대한조선학회논문집
Journal of the Society of Naval Architects of Korea
pISSN:1225-1143, Vol. 55, No. 3, pp. 222-235, June 2018
eISSN:2287-7355, https://doi.org/10.3744/SNAK.2018.55.3.222

모델기반 시스템엔지니어링을 활용한 해양플랜트 안전시스템(SIS, Safety Instrumented System)의 신뢰도 분석 및 안전설계 지식 모델링

배정훈[1] · 정민재[2,†] · 신성철[1]
부산대학교[1]
한국선급[2]

Knowledge Modeling of Reliability Analysis and Safety Design for Offshore Safety Instrument System with MBSE (Model-Based Systems Engineering)

Jeong-hoon Bae[1] · Min-jae Jung[2,†] · Sung-chul Shin[1]
Pusan National University[1]
Korean Register[2]

The hydrocarbon gas leak in the offshore plant can cause large accidents and lead to significant damages to human, property and environment. For prevention of fire or explosion accidents from gas leak, a SIS(Safety Instrumented System) should be installed. In the early stage of the offshore design, required SIL(Safety Integrated Level) is determined and reliability analysis is performed to verify the design in reliability aspects. This study collected data, information related to reliability analysis and created knowledge model of safety design for the offshore system with MBSE(Model-Based Systems Engineering) concept. Knowledge model could support safety engineer's design tasks as the guidance of reliability analysis procedure of safety design and make good conversation with other engineers in yard, class, company, etc.

Keywords : Offshore process(해양플랜트 프로세스), Model-Based Systems Engineering(MBSE, 모델기반 시스템엔지니어링), Safety design(안전설계), Safety Instrumented System(SIS, 안전시스템), Reliability analysis(신뢰도 분석), Knowledge modeling (지식 모델링), Safety Integrated Level(SIL, 안전 무결도)

1. 서 론

1.1 연구배경

해양플랜트의 설치 수가 전 세계적으로 증가하면서 관련 사고가 문제가 되고 있으며, 1995년 이후 석유생산에 관련된 해양플랜트에서의 사고는 한 해에 수백 건에 이르고 있으며, 수백 명이 다치거나 몇몇은 목숨을 잃는 경우도 있다 (HSE, 2011). 특히 해상에서 해저 수천 미터 아래에 있는 원유를 시추, 회수하여 정제, 송유 등의 작업을 수행하는 해양플랜트 공정의 경우 처리하는 가연성 기체 또는 원유의 양이 많으므로 화재/폭발 사고 시 막대한 피해를 남길 수 있다. 실제로 1988년 해양플랜트 'Piper Alpha'에서 일어난 사고의 경우, 167 여 명의 인명손실과 막대한 재산피해를 남기기도 했다. 해당 사고의 경우 안전시스템과 관련 장치들을 갖추고 있었음에도 불구하고 대형 사고로 이어진 것은, 예상치 못한 사고가 발생했거나 안전시스템이 정상적으로 작동하지 못했기 때문인 것으로 판단된다. 사고 이후, 해양플랜트 관련 산업에서는 높은 신뢰도를 가지는 안전시스템에 대한 중요성을 인식하고 있다. 노르웨이의 Norsk olje & gass에서는 기존 전기전자분야에서 널리 적용되어 오던 신뢰도 관련 규정인 IEC 61508과 프로세스 산업에서 적용되고 있는 IEC 61511을 노르웨이 석유산업에 적용하기 위한 가이드라인을 제시함으로써 신뢰

Received : 21 June 2017 | Revised : 5 December 2017 | Accepted : 11 April 2018
† Corresponding author : Min-jae Jung, mjjung@krs.co.kr

도 개념을 해양플랜트 시스템 설계에 적용하기 위한 초석을 마련하였다 (Norsk olje & gass, 2004). 또한 OLF(Oil Industry Association)는 'NORSOK STANDARD S-001'에 안전시스템에 대한 절차 및 요구조건과 관련된 규정을 포함시킴으로써 안전설계를 유도하고 있다 (The Norwegian Oil Industry Association (OLF) and The Federation of Norwegian Industry, 2008).

국내의 경우 기존의 철도, 화학플랜트, 원자력플랜트 분야에서의 안전시스템 관련 설계지식 및 경험을 해양플랜트 분야에 적용할 수 있는 방안을 모색하고 있다. 현재 조선소의 경우 해양플랜트 안전시스템의 신뢰도 분석과 안전설계 관련 업무를 수행하기 위해, 조선소 내의 기능 안전 엔지니어(functional safety engineer), HSE(Health, Safety, and the Environment) 담당자, 프로세스 담당자를 포함하여, 선급 및 선주 등의 외부 이해당사자들과 '요구사항문서 검토', 'SIL(Safety Integrity Level) 검증/확인', '문서 및 정보교환' 등의 업무를 진행하고 있다. 해양플랜트 시스템을 구성하는 요소들이 많아지고 복잡해짐에 따라 해당 업무와 관련된 원활한 의사소통이 점점 어려워지고 있으며, 설계오류, 항목 누락 및 중복 등으로 인한 시간적, 경제적 손실이 지속적으로 발생하고 있다. 오래전부터 이러한 복잡한 시스템 및 협업 체계를 효과적으로 관리하기 위해, 시스템엔지니어링 개념이 적용되어 왔으며, 최근 시스템을 이루는 구성요소들의 설계특성 및 연관관계들을 가시적인 다이어그램이나 구조화된 데이터로 구현한 전산 시스템 모델이 활용되고 있다. MBSE 모델은 복잡한 시스템 개발 프로젝트의 수행에 있어서 프로젝트 관리자, 사용자, S/W 전문가, 해석전문가, 설계자 등의 다양한 이해당사자들 간의 의사소통과 프로젝트 관련정보들의 교환을 네트워크 상에서 원활하고 신속하게 지원해줌으로써 효율적인 시스템 설계 및 개발을 가능하게 해주며, 해당 개념은 모델기반 시스템엔지니어링(이하 MBSE로 명칭) 개념으로 개발, 도입되어 발전되어 왔다.

1.2 연구동향

신뢰도가 높은 시스템을 설계하기 위해서는 먼저 신뢰도 분석이 수행되어야 하는데, 이와 관련된 국외연구의 경우, 시스템의 최적설계를 위해 단순화된 신뢰도 분석 기법을 제시한 후, 이를 해양플랜트 계류시스템에 적용한 연구가 있으며 (Mousavi & Paolo, 2014), 해양플랜트의 수명주기를 연장시키기 위해 구조물의 피로와 관련된 여러 가지 시나리오의 분석을 바탕으로 구조적 측면에서의 피로 신뢰도 분석을 수행한 연구도 있다 (Gholizada et al., 2012). 특히 안전시스템의 신뢰도 분석과 직접적으로 관련된 국외연구로는 FTA(Fault Tree Analysis)를 이용하여 시스템 구성요소의 고장률을 하위레벨로 정의한 후, HAZOP(HAZard and Operability) 수행을 바탕으로 설계를 개선함으로써 신뢰도를 향상시키는 방법을 제시한 연구가 있다 (Dragffy, 1998).

국내에서 신뢰도 분석과 관련된 연구는 비행제어시스템을 설계하여 신뢰도를 분석하고, 시뮬레이션 수행을 통해 시스템의 신뢰도 향상방안을 제안한 연구가 있으며 (Kim, 2011), 화재소방 분야에서 'Ethyl Benzene 공정의 화재/폭발 안전장치의 신뢰도 분석'을 통해 해당시스템이 목표 SIL에 알맞게 설계되었는지를 확인한 연구가 있다 (Ko et al., 2006). 또한 LNG bunkering 시스템에 설치된 가스센서, 압력센서, 차단밸브 등을 포함한 비상차단시스템의 신뢰도 분석을 수행하여 고장률 및 고장 간 평균시간을 도출한 연구도 있다 (Bae et al., 2014).

본 연구에서 대상으로 하는 해양플랜트 안전시스템의 설계와 같은 복잡한 시스템 및 협업체계를 관리하기 위한 개념인 MBSE와 관련된 연구는 비교적 최근부터 이루어져 왔다. 국외의 경우, NASA는 2016년부터 소행성 Bennu를 탐사하고 샘플을 채취해 오기 위한 프로젝트를 수행해오고 있으며, 이를 위해서 탐사선 개발뿐만 아니라 데이터의 송수신 및 처리, 동작 제어 등 수 많은 분야의 전문적인 지식이 필요하게 됨에 따라, SPOC(Science Processing and Operations Center)가 여러 관련 기관과의 업무를 원활하게 수행하기 위해 MBSE를 도입한 경우가 있다 (Daniel & Furfaro, 2015).

국내의 경우, Jaffari Aman (2015)이 의료공학에 MBSE를 적용함으로써 그 범위와 복잡도가 증가하고 있는 의료기기 개발에 있어, MBSE가 초기 설계된 시스템 모델을 수정, 보완하는 작업을 수행하는 데에 활용성이 높다는 것을 보였으며, 철도분야에서는 복잡하고 규모가 큰 고속철도 시스템에 대해, 안전기준 요구사항 및 성능시험 요구사항 구축을 위해 MBSE를 적용한 연구가 있다 (Choi et al., 2006). 항공분야에서는 Kim and Lee (2012)이 복잡한 통신 제어기능을 포함한 군사용 무인항공기를 개발하기 위해 시스템 공학 기법을 기반으로 개념설계 단계를 정의하고, SysML을 활용하여 MBSE를 적용한 연구가 있다.

