수 있으며, 이는 사상나무의 초기사건 발생빈도와 연동된다. 그리고 초기사건이 발생함으로 인해 사고 제어를 위해 작동되는 안전시스템의 고장발생 빈도에 사고의 제어 유/무가 결정되며 최종적으로 안전사고의 피해규모를 해석적으로 구할 수 있다. 그러나 보다 정확한 위험 평가를 위해서는 통합전력시스템의 수상과 수중으로 혼합된 운영시나리오, 보전의 정도에 따른 필수기능과 안전기능의 고장 발생 빈도 감소, 보전시간에 의한 안전사고의 피해규모 등을 고려해야 한다. 이는 시뮬레이션을 통해서 묘사가 가능하므로 제 3장에서는 통합전력시스템의 위험 평가를 위한 시뮬레이션을 설명한다.

Table 2. Types of the Safety Systems in the Warship

Safety system type	Function
Main ballast tank	To keep the level of buoyancy for preventing the leak of the compressed air
General float system	To input the high compressed air on the main ballast tank
Emergency float system	To drain the sea water quickly

3. 통합전력시스템의 위험도 분석 시뮬레이션 설계

제 3장에서는 먼저 통합전력시스템의 운용 특성을 고려한 위

Table 3. Example of the Event Tree for the Integrated Power System

Initiating event	Safety function 1	Safety function 2	Safety accident		
			Type	Effect(Case)	
	Main ballast tank	General float system		Life(Person)	System(%)
Failure of function for the charged battery	Yes	-	Safety accident 1	0.1	10
	No	Yes	Safety accident 2	0.8	40
		No	Safety accident 3	1.5	70
			Total		

험도 분석 시뮬레이션의 입력 정보에 대해 설명한다. 그 다음 시뮬레이션을 구성하는 객체와 사건 설계, 그리고 시뮬레이션 수행 후 산출되는 출력 정보에 대해 설명한다.

3.1 위험도 분석 시뮬레이션 입/출력 정보

본 연구에서 제안하는 위험도 분석 시뮬레이션의 입력은 <Figure 5>와 같이 고장나무와 사상나무에 따라 구분할 수 있다. 고장나무의 정상사건과 중간사건은 시뮬레이션에서 임무(Mission)와 기능(Function), 초기사건은 구성품(Component)으로 정의하고 임무의 조합은 운영시나리오(Operational scenario)에서 사용자가 자유롭게 설계할 수 있다. 사상나무의 초기사건은 시뮬레이션에서 정의한 기능들 중에서 선택하고, 중간사건인 안전기능과 이를 수행하는 안전시스템은 기능과 구성품으로 새로 정의한다. 마지막으로 안전사고는 시뮬레이션에서 안전사고 항목으로 정의하면 된다. <Figure 6>은 시뮬레이션과 고장 및 사상나무의 관계를 Class diagram으로 표현한 것이다.

통합전력시스템과 같은 다기능복합시스템의 RAM(Reliability, Availability, Maintainability) 성능을 시뮬레이션으로 평가하기 위해 필요한 입력 정보는 운영 시나리오, 임무, 기능, 그리고 구성품 등이다(Han *et al.*, 2013). 본 연구에서는 안전사고의 피해 규모를 분석하기 위해 필요한 사상나무의 입력 정보를 설명한다. <Table 4>와 <Table 5>는 위험도 분석 시뮬레이션에서 초기사건과 안전사고에 대한 입력 항목으로 초기사건의 경우 초기사건을 유발하는 기능과 이를 제어하는 안전기능 그리고 발생 가능한 안전사고를 설정한다. 안전사고의 정보는 사고의 발생으로 인한 사고의 심각한 정도를 입력한다.

위험도 분석 시뮬레이션을 통해 안전사고의 발생 빈도 수준과 안전사고를 유발하는 각 초기사건의 심각도 수준을 분석하기 위해서 시뮬레이션 시간 동안 관련 통계량을 수집한다. 본 연구에서 구현한 통합전력시스템 위험도 분석 시뮬레이션의 출력 가능한 정보는 시스템의 성능을 평가할 수 있는 RAM 관련 정보와 시스템의 위험도를 평가할 수 있는 위험도 분석 정보로 다음 <Table 6>과 같이 정의하며, <Figure 7>과 같은 관계를 가진다.