1.3 연구목표 및 방법

요구사항이 다양하며 시스템을 이루는 구성요소가 복잡하고, 프로젝트의 규모가 큰 특징을 가지는 해양플랜트 시스템 개발 프로젝트를 수행함에 있어서, NASA가 소행성 탐사 프로젝트에 MBSE를 적용한 것과 같이, 그 효용성을 확인하고자 하는 것이 최종 목표이며, 본 연구에서는 시간, 비용 및 현실적 제한사항을 고려하여 부분 시스템인 분리공정에 대한 MBSE 적용을 수행하였다. 해양플랜트의 분리공정(separation process)에 설치되는 안전시스템을 대상으로 신뢰도 분석과 안전설계를 수행하는데 필요한 데이터, 정보, 경험들을 MBSE 모델로 체계화 하였으며, 기능 안전 엔지니어가 안전시스템을 효과적으로 설계하고, 이해당사자들 간의 원활한 의사소통을 지원할 수 있도록 하는 것을 목표로 하였다.

연구방법으로는 Fig. 1과 같이 신뢰도 분석에 대한 지식을 정리하여 MBSE 모델링을 수행한 후, 대상시스템의 안전시스템에 대한 신뢰도 분석을 수행하였다. 안전설계와 관련해서는 신뢰도 분석결과와 안전설계 지식을 함께 정리, 모델링하여 대상 시스템에 적용하는 방법으로 진행하였다.

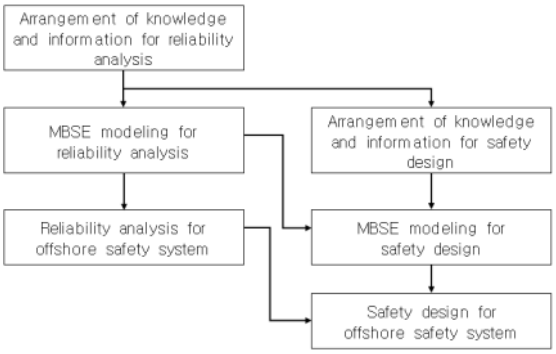

Fig. 1 Procedure of knowledge modeling with MBSE

신뢰도 분석 관련지식으로는 주로 안전시스템 개발 초기 설계 단계에서 검토하는 SIL 검증에 필요한 지식 및 정보를 중점적으로 정리하였다. 안전시스템에 대한 최소 요구 SIL을 설정하고, 설계 대안이 이를 만족하는지를 확인하기 위해 SIL을 결정하는 고장률 요소인 PFD(the average Probability of Failure to perform its design function on Demand)를 계산하고, 이를 통해 SIL을 평가하는데 까지를 대상 범위로 설정하였다.

PFD 계산 방법 및 관련 지식을 포함한 신뢰도 분석과, 다목적 최적설계 방법에 대한 안전설계 지식은 Eclipse 환경 기반 MBSE 모델링 툴인 'Papyrus'를 사용하여 모델링하였다. 블록정의(block definition) 다이어그램, 액티비티(activity) 다이어그램, 유스케이스(usecase) 다이어그램 등이 사용되었으며, 이들을 해양플랜트 첫 번째 분리공정에 설치되는 안전시스템의 신뢰도 분석 및 안전설계에 적용하여 MBSE 모델의 활용 가능성을 확인하였다.

2. 신뢰도 분석 MBSE 모델링

2.1 신뢰도 분석 지식 정리

2.1.1 신뢰도 분석

신뢰도 분석이란 특정 시스템이 주어진 환경에서 정해진 기능을 일정 시간 동안 올바르게 수행할 확률로써 해당 시스템의 설계 특성이라고 할 수 있으며, 단순히 고장률로 나타내거나, SIL로 나타내기도 한다. SIL이란 신뢰도 측면에서 안전시스템이 수행할 수 있는 능력의 정도를 PFD 값으로 정량적화 하여 분류한 것이며 Table 1과 같이 4 가지 수준으로 정의된다 (IEC, 2010).

Table 1 Definitions of SILs from IEC 61508

SIL	PFD (the average Probability of Failure to perform its design function on Demand)
4	$10^{-5} \le PFD < 10^{-4}$
3	$10^{-4} \le PFD < 10^{-3}$
2	$10^{-3} \le PFD < 10^{-2}$
1	$10^{-2} \le PFD < 10^{-1}$

PFD는 SIL을 결정하기 위한 시스템의 요구 시 고장률을 나타내는 값으로 본 연구에서는 PFDAVG와 의미가 같으며, 식 (1)과 같이 계산된다 (IEC, 2010).

$$PFD_{AVG} = \sum PFD_{SE} + \sum PFD_{LS} + \sum PFD_{PE} \quad (1)$$

PFDAVG는 안전과 관련된 시스템 전체의 요구 시 평균고장률이며, 시스템을 이루는 하부시스템인 PFDSE,, PFDLS, PFDPE는 각각 센서, 로직, 차단시스템의 PFD 값들의 합을 의미한다. PFDAVG 값은 시스템의 구성형태에 따른 고장률, 수리시간, 보증시험 주기 등의 변수들을 바탕으로 IEC 61508-6에서 제시한 계산식을 이용하여 계산할 수 있다 (IEC, 2010).

2.1.2 신뢰도 분석 관련 지식

신뢰도 분석과 관련된 표준으로는 미국에서 안전장치 및 제어시스템의 고장 감소를 위한 'IEC 61508'이 있으며, 전기전자 혹은 프로그래밍 가능한 전기적 안전시스템을 기본으로 자동차, 철도, 원자력 등의 모든 산업에 적용이 가능한 표준이다. 해당 표준에는 안전에 대한 시스템 요구사항, PFD 계산방법, SIL 개념 및 도출 방법에 대한 기본적인 것들을 포함하고 있다.

'IEC 61511: Functional safety – Safety instrumented systems for the process industry sector'는 프로세스 산업 분야에서의 안전시스템에 대한 표준으로, 본 연구의 대상인 해양플랜트 안전시스템에 대한 신뢰도 분석 및 안전설계를 수행하는데 있어서 주요 참조 문서로 볼 수 있다. IEC 61511는 안전시스템에 대한 요구사항, 설계, 설치, 유지/보수 등 수명주기 전체에 걸친 고려요소 및 지시 사항을 포함하고 있다.

신뢰도 분석을 위해서는 각종 장치들의 고장데이터가 필요하며, 이를 통계적으로 분석하여 정리한 데이터는 전기전자, 철도, 원자력플랜트 등 다양한 분야에 존재한다 (NTNU, 2017). 그 중 해양플랜트 안전시스템에 사용하기 적합하다고 판단되는 것은 'OREDA 2015 (SINTEF, 2015)', 'PDS data handbook (SINTEF, 2017)', 'Safety Equipment Reliability Handbook (Exida, 2015)' 등으로, 이를 신뢰도 분석 관련 지식으로 정의하였다.

신뢰도 분석에 대한 정의나 이론의 경우, 앞서 언급한 표준, 가이드라인, 데이터 등에 포함되어 있지만 일반적인 개념에 대한 이해가 필요한 경우, 'Risk-Based Reliability Analysis and Generic Principles for Risk Reduction (Michael, 2006)' 과 같이 'Reliability analysis' 키워드를 포함한 다양한 저서의 참조가 가능하다.

Fig. 2는 앞서 언급한 표준 및 데이터를 포함한 신뢰도 분석 관련 지식을 블록정의 다이어그램으로 모델링 한 그림이다. IEC 61508과 IEC 61511을 중심으로 주요 항목들과 그들 간의 관계들을 정리하였는데, IEC 61508는 7개의 소제목으로 이루어져 있으며, 그 중 IEC 61508-6이 일반적인 안전과 관련된 요구사항들

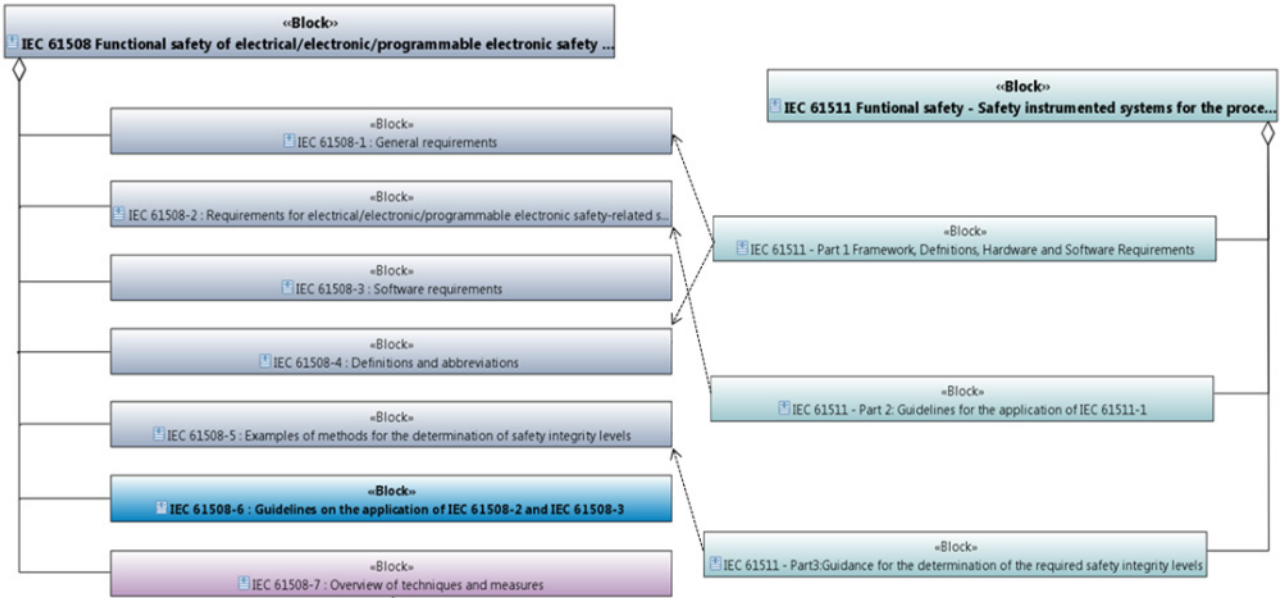

Fig. 2 Block definition diagram – 'Related guidelines and knowledge of reliability analysis'

을 기반으로 신뢰도 분석을 수행하는 실질적인 부분으로써 PFD를 포함한 각종 신뢰도 관련 값들을 계산하는 방법들이 기술되어 있다. IEC 61511의 경우 IEC 61508을 기반으로 프로세스 분야에서 어떻게 신뢰도 분석을 수행할 것인지에 대한 가이드라인을 3개의 파트로 제시하고 있으며 각 파트는 Fig. 2에서 점선으로 표시된 것과 같이 IEC 61508의 특정 소제목과 연관시켜 참조관계를 정리하였다. 특히 진하게 표시된 '<Block> IEC 61508-6: Guidelines on the application of IEC 61508-2 and IEC 61508-3'의 경우 고장률 계산 예시 및 관련 변수들의 도출방법을 포함한 부록들을 포함하고 있어, 실질적인 신뢰도 분석업무에 활용가능하다.

2.2 신뢰도 분석 MBSE 모델링

2.2.1 요구사항, 기능 분석 및 할당

신뢰도 분석에 대한 하위 요구사항은 'SIL 평가'와 'PFD 계산'으로 정의될 수 있으며, 이들을 만족하기 위한 기능은 Fig. 3과 같이 'SIL 평가 기능'과 'PFD 계산 기능'에 각각 할당된다. 할당된 기능들이 정상적으로 구현되어 SIL 값을 도출하거나 PFD 값 계산을 통해 하위 요구사항들을 모두 만족시키면 가장 상위 단계의 요구사항인 '신뢰도 분석'을 만족시키는 것으로 판단한다.

2.2.2 시스템 아키텍처 및 거동 분석

'PFD 계산'과 'SIL 평가' 기능들을 구현하기 위한 구성요소(component)들을 할당하고 하위 세부 구성요소들을 Fig. 4와 같이 블록정의 다이어그램으로 모델링하였다. 'SIL 평가 기능'은 'PFD 계산 기능'을 통해 PFD 값이 계산되고, 해당 값이 구성요

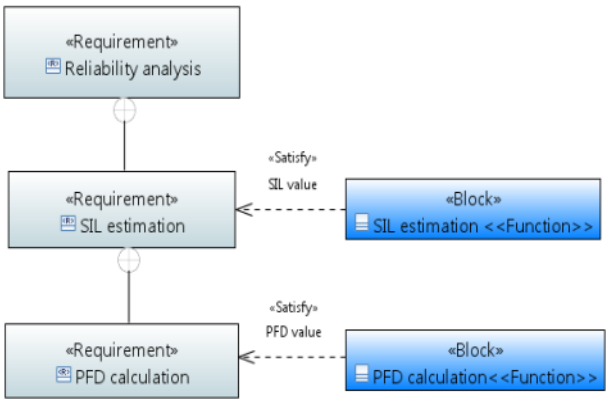

Fig. 3 Requirement diagram – 'Function allocation for reliability analysis model'

소 'SIL 평가기'(SIL estimator)에 입력 값으로 들어가게 되면, SIL을 도출하고 평가하는 역할을 한다. 이때, 구성요소 'PFD 계산기'는 각각 센서, 로직, 차단시스템의 PFD 값들을 계산하는 하부 구성요소들인 'PFDSE', 'PFDLS', 'PFDPE'로 구성된다. 각 구성요소들은 Fig. 4와 같이 계산에 필요한 변수, 계산을 수행하는 오퍼레이션(operation), 제한조건(constraints) 등으로 구성된다. 이들 간의 관계들을 정의함으로써 신뢰도 분석과 연관된 정보나 데이터들을 빠짐없이 확인하거나 추적, 관리가 가능하며, 필요에 따라 설계자의 경험 및 지식을 모델에 추가하여 활용할 수 있다.

신뢰도 분석 절차 및 거동을 확인하고 검증하기 위해 Fig. 5와 같이 액티비티 다이어그램을 활용하여 모델링을 수행하였다. SIL 평가 및 PFD 계산은 대상 시스템을 선정한 후, 고장시나리오를 작성하고 신뢰도블록 다이어그램(RBD: Reliability Block Diagram)을 모델링하는 절차로 수행된다. 시스템을 구성하는 장치들의 고장데이터를 OREDA 2015 (SINTEF, 2015), PDS data

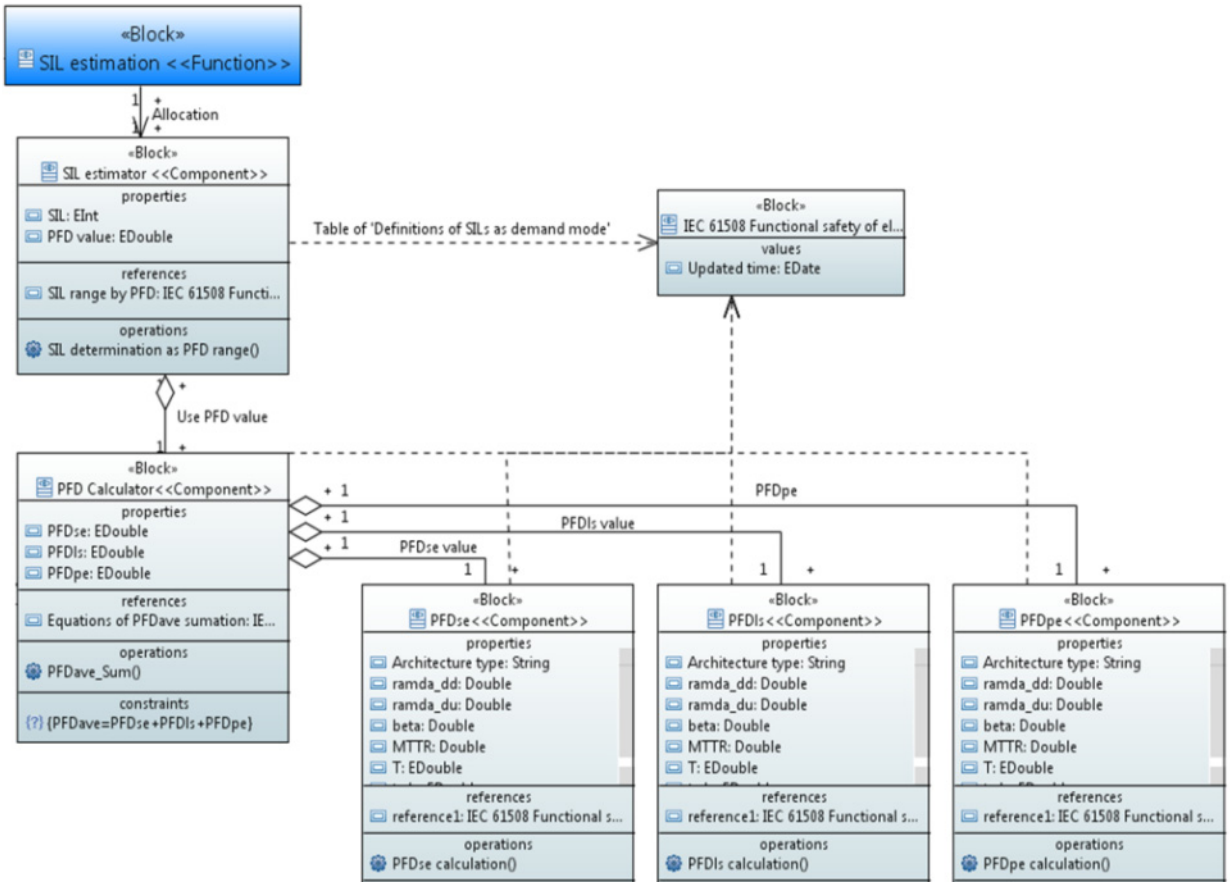

Fig. 4 Block definition diagram – 'SIL estimation & PFD calculation'

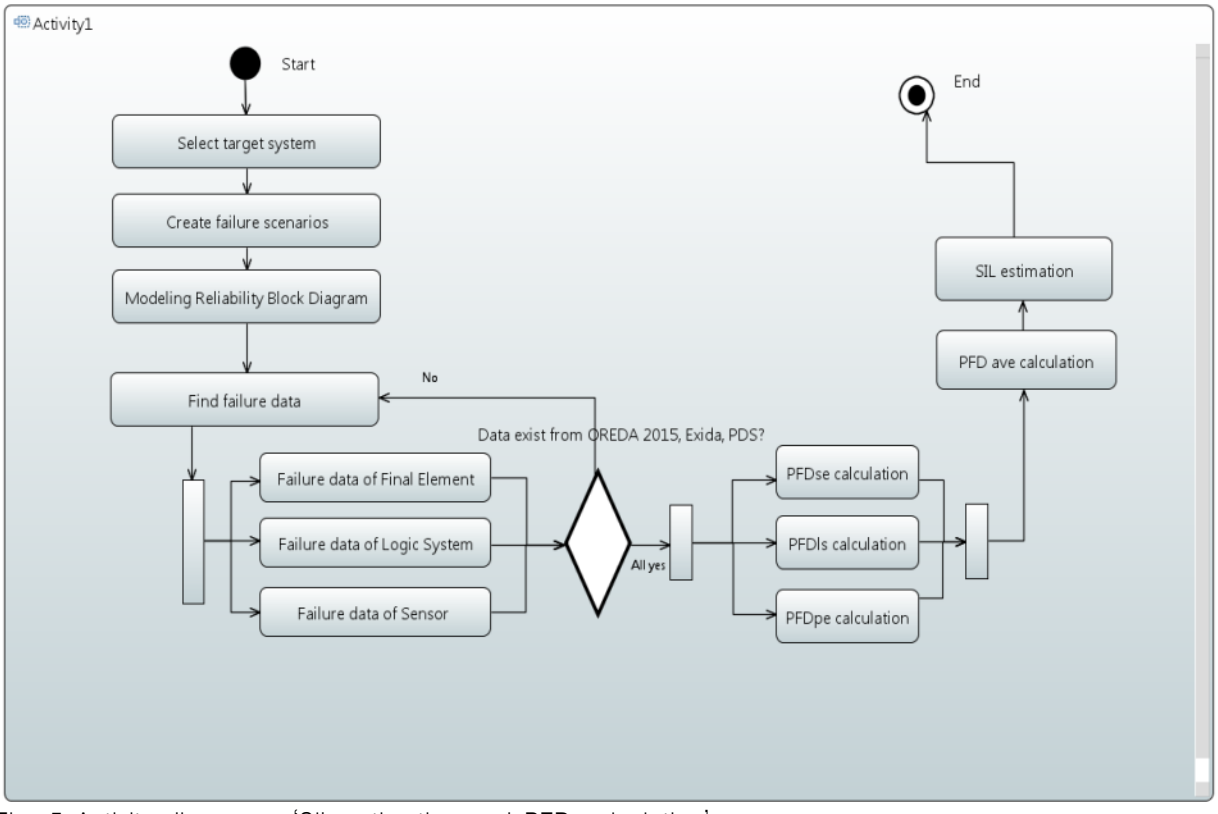

Fig. 5 Activity diagram – 'SIL estimation and PFD calculation'

handbook (SINTEF, 2015), Safety Equipment Reliability Handbook (Exida, 2015)에서 찾는 것이 모두 완료되면 센서, 로직, 차단시스템에 대한 PFD를 계산하고 합산하여 PFDAVG 값을 얻는다. 마지막으로 PFDAVG 값과 SIL 분류표를 비교하여 SIL을 평가한다.