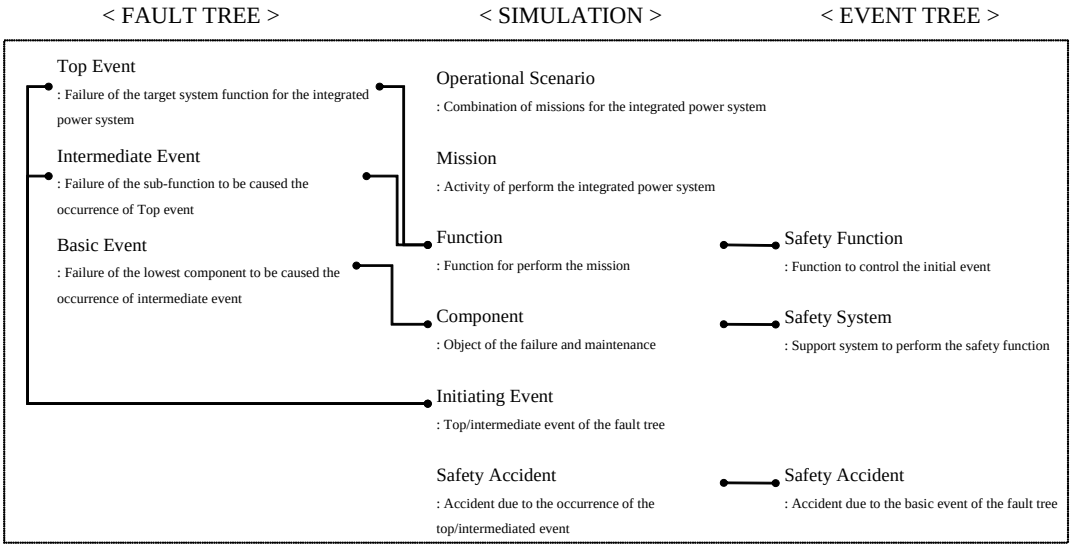

Figure 5. Relationship between Input Module and Fault and Event Trees in the Risk Analysis Simulation

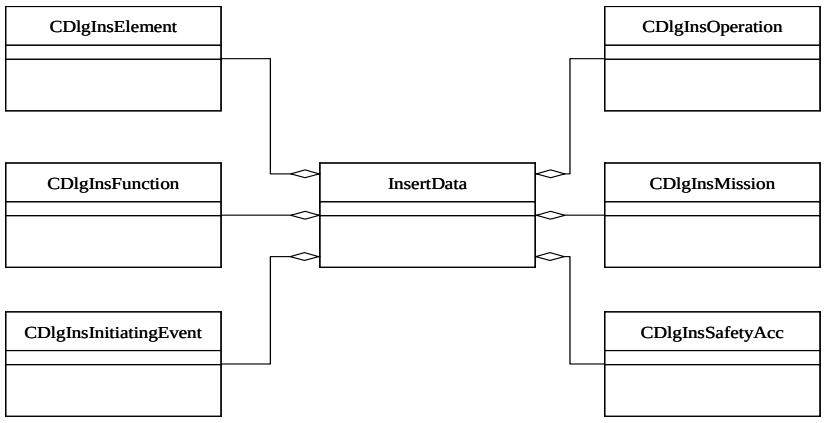

Figure 6. Class Diagram of the Input Information for the Risk Analysis Simulation

Table 4. Input Information of the Initiating Event

Name	Description
ID	Identification of an initiating event
Description	Explanation of an initiating event
Function	Top or intermediate event to be caused the occurrence of an initial event
Safety function	Function to control and reduce the effect of the initial event
Safety accident	Accident to be occurred by occurring the initiating event

Table 5. Input Information of the Safety Accident

Name	Description
ID	Identification of a safety accident
Description	Explanation of a safety accident
Human damage	Degree of human damage for the safety accident

3.2 위험도 분석 시뮬레이션의 객체와 사건 설계

위험도 분석 시뮬레이션에서 임무, 기능, 구성품, 안전사고, 초기사건을 객체로 정의하고, 시뮬레이션 수행 동안 이들의 상호작용에 의해 사건은 진행된다. 각 객체간의 관계를 <Figure 8>과 같이 Class diagram으로 표현 할 수 있다.

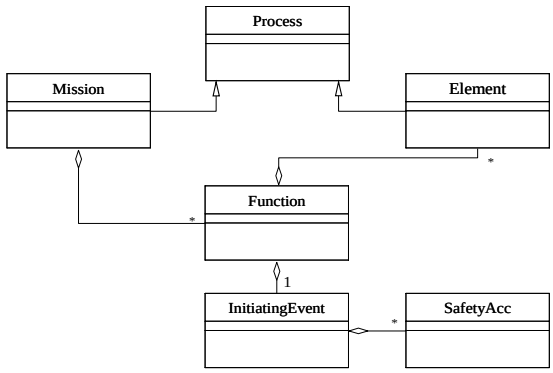

Figure 8. Class Diagram of the Objects in the Risk Analysis Simulation

Table 6. Output Statistics of the Risk Analysis Simulation

Category			Description
RAM		Total run time	Total run time of normal operating during perform the simulation
		Total down time	Total down time due to failure of the integrated power system during perform the simulation
		Total failure number	Total failure number of the integrated power system during perform the simulation
		Availability	Availability for the integrated power system
RISK	Initiating event	Occurrence frequency	Occurrence frequency of an initiating event
		Occurrence frequency index	Occurrence frequency index of an initiating event(5 Step)
		Risk level	Risk level for the initiating event
	Safety accident	Severity degree	Severity degree of an initiating event
		Severity degree index	Severity degree index of an initiating event according to the accident result (5 Step)
	Risk level		Risk level for the integrated power system