3. 안전설계 MBSE 모델링

3.1 안전설계 지식정리

3.1.1 안전설계 정의

본 연구에서의 안전설계는 요구되는 SIL을 만족시키는 범위에서 가장 경제적인 설계안을 찾는 것으로 정의하였으며, 절차는 다음과 같다.

1) 기존 시스템에 대한 신뢰도 분석 및 SIL 도출

2) 신뢰도를 바탕으로 설계변경 대상 선정('요구 SIL을 만족하지 못하는 경우', '신뢰도 측면에서 과잉 설계된 경우', 'SIL을 만족하지만 PFD 값에 여유가 있는 경우')

3) 센서 및 차단시스템 종류, 보증시험주기, 시스템 구성 방법 등을 설계변수로 설정, 요구 SIL 범위 내에서 신뢰도와 경제성을 만족하는 다목적 최적설계 수행

안전시스템을 이루는 기본 요소인 센서, 로직, 차단시스템들을 다른 제품으로 대체하거나 여분(redundancy)을 추가하여 시스템 구조를 변경하는 방향으로 설계변경을 수행하였으며, 신뢰도와 경제성을 모두 만족시키는 설계안을 전역적으로 탐색할 수 있도록 NSGAII(Non-dominated Sorting Genetic Algorithm-II)를 적용하였다 (Deb et al., 2002).

3.1.2 문제의 정식화

안전설계를 위한 목적함수는 신뢰도를 나타내는 PFD와 경제성을 나타내는 비용함수로 설정하였다. PFD 값은 IEC 61508-6에서 제시한 시스템 구성에 따른 계산식을 참고하여 계산하였으며, 비용함수(CostTotal)는 장비교체비용(CReplace), 보증시험비용(CProoftest), 생산중단에 따른 손실비용(LossProducion)의 합으로 식 (2)와 같이 정의하였다.

$$Cost_{Total} = C_{Replace} + C_{Proof\ test} + Loss_{Production} \quad (2)$$

장치교체비용은 각 장치의 MTTF(Mean Time To Failure)를 바탕으로 해양플랜트 수명기간 25년 동안의 교체비용으로 식 (3)과 같이 정의하였다.

$$C_{Replace} = \frac{lifetime}{MTTF} \times Cost_{Product} \times Numbers_{\ Equipment} \quad (3)$$

보증시험 비용은 수명기간 동안 수행하는 시험 횟수와 장치 1개당 시험을 위해 소요되는 인건비인 단위 테스트 비용, 장치 수와의 곱으로 식 (4)를 이용하여 계산하였다.

$$C_{Prooftest} = \frac{Lifetime}{Test\ interval} \times Test cost_{\ Labor} \times Numbers_{Equip.} \quad (4)$$

보증시험수행으로 인한 생산중단에 따른 손실비용은 2017년 8월 17일 기준 WTI 국제원유 가격, Heidrun 유전의 단위시간 당 생산량, 시험시간 (Marvin, 2014)을 곱하여 식 (5)와 같이 계산하였다 (Smith, 2011).

$$Loss_{Production} = Price_{\ Oil} \times Production_{\ per time} \times Test\ time \quad (5)$$

안전시스템은 센서, 로직, 차단시스템 3가지로 구분되며 설계변수는 각 장치 별 예비 시스템의 수, 센서와 차단시스템의 종류, 보증시험주기를 포함한 총 6개의 설계변수를 Fig. 6과 같이 설정하였으며, 각 설계변수의 단위는 Table 2와 같이 설정하였다. 센서, 로직, 차단시스템의 여분 시스템의 수는 0개, 1개, 2개로 3가지 경우를 설계공간으로 정의하였으며, 센서는 3종류, 차단시스템은 9종류, 보증시험주기는 1~3년 범위로 설정하였다.

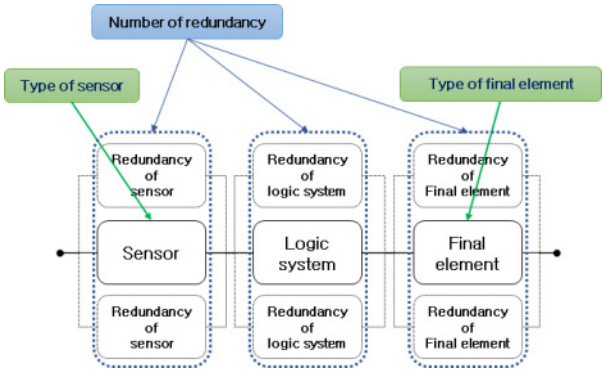

Fig. 6 Design variables

Table 2 Design variables and units

Design variable	unit
Number of redundancy - sensor	number
Number of redundancy - logic system	number
Number of redundancy - final element	number
Type of sensor	type
Type of final element	type
Proof test interval	year

제한조건은 PFD 값이 대상시스템에 요구되는 신뢰도 SIL을 만족하는 범위 내에 존재함으로 설정하여, 설계자가 요구하는 신뢰도 수준을 만족시킬 수 있도록 하였다.

3.1.3 결과 분석

각 시나리오에 대한 최적화 결과는 Fig. 7과 같이 두 가지 목적함수의 값이 설계공간 내에서 가장 최대인 점들을 이은 경계인 Pareto-frontier 형태로 도출되며, 이는 곧 frontier 상에 있는 설계 대안들은 목적함수가 모두 같은 수준의 적합도를 가지는 대안으로 볼 수 있으므로 설계자가 안전시스템의 상황과 특성에 맞는 대안을 선택해서 쓰면 되는 것으로 판단하였다. Fig. 7의 왼쪽 점의 경우 설계자가 신뢰도와 비용을 0.5, 0.5의 가중치를 주어 설계 대안을 선택한 예이며, 오른쪽 점은 본 연구에서 요구 SIL을 2 ($10^{-3} \leq PFD < 10^{-2}$)로 설정하였을 때, 이를 만족하는 대안 중, 가장 저렴한 비용을 가지는 설계대안의 값이다.

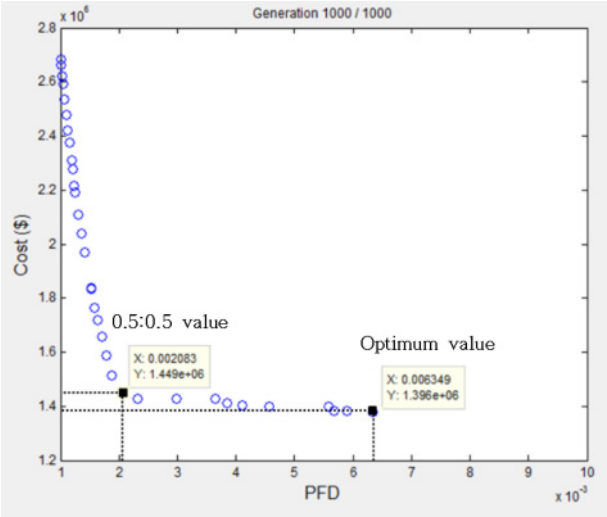

Fig. 7 '0.5:0.5' weighted value and chosen optimum value

3.2 안전설계 MBSE 모델링

3.2.1 요구사항 분석 및 기능할당

안전시스템의 설계에 대한 요구사항은 Fig. 8과 같이 '신뢰도'와 '비용' 2가지로 표현하였으며, 요구사항 다이어그램을 활용하여 기능과 구성요소의 할당 관계를 모델링하였다.

3.2.2 거동 분석

할당된 기능을 바탕으로 Fig. 9와 같이 유스케이스 다이어그램을 작성하였다. 기능 안전 엔지니어는 안전시스템에 대한 신뢰도 분석을 수행하는 기능과 설계자가 주도하는 설계에 대한 안전기능에 관여하며, 설계자는 최적설계를 위한 목적함수인 신뢰도

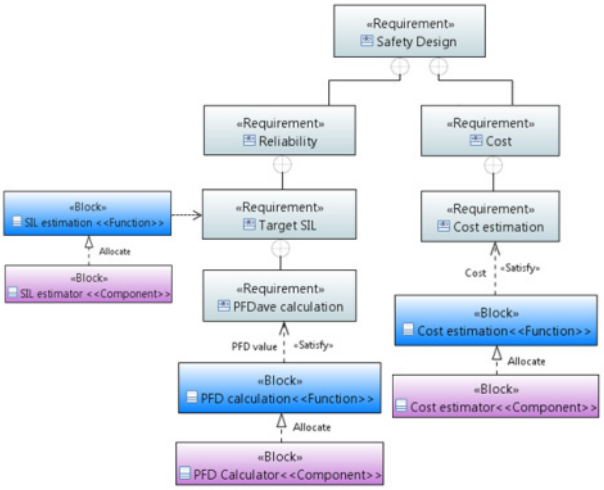

Fig. 8 Requirements diagram – 'Safety design'

와 경제성평가 기능, 설계기능 모두에 관여하며, 유스케이스 다이어그램을 통해 관련당사자들은 안전설계 시스템에 대한 경계 및 각자의 역할과 기능을 이해할 수 있다.