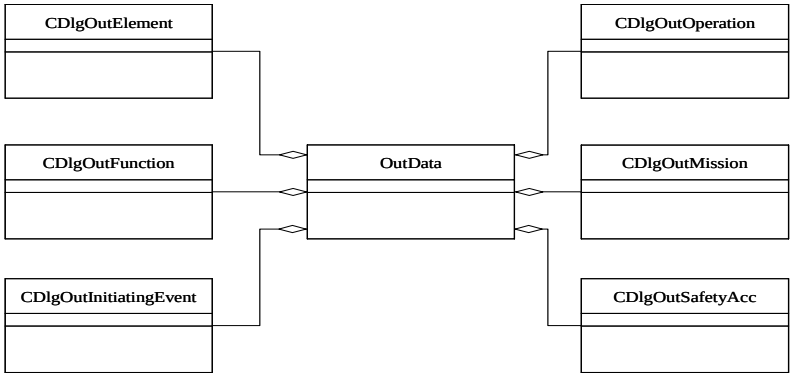

Figure 7. Class Diagram for the Output Information of the Risk Analysis Simulation

각 클래스는 속성(Attribute)과 멤버함수(Member function)를 가지며, 객체의 속성은 <Table 7>과 같이 정의한다. 각 객체의 공통적인 속성은 자신을 나타내는 ID와 현재 자신의 상태를 나타내는 변수가 있다. 임무, 기능, 구성품의 상태는 가동(RUNNING), 고장(DOWN), 유휴 (IDLE)로 표현할 수 있으며, 초기사건과 안전사고의 상태는 발생(Occurrence)과 발생하지 않음(NonOccurrence)으로 표현한다. 여기서 유휴 상태란, 만약 기능이 유휴 상태에 놓이면 기능을 이루고 있는 하위 기능 또는 구성품의 고장이 발생하지 않은 것을 의미한다. 그러나 시뮬레이션 수행 동안 통합전력시스템의 상태는 운영되는 전체 시간 동안 가동과 고장의 상태만 가능하며 유휴 상태로 놓이지는 않는다. 또한 기능, 초기사건, 구성품 객체들은 <Figure 9>와 같이 자기 자신만이 상태를 변경 시킬 뿐 아니라 다른 객체들과 유기적인 관계를 가지고 상호작용을 한다.

위험도 분석 시뮬레이션의 로직에서 메서드 실행 내용 및 로직을 <Figure 10>～<Figure 12>와 같은 Activity diagram으로 표현할 수 있다. <Figure 10>은 구성품의 execute가 실행되는 Logic으로 구성품이 가지는 사건의 종류는 고장 발생(Breakdown)과 수리 완료(Endfix)가 있으며, 고장 발생이라면 상위 기능에게 자신의 고장을 전달하기 위해 *noticeDown*을 호출한다. 그 다음 <Figure 11>과 같이 상위 기능의 고장 여부에 따라 상태가 변경되는데, 만약 기능의 고장이 발생하지 않는다면, 더 이상 진행되는 단계는 없다. 고장이 발생한다면, 해당 기능의 상태를 RUNNING에서 DOWN으로 변경하고 종류(안전기능 또는 초기사건)에 따라 다른 흐름으로 시뮬레이션이 진행 된다. 해당 기능이 안전기능인 경우에는 현재 제어하고 있는 안전사고가 있다면, 현재 상태가 Down이므로 안전사고의 제어가 불가능하므로 초기사건의 심각도를 업데이트 한다. 반면, 초기사건이라면 <Figure 12>와 같이 초기사건의 상태를 발생으로 변경하고 안전기능의 상태 확인을 통해 초기사건의 심각도를 업데이트하기 위해 초기사건의 *execute*를 호출한다. 그 다음 해당 기능이 최상위기능이라면, 고장이 발생하지 않은 하위 기능 또는 구성품의 동작을 중지시키고 상태를 IDLE로 변경하기 위해 기능 또는 구성품의 *deactivated*를 호출한다. 만약

Table 7. Attribute of the Safety Accident and Initiating Event in the Risk Analysis Simulation

Category	Name	Description
Safety accident	ID	Identification of a safety accident
	Description	Explanation of a safety accident
	HumanDamage	Degree of human damage for the safety accident
	NumOccur	Number of occurrences for the safety accident
initiating event	ID	Identification of an initiating event
	Description	Explanation of an initiating event
	NumSafetyFunc	Number of the safety functions controllable the initiating event
	SafetyFunc	Identification of the controllable safety function
	NumSafetyAcc	Number of the safety accidents due to the initiating event
	SafetyAcc	Identification of the safety accident
	NumOccur	Total number of occurrences of the initiating event
	CurSeverity	Degree of the human damage for the present initiating event