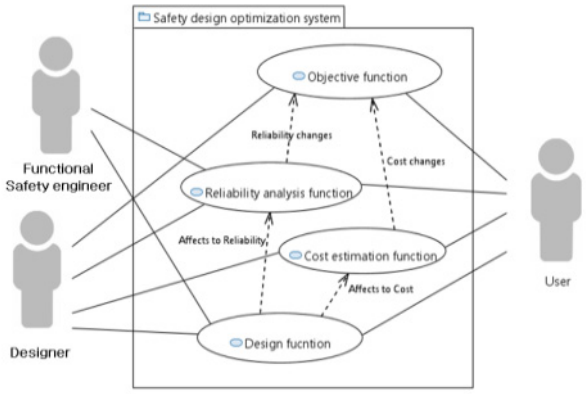

Fig. 9 Usecase diagram – 'Safety design system'

안전설계의 대상이 되는 안전시스템의 물리적 구성을 쉽게 이해하기 위해 Fig. 10과 같이 구성요소를 구조다이어그램 형태로 모델링하였다. 안전시스템의 주요 3가지 요소인 센서, 로직, 차단시스템과 여분 시스템의 개수를 Fig. 10의 중간 행, 가장 아래 행에는 각 구성 시스템들이 가지는 특성인 고장률, MTTR(Mean Time To Repair), 가격 등을 구성하여 신뢰도 분석, 경제성 평가 측면에서의 구성요소 정보를 파악할 수 있도록 하였다.

앞서 작성된 모델 중 Fig. 3, Fig. 4를 바탕으로 신뢰도 관련 블록을 작성하였으며, 문제의 정식화에서 정의된 비용함수를 포함하여 Fig. 11과 같이 안전설계를 수행하는 시스템의 거동을 블록정의 다이어그램으로 작성하였다. Fig. 11에서 왼쪽의 'PFD calculator'를 포함한 블록이 신뢰도 목적함수, 오른쪽의 'Cost estimator'를 포함한 블록이 경제성 목적함수를 구하는 구성요소이다. 해당 모델을 이용하면 최적화 관점에서 목적함수로 구성되는 신뢰도와 경제성을 이루는 요소들의 관계나 역할을 빠르고 명확하게 이해할 수 있다.

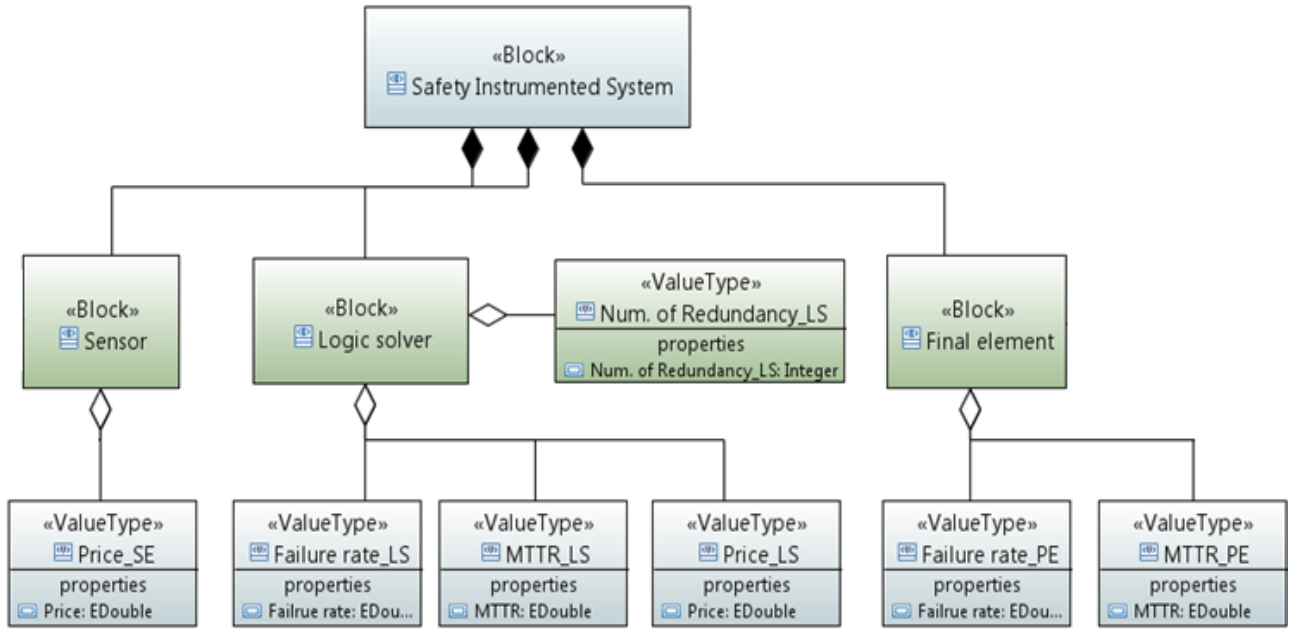

Fig. 10 Block definition diagram – 'Component structure of safety instrument system'

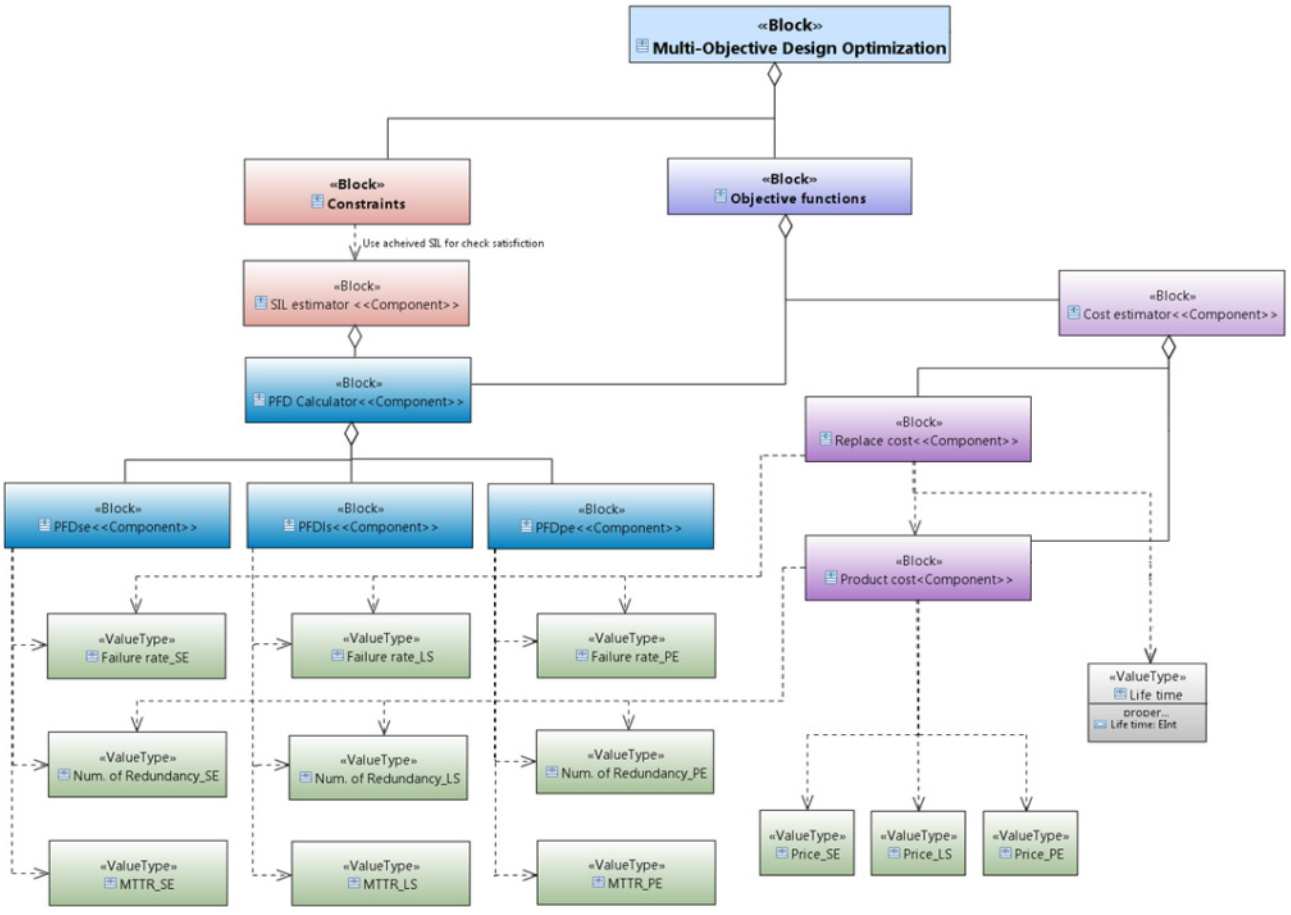

Fig. 11 Block definition diagram – 'Safety design optimization'

4. 적용 예 – 첫 번째 분리공정 안전시스템 설계

4.1 대상시스템 정의

대상시스템은 '첫 번째 분리공정 안전설계 시스템'으로 노르웨이 Heidrun 유전 TLP의 '첫 번째 분리공정 안전시스템'을 기능안전 엔지니어가 신뢰도, 경제성 기반 안전설계를 수행하기 위한 지식을 체계화한 모델로써 Fig. 12와 같이 선급, 선주(company) 및 조선소(yard or EPC) 관계자들과의 원활한 의사소통과 협업을 지원할 수 있도록 해주는 지원하는 역할을 한다.