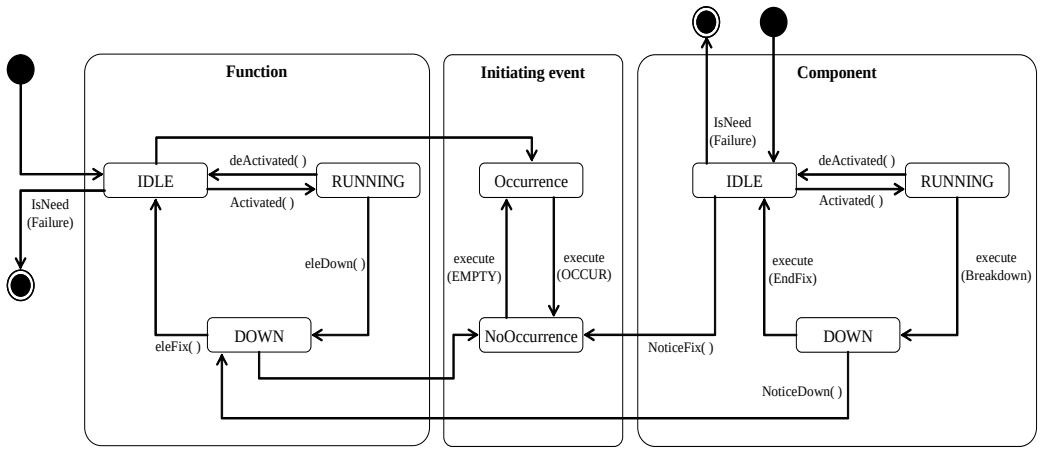

Figure 9. State Diagrams of the Function, Initiating Event and Component

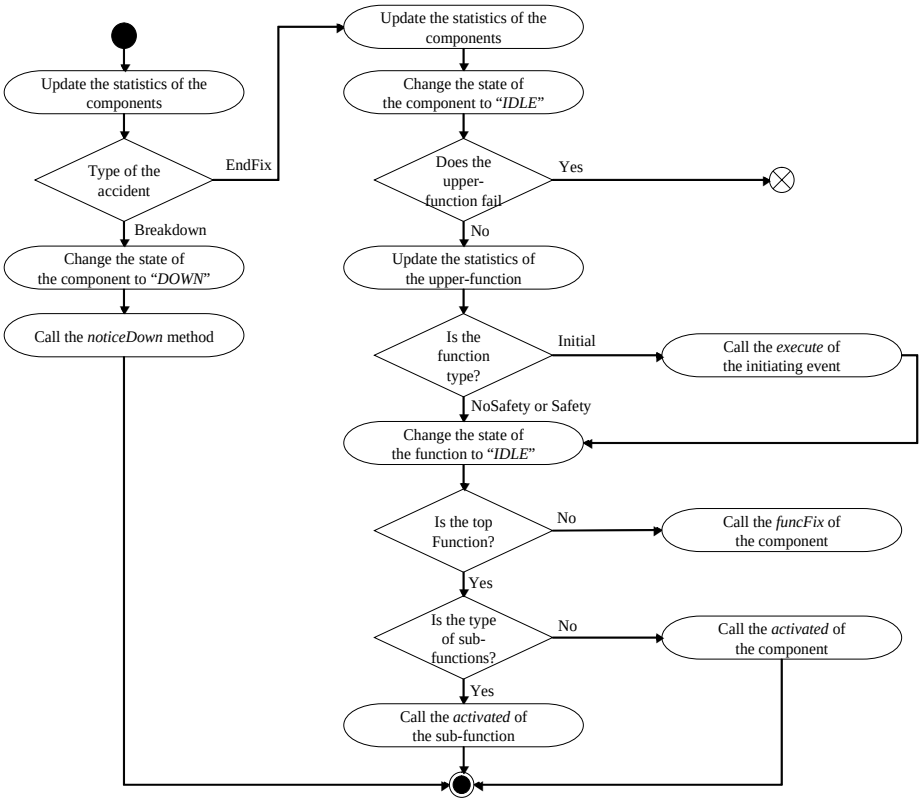

Figure 10. Activity Diagram of the Element *execute*

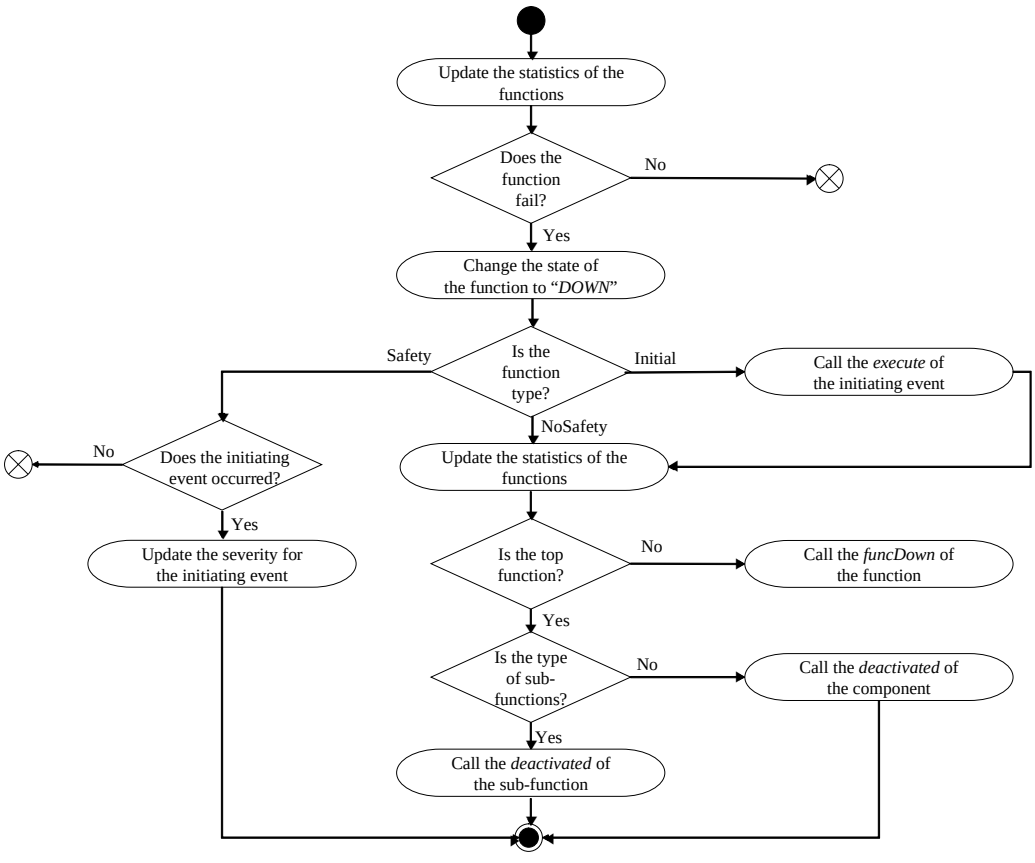

Figure 11. Activity Diagram of the *noticeDown*

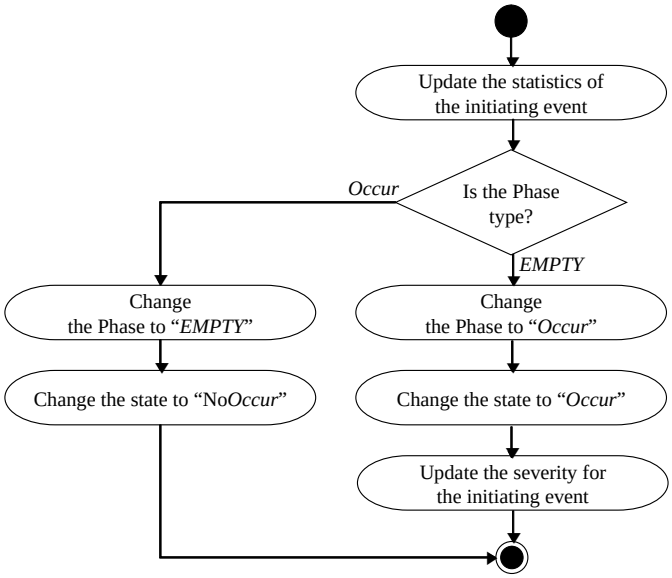

Figure 12. Activity Diagram of the Initial Event *execute*

최상위기능이 아니라면, 상위 기능에 자신의 고장을 알리기 위해 *funcDown*를 호출하고 이는 최상위 기능에 도달할 때까지 반복해서 진행된다. <Figure 10>에서 발생된 구성품의 사건이 수리 완료(EndFix)라면, 구성품의 상태를 DOWN에서 IDLE로 변경하고 상위 기능의 고장 여부를 확인한다. 구성품의 수리로 상위 기능이 복구가 안 된다면, 더 이상 진행되는 단계는 없다. 만약 복구가 가능하다면, 상위 기능의 상태를 IDLE로 변경한 후 다시 상위 기능에 자신의 상태 변경을 알리는 *funFixed*를 호출한다. 이는 최상위기능에 도달할 때까지 반복해서 진행이 된다. 또한, 해당 기능이 초기사건으로 설정이 되어 있다면, 심각도 업데이트를 위해 *execute*를 호출한다. 만약 최상위기능이라면 자신의 고장으로 인해 작동이 중지된 하위 기능 또는 구성품을 작동시키는 위해 기능 또는 구성품의 *activated*를 호출한다.

4. 시뮬레이션을 이용한 통합전력계통의 위험도 분석 실험

제 4장에서는 본 연구에서 제안한 시뮬레이션을 이용한 통합전력시스템의 위험 수준 분석 실험에 대해 설명한다. 실험 예제의 통합전력시스템은 고장나무분석을 통해 전력 공급 기능의 고장을 유발하는 구성품은 32개이며, 사상나무분석을 통해 안전사고 발생 시 사고를 제어하고 함정을 수상으로 부상시키는 안전시스템은 3개로 분석되었다. 시뮬레이션을 이용하여 통합전력시스템 위험도 분석을 수행하기 위해 필요한 운용 시나리오, 물리적 구조를 분석하고, 사고의 원인 분석과 사고로부터 발생할 수 있는 안전사고는 고장나무기법과 사상나무기법을 통해 전개하였다. 이러한 정보는 제 2장에서 분석된 내용을 기반으로 한다.

4.1 위험도 분석 시뮬레이션을 이용한 예제 실험

고장나무의 기본사건은 최하위 기능의 고장을 유발하는 중요부품의 고장모드(Failure mode)를 고려하였으며, 고장모드와 안전시스템의 고장이 발생하는 시간과 복구시간은 지수분포를 따른다고 가정하였다. 실제 함정에서 사용되는 구성품 및 안전시스템의 신뢰도 데이터 획득의 어려움이 있어 구성품의 MTBF(Mean time between failure)는 함정이 임무를 수행하는 단위시간 25년, 그리고 안전시스템의 MTBF는 수중을 수행하는 단위시간 12.7년 동안 신뢰도 60~70%를 만족하는 값을 임의로 입력하였다. 그리고 하나의 구성품이 가지는 고장모드의 수가 2개 이상인 경우 확률 값을 임의로 할당하였으며, 시뮬레이션에서는 주어진 확률 값에 따라 고장모드가 발생한다. 고장모드와 안전시스템의 MTTR(Mean time to repair)은 10~20시간 사이의 값을 임의로 입력하였다. 실험 예제의 시뮬레이션 수행 시간은 219,000시간(25년)이며, 반복은 총 100회 수행하였다. 통합전력시스템의 구성품을 단일로 구성하였을 때(실험 (1))와 위험도 개선을 위해 구성품을 중복할당 하였을 때(실험 (2))로 구분하여 위험도 분석 시뮬레이션을 통해 확인하였다. 실험 (2)의 경우 구성품을 중복 대상을 선정하기 위해 기여도 평가를 실시하였다. 기여도 평가는 통합전력시스템의 구성품이 단일로 구성된 경우의 가용도로부터 각 구성품의 중복으로 인해 증가되는 가용도가 큰 구성품부터 차례대로 1개씩 중복할당하여 설정하였다. 그리고 실험 (3)은 모듈을 중복 할당하여 위험도 개선을 확인한다. 실험 (2)와 동일한 방법으로 기여도 평가 후 중복 대상을 설정하여 중복 할당하여 중복 수량을 설정하였다. <Table 8>는 기본 사상과 안전시스템의 MTBF, MTTR의 기준 값 및 고장모드의 발생확률과 실험별 중복 수량을 정리한 표이다.