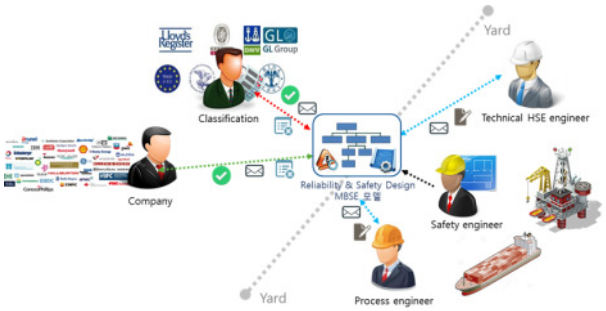

Fig. 12 Application of the MBSE for safety design system

4.2 MBSE 적용 절차

첫 번째 분리공정의 안전시스템에 대한 신뢰도 분석 및 안전설계를 위해서 Fig. 13과 같은 절차로 MBSE 모델을 적용하였다.

먼저 주어진 요구사항을 바탕으로 그를 만족 할 수 있게 해주는 기능을 할당하고, 기능을 구현하기 위한 구성요소들을 정의하였다. 두 번째로 액티비티 다이어그램을 작성하여 신뢰도 분석을 위한 업무 흐름을 이해할 수 있도록 하였다. 세 번째로 대상 시스템에 고장 시나리오를 신뢰도블록 다이어그램을 활용하여 작성한 후 네 번째, 다섯 번째로 SIL 평가 및 PFD 계산 방법을 확인하여 최종적으로 신뢰도 분석과 안전설계의 전체 레이아웃을 블록정의 다이어그램으로 모델링하여 MBSE 개념을 적용하였다.

4.3 신뢰도 분석

첫 번째 분리공정은 P&ID를 바탕으로 센서, 로직, 차단시스템에 해당하는 안전장치의 설치 위치에 따라 Fig. 14의 점선과 같이 아홉 부분으로 나누어 안전시스템을 정의하였다.

Fig. 14에서 정의된 안전시스템을 바탕으로 9개의 고장시나리오를 가정하였으며, 시나리오의 이름은 scenario의 약자를 따서 'S'로 시작되어 주요 라인의 특징 및 차단시스템의 종류에 따라 'S-PSV'(Pressure Safety Valve가 설치된 시나리오), 'S-Jet'(Jet water pump 연결 라인), 'S-Compressor'(압축기와 연결된 라인)

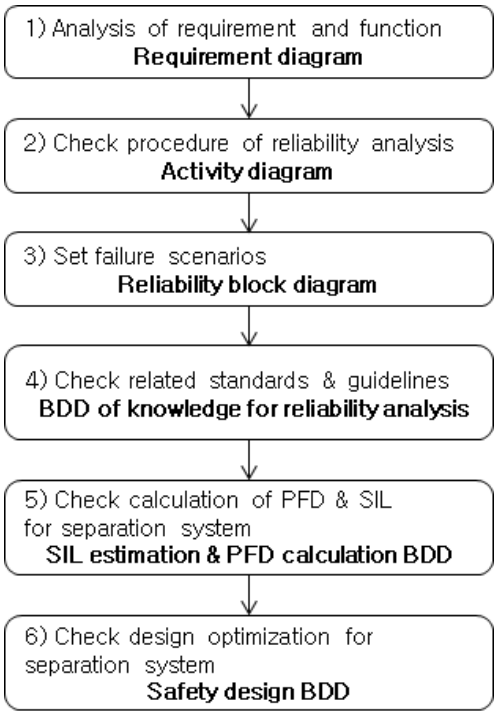

Fig. 13 The application procedure of the MBSE model for safety design

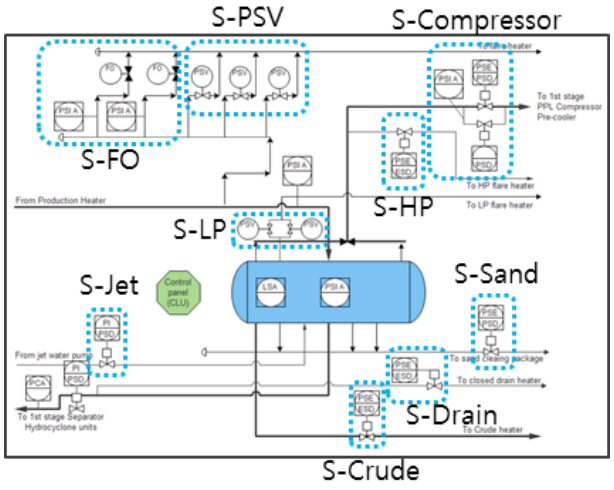

Fig. 14 Safety instrument system for 1st stage separation process

등으로 설정하였다. 고장시나리오들은 이상신호를 감지하는 센서, 센서로부터 받은 신호를 바탕으로 차단신호를 보낼 것을 판단하는 로직시스템, 차단을 수행하는 차단시스템으로 3가지 개념을 기본으로 하여 설정되었다.

IEC 61508-6에서 제시한 식 (1)을 참고하여 각 시나리오 별 PFD를 계산하였으며, 이를 바탕으로 Fig. 15와 같이 SIL을 평가하였다.

SIL 평가 결과, 시나리오 'S-Compressor'가 SIL 1로 신뢰도가 낮게, 'S-PSV'와 'S-LP'는 SIL 3으로 높게 도출되었다. 3개의 시나리오 이외에는 모두 SIL 2로 도출되었는데 해양플랜트의 원유

분리공정의 비상차단시스템이 SIL이 2가 되어야 한다고 가정하여, SIL 1 및 SIL 3인 시스템은 설계 개선이 필요한 것으로 판단하였다.

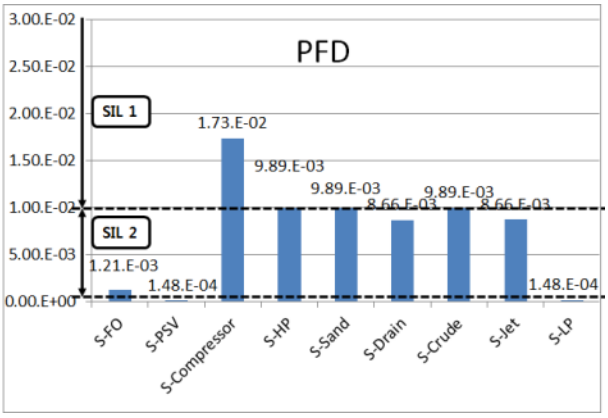

Fig. 15 Comparison of SIL and PFD as scenarios

4.4 안전설계

Fig. 11의 '안전설계 최적화' 블록정의 다이어그램을 활용하여 3.1.1절에서 정의한 안전설계의 절차에 따라 첫 번째 분리공정에 대한 최적설계문제를 정식화하고 최적화를 수행하였다. 설계변수로 센서 종류는 3가지, 차단시스템으로는 비상차단용 볼 밸브, 버터플라이 밸브 등을 포함한 9개의 종류를 Table 3과 같이 데이터베이스화하여 선택하는 개념으로 구현하였다 (Metso Automation, 2005).

각 하부시스템들의 특성 값 중 고장률, MTTR, 구입가격 등의 정보들이 최적화 시 목적함수 계산에 사용되었으며, 제한조건은 대상시스템이 해양플랜트 원유분리공정에 대한 비상차단시스템인 것을 고려하여 SIL 2로 설정하였다 (Norsk olje & gass, 2004). 9개의 시나리오들에 대한 안전설계의 결과 중, 'S-FO'(Flow Orifice가 설치된 라인) 시나리오의 결과만 예를 들어 살펴보면, 해양플랜트 분리공정에 적절한 수준이라고 판단되는 SIL 2를 만족하는 대안 중 비용이 최소인 대안 'Optimum value (0.07, 2013)'을 Fig. 16의 Pareto-frontier 상에서 선택할 수 있으며, 이때 설계변수는 Table 4와 같고, 이를 RBD로 나타내면 차단시스템 여분은 0개, 센서 종류는 'No. 2', 차단시스템의 종류는 'No. 3' 등으로 Fig. 17과 같다.

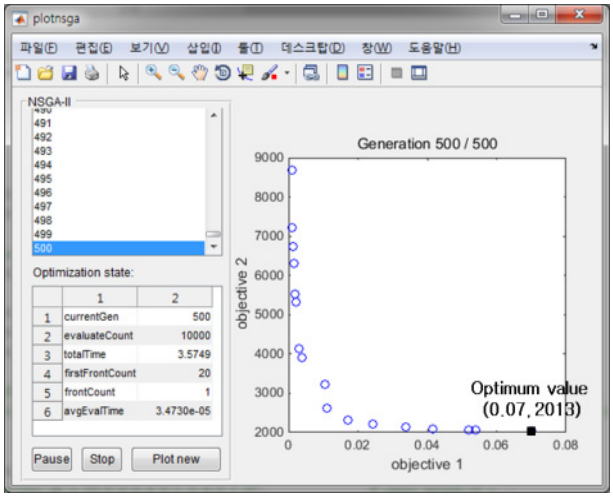

Fig. 16 Optimum value of scenario 'S-FO' on Pareto - frontier

Table 4 Design variables of optimum alternative 'S-FO'

Design variable	value	details
Sensor or input	0	No redundancy
Logic system	0	No redundancy
Final element or output	0	No redundancy
Type of sensor	2	Pressure sensor (Piezoelectric)
Type of final element	3	Flow orifice
Proof test interval	1.39	1year 4months 20days

Table 3 Type of sensors, logic system, final element for the safety design

element	Pressure sensor	Pressure sensor	Pressure sensor	Logic system	Final element	Final element	Final element	Final element	Final element	Final element	Final element	Final element
no.	1	2	3	-	1	2	3	4	5	6	7	8
name	S sensor	Pressure safety sensor (piezoelectric)	Rangeable wet differential pressure transmitter	All in one programmable logic controllers	L series butterfly valves	High pressure safety valve (pressure safety valve)	Restriction orifice plate meter (multiple orifice)	T series ball valve (ESD ball 1.1-5.0 inch)	T series 77 ball Valve (ESD ball)	D series ball valves	X series ball valves	X series ball valves 2
Failure rate	3.30E-7	4.10E-7	9.25E-7	28.54E-6	1.63E-06	8.47E-6	4.23E-6	22.27E-6	26.82E-6	4.75E-7	1.63E-6	3.80E-6
MTTR	4	4	6	6	4	8	8	6	6	8	6	4
DC	0.92	0.69	0.92	0.92	0.77	0.92	0.92	0.77	0.77	0.77	0.77	0.77
cost	$1,920	$605	$1,251	$1,077	$3,527	$642	$720	$1,417	$1,310	$5,641	$3,430	$3,041

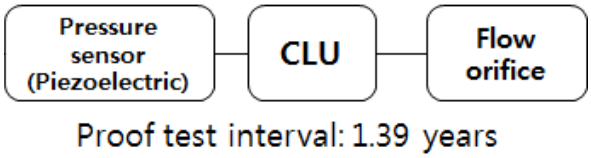

Fig. 17 RBD of optimum alternative 'S-FO'

4.5 MBSE 활용 요약

Table 5는 기능 안전 엔지니어가 첫 번째 분리공정의 안전시스템에 대한 최적설계를 수행하는데 직접적으로 활용한 MBSE 모델을 정리한 예이다.