Table 8. Input Data of the Risk Analysis Simulation of Components

Module	Component	MTBF(h)	MTTR(h)	Failure mode	Probability	Case (1)	Case (2)	Case (3)
Cooling system	Cooling fan 1	2,939	13	Failure mode 1	1.0	0	1	2
	Water temperature sensor	3,133	14	Failure mode 2	1.0	0	0	
	Fan belt	3,156	11	Failure mode 3	1.0	0	2	
	Fly wheel	2,716	11	Failure mode 4	1.0	0	1	
	Cooling pump	2,950	15	Failure mode 5	1.0	0	2	
	Cooling water storage tank	3,011	13	Failure mode 6	1.0	0	2	
	Cooling fan 2	3,047	17	Failure mode 34	1.0	0	0	
	Temperature sensor	2,828	20	Failure mode 38	1.0	0	0	
Intake system	Intake manifold pressure sensor	2,581	16	Failure mode 7	0.3	0	2	1
				Failure mode 8	0.7	0		
	Air filter	2,618	14	Failure mode 9	1.0	0	1	
	Manifold	2,765	12	Failure mode 10	0.4	0	0	
				Failure mode 11	0.6	0		
	Valve	2,534	12	Failure mode 12	0.6	0	0	
				Failure mode 13	0.4	0		
	Intake manifold temperature sensor	2,744	11	Failure mode 14	1.0	0	2	
Fuel system	Fuel	3,096	15	Failure mode 17	1.0	0	0	1
	Fuel pressure sensor	2,414	20	Failure mode 18	0.2	0	1	
				Failure mode 19	0.8	0		
	Pressure pump	2,850	12	Failure mode 20	1.0	0	0	
	Solenoid valve	2,953	14	Failure mode 21	1.0	0	1	
	Nozzle	2,952	10	Failure mode 22	1.0	0	0	
	Filter	2,970	18	Failure mode 23	1.0	0	0	
AC generator	Crank-shaft position sensor	3,080	16	Failure mode 15	1.0	0	0	3
	Crank-shaft	2,506	18	Failure mode 16	1.0	0	2	
	Ball bearing	2,321	19	Failure mode 24	1.0	0	2	
	Permanent magnet	2,264	10	Failure mode 25	1.0	0	0	
	Coil	2,675	15	Failure mode 26	1.0	0	2	
	Voltage sensor 1	3,182	19	Failure mode 27	0.3	0	0	
				Failure mode 28	0.2	0		
				Failure mode 29	0.5	0		
	Current sensor 1	2,891	10	Failure mode 30	0.4	0	1	
				Failure mode 31	0.3	0		
				Failure mode 32	0.3	0		
	Diode	2,345	14	Failure mode 33	1.0	0	2	
	MCU	2,310	16	Failure mode 35	1.0	0	2	
	ECU	2,423	13	Failure mode 36	1.0	0	1	
	Frequency measurement sensor	2,919	20	Failure mode 37	1.0	0	0	
	Voltage sensor 2	2,885	15	Failure mode 39	0.4	0	0	
				Failure mode 40	0.6	0		
	Current sensor 2	2,887	17	Failure mode 41	0.3	0	0	
				Failure mode 42	0.7	0		
Safety system	Main ballast tank	1,154	19	-	-	-	-	-
	General float system	1,288	12	-	-	-	-	-
	Emergency float system	1,308	17	-	-	-	-	-

Table 9. Results of the Risk Analysis Simulation

Category		Initiating event		Safety accident		Risk level[3]
		Occurrence frequency	Occurrence frequency index[1]	Severity degree	Severity index[2]	
Case (1)	Failure of function for the charged battery	0.0127	5	0.1097	3	15
	Failure of function for the rectification	0.0056	5	0.4109	3	15
	Integrated power system	0.0183	5	0.2331	3	15
Case (2)	Failure of function for the charged battery	0.0053	5	0.1031	3	15
	Failure of function for the rectification	0.0039	5	0.4000	3	15
	Integrated power system	0.0092	5	0.2024	3	15
Case (3)	Failure of function for the charged battery	0.0067	5	0.1121	3	15
	Failure of function for the rectification	0.0042	5	0.4012	3	15
	Integrated power system	0.0109	5	0.2217	3	15