Table 5 Usages of the MBSE models

MBSE model	Fig. num.	purpose
Requirements diagram	3, 8	Requirements elicitation and function allocation
Usecase diagram	9	Define and analyze concept of systems with actor
Block definition diagram – 'Related guidelines and knowledge of reliability analysis'	2	To recognize relation of IEC 61508 and 61511 standards
Block definition diagram – 'SIL estimation & PFD calculation'	4	Define PFD estimation with detail equation from IEC standards
Activity diagram – 'SIL estimation and PFD calculation'	5	Define procedure of PFD calculation and SIL estimation
Block definition diagram – 'Component structure of safety instrument system'	10	To show general structure of safety instrument systems and components
Block definition diagram – 'Safety design optimization'	11	To explain optimization method of safety instrument system

Fig. 18은 첫 번째 분리공정에 대한 PFD 계산과 SIL 평가를 수행하는데 있어서 앞서 작성한 Fig. 5의 액티비티 다이어그램을 활용한 예이며, 기능 안전 엔지니어가 각 절차 별 확인하고 수행해야할 자신의 업무들을 빠짐없이 업무 순서대로 파악하여 SIL 평가업무를 지원하는데 활용되었다.

또한 기능 안전 엔지니어가 선급, 선주 및 조선소 관계자들의 이해관계를 고려하여 효율적인 안전설계를 수행하기 위해서는 Table 6의 SIL 관련 이해당사자들과의 원활한 의사소통과 협업을 이끌어 내야 하는데, MBSE 모델의 주요 장점인 추적성을 해당 업무에 활용할 수 있다.Table 6의 첫 번째 항목인 'SIL study report'의 경우 선급 'ABS'에서 주요 업무를 수행한 후, 기능 안전 엔지니어 'FSE – EPC'는 'Technical HSE – EPC' 담당자와 프로세스 담당자 'Process – EPC'의 의견을 바탕으로 승인/거절하고, 그 결과를 선주 'company'에 알려주는 절차로 수행된다. 이 때 조선소'EPC' 내에서 의견을 교환하고 수렴하는 과정에서 가시적이고 추적성을 가지는 MBSE 다이어그램들을 공유, 활용함으로써 'SIL study report'에 관련된 개념을 쉽게 이해하고, 원활한 의사소통의 지원이 가능하다고 판단된다.

Table 6 The part of RAC matrix for SIL related tasks (NAM, 2017)

Task/deliverable description	Technical HSE – EPC	FSE – EPC	Process – EPC	ABS	company
SIL study report	C	A	C	R	
Collate comments on SIL draft report	A	R			
SIRS		R	C		A
SIL design verification	C	R	C		

R = Responsible; Those who do the work to deliver the task
A = Accountable; Those who have the authority to approve or disapprove the delivery of the task
C = Consultative; Those whose opinions are sought; and with whom there is two-way communication

Fig. 19는 센서의 고장률인 PFDSE 값이 변경되는 경우, PFDAVG와 함께 SIL과 교체비용이 변경되며, 이는 결과적으로 신뢰도와 비용에 영향을 주는 것을 보여주는 예이다. SIL은 최적설계 문제에서 제한조건과도 연관이 있으므로 'FSE – EPC'는 이에 대한 확인까지도 수행해야한다. 또한 비용 목적함수를 이루는 요소 중 교체비용이 달라짐에 따라 비용함수 전체에 변화를 가져올 수 있다. 이러한 추적성을 바탕으로 설계자는 설계변수나 제한조건, 시스템 환경, 요구사항 등이 달라짐에 따라 관련된 항목들을 확인하고 추적할 수 있어 변경으로 인한 후속업무를 누락시키지 않고 빠르게 처리할 수 있다.

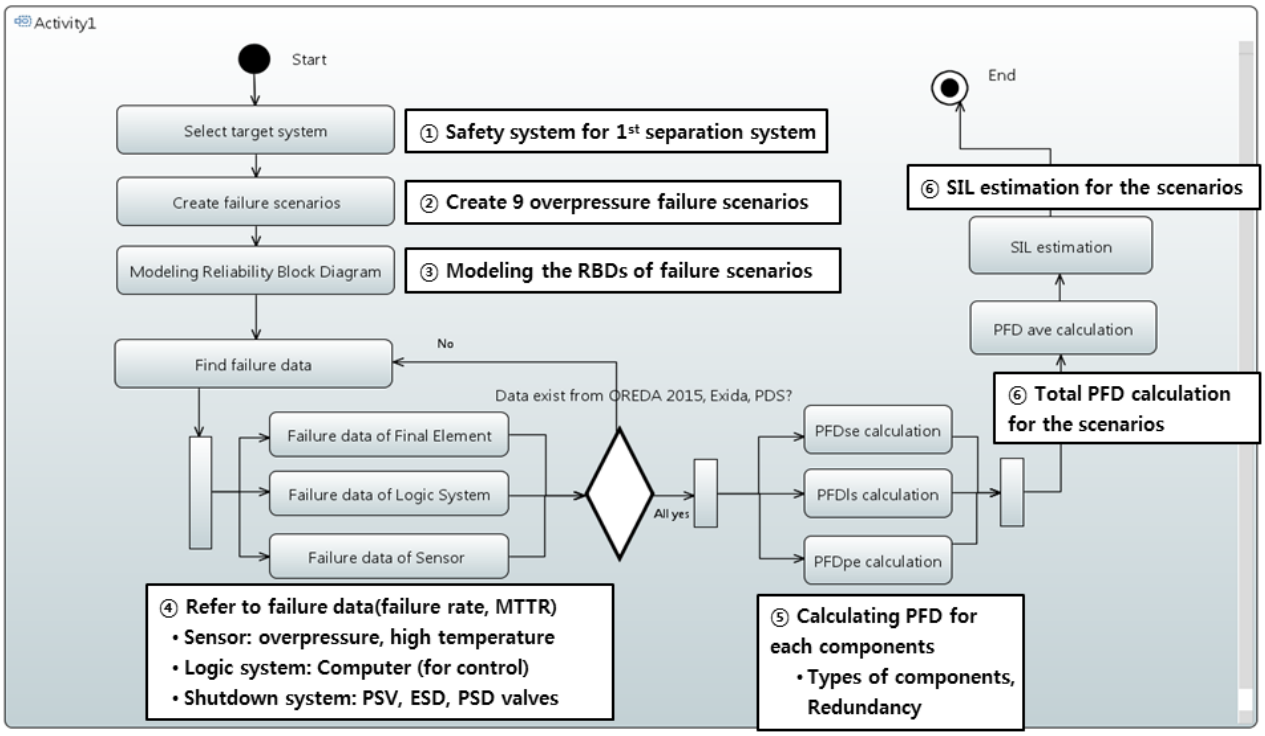

Fig. 18 The application procedure of 'Activity diagram – SIL estimation and PFD calculation'

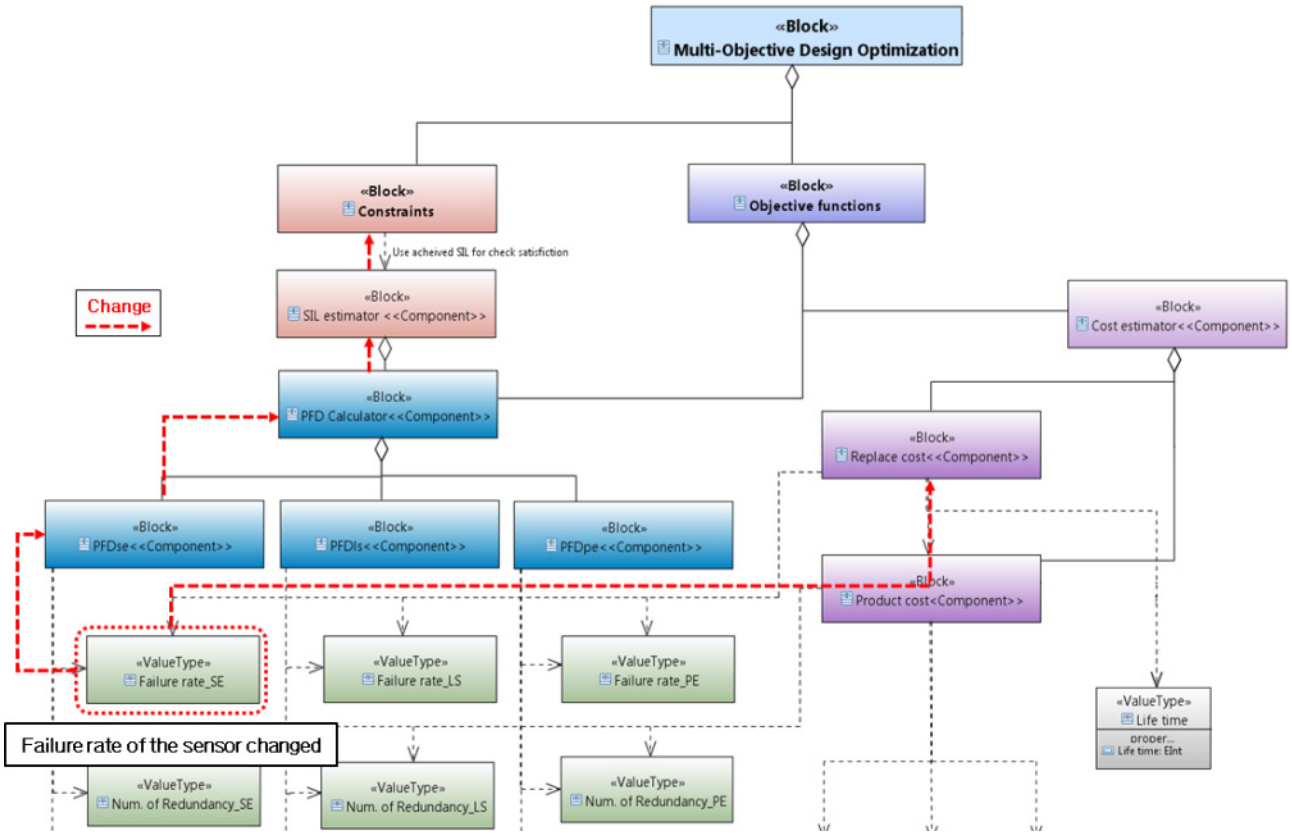

Fig. 19 Application of MBSE model – 'Use traceability'

5. 결 론

상기 연구를 통해 해양플랜트 안전시스템의 신뢰도 분석 중 SIL을 평가하는 방법과 관련지식을 MBSE를 활용하여 모델링함으로써, 기능 안전 엔지니어가 설계를 수행하는데 있어서 자신의 업무절차, 관련지식, 정보 등을 확인하거나 파악하기 용이하고, 관련 이해당사자들과 원활한 의사소통을 지원하는데 이용할 수 있다고 판단된다. 이는 기존의 설계자의 경험 및 기억이나 체계적으로 정리되지 않은 자료들을 기반으로 이루어지던 안전설계의 복잡한 업무를 MBSE 개념으로 모델링하여 체계화함으로써 중복, 누락으로 인한 업무오류를 예방하고 효율적인 설계를 수행할 수 있게 해주는 측면에서 활용성이 있다고 판단한다.

또한 해양플랜트 시스템에서 중요시 다루어지고 있는 안전시스템의 신뢰도와 경제성을 고려한 최적설계를 수행하는 방법과 관련된 지식, 정보들을 MBSE 모델로 체계화하여, 신입 기능 안전 엔지니어나 해당분야에 익숙하지 않은 설계자도 빠르게 업무를 파악할 수 있으며, 설계 결과의 품질도 일관성을 유지할 수 있을 것으로 판단한다.

본 연구에서는 해양플랜트 안전시스템의 신뢰도 분석 및 안전설계에 대하여 비교적 간단하고 작은 범위를 대상으로 함으로써, MBSE의 기본적인 적용 방법, 지식체계화, 활용성을 등을 확인하였다. 해당 연구결과를 바탕으로 분리공정 외의 다른 시스템을 추가, 포함하여 요구사항이 수백, 수천 개에 달하는 복잡하고 거대한 해양플랜트 개발 프로젝트 전체에 대하여 MBSE를 확장하여 적용해 나간다면, 더욱 의미 있는 지식의 모델링이 가능할 것이며, 그 활용성도 높아질 것으로 생각한다. 이를 위해서는 해당 시스템에 대한 경험이 많은 현업 전문가들을 중심으로 요구사항 분석 및 관리, 기능할당, 검증 등을 MBSE 개념으로 적용해야 할 것이다. 지식의 체계화 관점에서는, 표준 이외의 다양한 관련문서나 서적, 인터넷 링크들을 연관 모델링함으로써 관련 담당자 간의 업무 흐름파악이나 정보교환, 의사소통에 도움을 줄 수 있도록 한다면 효율적인 설계에 도움을 줄 수 있다고 판단된다.

추후, MBSE 모델의 활용성을 높이고 자동화 개념을 적용할 수 있도록 모델이 온라인으로 공유되고, 모델을 이루는 요구사항, 기능, 구성요소들 간의 변수 및 관계들이 파라메트릭하게 거동 될 수 있는 방안에 대한 연구가 필요하다고 생각된다.

후 기

이 논문은 부산대학교 기본연구지원사업(2년)에 의하여 연구되었음

References

Bae, J.H., Shin, S.C. & Kim, S.Y., 2014. Reliability analysis of ESD (Emergency ShutDown) system for supporting offshore plant design. *Proceedings of Naval Architects of Korea*, S.Korea, Busan, 2014. May, 22, pp.965-970.

Choi, Y.C., Park, Y.W. & Wang, J.B., 2006. A Study on constructing the requirement management system of the performance tests and safety standards of the high speed railway using model-based systems engineering approach. *International Journal of Railway*, 9(3), 2006.

Daniel, R. & Furfaro, R., 2015. Model-Based Systems Engineering approach for the development of the science processing and operations center of the NASA OSIRIS-Rex asteroid sample return mission. *Journal of Acta Astronautica*, 115, pp.147-159.

Deb, K., Pratap, A., Agarwal, S., Meyarivan, T., 2002. A fast and elitist multiobjective genetic algorithm: NSGA-II. *IEEE Transactions on Evolutionary Computation*, 6(2), pp.182-197.

Dragffy, G., 1998. The design of a highly reliable safety critical emergency shutdown system. *Reliability Engineering and System Safety*, 61, pp.215-227.

Exida, 2015. *SERH (Safety Equipment Reliability Handbook)*. Fourth Edition. exida.com LLC: PA, USA.

Gholizada, A., Golafshani, A.A. & Akrami, V., 2012. Structural reliability of offshore platforms considering fatigue damage and different failure scenarios. *Ocean Engineering*, 46, pp.1-8.

HSE (Health and Safety Executive), 2011. *Offshore Injury, ill health and incident statistics 10/2011*. [Online] (Updated 13 December 2012) Available at: http://www.hse.gov.uk/offshore [Accessed 27 March 2018].

IEC (INTERNATIONAL ELECTROTECHNICAL COMMISSION), 2010. I*EC 61508-6 Function safety of electrical/electronic/programmable electronic safety-related systems Part 6: Guidelines on the application of parts 2 and 3. : IEC Standards+ 61508:2010*. [Online] (Updated 30 April 2010) Available at: https://webstore.iec.ch/publication/5520 [Accessed 27 March 2018].

Jaffari, A., 2015. *Upper-arm rehabilitation robotics system modeling using SysML*. Maste's Thesis. Chonbuk National University.

Kim, S.S., 2011. *Study of reliability analysis method for redundant flight control system*. Ph.D. Thesis. Inha University.

Kim, Y.M. & Lee, J.C., 2012. On the use of SysML

models in the conceptual design of unmanned aerial vehicles. *The Journal of the KICS*, 37(2), pp.206-216.

Ko, J.S., Kim, H. & Lee, S.K., 2006. Reliability analysis on safety instrumented system by using safety integrity level for fire&explosion prevention in the ethyl benzene processes. *Fire Science and Engineering*, 20(3), pp.1-8.

Marvin, R., 2014, Reliability of safety-critical systems: theory and applications. John Wiley & Sons, Inc.: Hoboken, Newjersy.

Metso Automation, 2005. *ESD valve selection guide general ESD valve definition.* [Online] Available at: http://www.iceweb.com.au/valve/sdv_bdv_esd_valves/esdvalveselguide.pdf [Accessed 27 March 2018].

Michael, T., 2006. *Risk-based reliability analysis and generic principles for risk reduction*. Elsevier Science & Technology Books,: ELSERVIER B.V. Radarweb 29 P.O. Box 211, 1000 AE Amsterdam The Netherlands.

Mousavi, M.E. & Paolo, G., 2014. A simplified method for reliability- and integrity-based design of engineering systems and its application to offshore mooring systems. *Marine Structures*, 36, pp.88-104.

Nam, H.J., 2017. *Functional safety engineering (Professional training course)*. The 3rd seminar for sharing results of 'Project-based Process Engineer Coaching Program on Basic Design', Ch.4. EDRC: S. Korea, Seoul National Univ. building 311, 506.

Norsk olje & gass, 2004. *070 - Application of IEC 61508 and IEC 61511 in the norwegian petroleum industry*. [Online] (Updated 1 January 2017) Available at: https://www.sintef.no/projectweb/pds-main-page/pds-forum/olf070/ [Accessed 27 March 2018].

NTNU, 2017. *Ross gemini centre/resources/reliability data/reliability data sources*. (Updated 21 August 2013) Available at: https://www.ntnu.edu/ross/ info /data [Accessed 27 March 2018].

SINTEF, 2015. *OREDA Offshore reliability data 5th edition*. SINTEF Technology and Society Safety Research, N-7465 Trondheim NORWAY.

SINTEF, 2017. *Reliabilitiy data for safety instrumented systems*. SINTEF Technology and Society Safety Research. N-7465 Trondheim NORWAY.

Smith, D., 2011. *Reliability Maintainability and risk practical methods for engineers 8th edition*. Butterworth-Heinemann: The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, UK.

The Norwegian Oil Industry Association (OLF) and The Federation of Norwegian Industry, 2008. *Norsok standard S-001 technical safety*. (Updated 12 February 2009) Available at: http://www.standard.no/petroleum [Accessed 27 March 2018].


배 정 훈


정 민 재


신 성 철