Occurrence frequency index[1] : 초기사건의 발생빈도에 따라 최소 1등급에서 최대 5등급으로 분류
Severity index[2] : 사고 발생으로 인해 발생하는 사고의 피해규모 또는 심각 정도를 최저 1등급에서 최고 5등급으로 분류
Risk index[3] : 발생빈도와 심각도의 곱으로 산출 (Occurrence frequency index×Severity index)

4.2 통합전력시스템의 위험도 분석 결과

<Table 9>은 통합전력시스템의 위험도 분석 시뮬레이션을 통해 산출된 결과이다. 실험을 통해 구성품이 단일로 구성된 통합전력시스템(실험 (1))보다 구성품의 중복으로 구성된 통합전력 시스템(실험 (2))의 초기사건별 단위 시간당 발생 빈도와 안전사고의 심각 정도가 더 낮음을 알 수 있다. 그 이유는 통합전력시스템의 구성품 중복으로 인해 구성품의 고장 발생 빈도를 감소시킴으로써 위험도를 감소시키기 때문이다. 통합전력시스템의 모듈 중복을 고려한 실험 (3)의 경우, 실험 (1)과 실험 (2)의 사이 값이 산출 되었다. 단일 구성품을 고려한 경우보다 모듈 중복을 설정하였을 때 초기사건의 발생 빈도가 감소되었으나 구성품 단위를 중복 설정하였을 때보다는 높은 발생 빈도가 발생하였다. 그 이유는 구성품 단위로 중복 할당하는 것이 모듈 단위 중복 할당보다 전체의 가용도를 향상시키므로 가용도에 따라 초기사건의 발생 빈도가 변화되는 것을 알 수 있다.

5. 결 론

함정의 통합전력시스템은 다른 하위 시스템들의 작동을 위해 필요한 전력을 공급하는 기능을 수행하는 주요 시스템으로 시스템의 고장은 임무 실패뿐만 아니라 승조원의 생명 피해를 유발할 수 있다. 따라서 설계와 개발 단계에서부터 정량적인 위험 분석이 수행되고 결과를 바탕으로 요구되는 위험 수준을 만족하는 시스템이 개발되어야 한다. 위험 수준은 사고의 발생 빈도와 피해 규모를 바탕으로 산출되므로, 기존 연구에서는 고장나무분석과 사상나무분석을 통해 위험 요인을 분석하고 해석적으로 사고의 발생 빈도를 산출하고 피해 규모를 분석하였다. 그러나 보다 정확하게 위험 수준을 평가하기 위해서는 고장나무를 통해 임무 실패를 유발하는 필수 기능의 고장을 정의하고, 이를 통해 유발된 안전사고가 확산되는 과정과 제어를 위해 작동하는 안전시스템을 사상나무로 표현된 위험 분석 모델이 필요하다. 이에, 본 연구에서는 고장나무 기법과 사상나무분석기법을 연동한 통합전력시스템의 위험도 분석 절차를 제시하였다. 먼저 고장나무와 사상나무를 작성하기 위해 필요한 기본 정보(운용 시나리오, 물리적 구조, 안전 시스템)를 분석한다. 그리고 전력 공급 기능의 고장을 정상사건으로 정의하고 이를 유발하는 하위 기능의 고장 분석을 통해 고장나무를 작성한다. 사상나무 작성을 위해서 고장나무의 정상 또는 중간사건을 초기사건으로 설정하고, 이로부터 발생 가능한 안전사고를 정의함으로써 고장나무와 사상나무가 결합이 된다. 연동된 고장나무와 사상나무를 통해 위험 수준을 산출하기 위해서는 통합전력시스템의 운용 환경, 중요 구성품과 안전시스템의 고장 및 보전 특성을 반영해야 하므로 수리적으로 계산하기에는 어려움이 있다. 따라서 본 연구에서는 이러한 복합적인 요소를 묘사하기 위해 객체지향설계 기법으로 설계된 위험도 분석 시뮬레이션을 제안하였으며, 시뮬레이션을 구성하는 객체들의 관계를 표현하기 위해 다양한 Diagram을 활용하였다. 제안한 위험도 분석 시뮬레이션을 활용하여 실험 예제를 통해 통합전력시스템의 사상나무에서 두 개의 초기사건의 위험 수준을 평가하였으며, 구성품과 모듈 단위의 중복 설계를 통해 위험도를 구성하는 초기사건의 발생 빈도와 심각 정도가 감소됨을 알 수 있었다.

본 연구에서 수행한 실험 예제는 통합전력시스템의 구성품과 모듈 단위로 중복 설계하여 위험도 분석을 수행하였지만 추후 통합전력시스템의 구성품 중요도를 고려하여 고장 발생 빈도를 개선시키거나 모듈 중복 설계를 통하면 더 효과적인 설계 대안을 제시할 수 있을 것이다. 통합전력시스템의 고장

분석과 안전시스템에 대한 더 자세한 정보와 통합전력시스템에 적합한 발생 빈도 및 심각도 범주를 설정한다면 본 연구에서 구현한 위험도 분석 시뮬레이션을 통해 위험도 개선 연구에 도움이 될 것이라 기대한다.

참고문헌

Byun, S. I., Yang, I. S., Seo, B. S., and Lee, D. I. (2012), Analysing steering system reliability using dynamic fault tree analysis, *Journal of the Korean Society of Automotive Engineers*, 1290-1294.

Chi, M. G., Lee, E. C., and Bahng, K. I. (2010), Evaluation of single point vulnerability using failure analysis of auxiliary power system in nuclear power plants, *The Transactions of the Korean Institute of Electrical Engineers*, 780-781.

Choi, D. B., Wang, J. B., Kwak, S. L., Park, C. W., and Kim, M. S. (2008), Development of the risk assessment model for train collision and derailment, *Journal of the Korean Society for Railway*, 1505-1510.

Choi, J. R., Kim, Y. S., and Shin, S. K. (2009), SIL assessment and validation of ATD on-board system using fault tree analysis, *Journal of the Korean Society for Railway*, 1439-1447.

Han, Y. J., Yun, W. Y., You, J. W., Choi, C. H., and Kim, H. W. (2013), Simulation-based reliability and maintainability design of a warship, *Journal of the Korean Institute of Industrial Engineers*, **39**(6), 461-472.

Heo, E. J. and Kang, H. K. (2012), FMEA for risk assessment of marine electric propulsion system, *Journal of the Korean Society of Marine Engineering*, 227-231.

Hwang, J. G., Jo, H. J., Han, C. H., Cho, W. S., Ahn, J., and Ha, D. M. (2010), A study on the HAZOP-KR for hazard analysis of train control systems, *Journal of the Korean Society for Railway*, **13**(4), 396-403.

Jeon, G. R. and Kim, D. J. (2008), A study on risk assessment for fire onboard a naval vessel, *Journal of the Korean Institute of Fire Science and Engineering*, **22**(5), 35-42.

Jo, H. J., Hwang, J. G., and Yoon, Y. K. (2006), Risk assessment method for guaranteeing safety in the train control system, *Journal of the Korean Society for Railway*, 60-67.

Jung, H. J. and Lee, J. C. (2012), On the safety analysis of high speed railway systems using the hazard and operability(HAZOP) technique, *Korea Safety Management and Science*, 527-534.

Kim, D. H. and Lee, J. W. (2012), Study on the hazard analysis in lineside electronic unit system, *Journal of the Korean Society for Railway*, 706-711.

Kim, H. B., Hee, S. K., Kim, K. S., and Kim, J. H. (2011), Application of ETA(Event Tree Analysis) to the performance-based design of fire protection, *Korean Institute of Fire Science and Engineering*, 454-457.

Kim, M. B., Choi, B. I., Han, Y. S., Do, K. H., Kim, T. H., and Lee, Y. H. (2012), Hazard evaluation and analysis for LNG storage tank, *Journal of the Korean Society of Mechanical Engineers*, 1417-1422.

Kim, M. H., Jin, E. J., and Park, M. G. (2013), Fault tree analysis and fault modes and effect analysis for security evaluation of IC card payment systems, *Journal of Korea Multimedia Society*, **16**(1), 87-99.

Kim, M. S., Wang, J. B., Park, C. W., and Cho, Y. O. (2009), Development of the risk assessment model for railway level-crossing accidents by using the ETA and FTA, *Journal of the Korean Society for Railway*, **12**(6), 936-943.

Kim, Y. S. (2013), *A Study on Methodology for the Risk Assessment of Monorail Vehicle System*, Ph.D Thesis, Seoul National University of Science and Technology.

Ku, B. H., Cha, J. M., and Kim, H. C. (2008), Reliability analysis of catenary of electric railway by using FTA, *The Transactions of the Korean Institute of Electrical Engineers*, **57**(11), 1905-1909.

Kwak, S. L., Wang, J. B., Lee, B. S., and Park, C. W. (2008), Construction of event tree and fault tree for train fire risk assessment, *The Korean Society for Railway*, **11**(6), 530-535.

Lee, C. H., Yang, K. W., and Kim, S. B. (2012), Reestablishment of RPN evaluation method in FMEA procedure for K21, *Journal of the Korean Society for Quality Management*, **40**(3), 306-315.

Lee, D. S. (2010), *Study for Reliability improvement of Belt Type Door System using FMECA*, Master's Thesis, Seoul National University of Science and Technology.

Park, C. W., Wang, J. B., Kim, M. S., Choi, D. B., and Kwak, S. L. (2009), Development of risk assessment models for railway casualty accidents, *The Korean Society for Railway*, **12**(2), 190-198.

Seo, B. S. and Lee, D. I. (2011), Analysis of electric vehicle fault mode using fault tree analysis, *The Korean Society of Automotive Engineers*, 1239-1242.

Seong, D. H., Rhie, K. W., Kim, T. H., Oh, D. S., Oh, D. H., Kim, Y. G. and Kim, E. J. (2012), Quantitative safety assessment for hydrogen station, *Journal of the Korean Society of Safety*, **27**(3), 111-116.

Soman, R. R., Davidson, E. M., and McArthur, S. D. J. (2009), Using functional failure mode and effects analysis to design the monitoring and diagnostics architecture for the zonal MVDC shipboard power system, *Electric Ship Technologies Symposium*, 123-128.

Song, G. W., Kim, B. S., Choi, W. S., and Park, M. S. (2013), Prediction of maintenance period of equipment through risk assessment of thermal power plants, *Journal of the Korean Society of Mechanical Engineers*, **37**(10), 1291-1296.